Release Notes

Published
2021-04-07

Junos® OS Release 21.1R1 for the ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX

KEY FEATURES

- Refer to Key Features in Junos OS Release 21.1 to quickly learn about the most important Junos OS features and how you can deploy them in your network.

SOFTWARE HIGHLIGHTS

- Support for configuring multiple independent IGP instances of IS-IS (ACX Series, MX Series, and PTX Series)
- Support for flexible algorithm in OSPFv2 for segment routing traffic engineering (ACX Series, MX Series, and PTX Series)
- Support for strict SPF and IGP shortcut (ACX710, MX960, MX10008, MX2020, PTX5000, and PTX1000)
- New transport class-based architecture to facilitate service mapping over colored tunnels (ACX Series, PTX Series, MX Series)
- Support for BGP MVPN (Junos fusion for provider edge)
- Support for EVPN-MPLS (Junos fusion for provider edge)
- Support for interprovider and carrier-of-carrier VPNs (Junos fusion for provider edge)
- Next Gen Services (MX240, MX480, and MX960 with MX-SPC3)
- MVPN live-live solution support (MX Series)
- IS-IS link delay measurement and advertising (MX Series)
- Support for BGP Auto-discovered Neighbor (MX Series, PTX1000, PTX10008, QFX5120-32C, QFX5200, QFX5210, and QFX10008)

Juniper NETWORKS | Engineering Simplicity

- Support for displaying the timestamp in syslog (MX Series routers with MS-MPC, MS-MIC, and MX-SPC3)
- Support for PWHT (over EVPN-VPWS, on a transport logical interface) with subscriber management (BNG) service logical interfaces (MX Series)
- Support to view the software package installation or uninstallation status (MX480, MX960, MX2010, MX2020, SRX1500, SRX4100, SRX4400, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)
- Support for VRRP (PTX1000, PTX10002, PTX10008, and PTX10016)
- Support for microsegmentation on VLANs and VXLANs (QFX5110 and QFX5120)
- EVPN-VXLAN tunnel inspection (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)
- LLDP on routed and reth interfaces (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800)
- Policy-based threat profiling (SRX Series devices and vSRX)
- Traffic selector enhancements (SRX Series)
- Security policy enhancement for EVPN-VXLAN tunnel (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)
- Enhanced monitoring and troubleshooting of the flow session (SRX Series)
- Support for Snort IPS signatures (SRX Series and NFX Series)
- Packet-based ECMP support for Express Path (SRX5400, SRX5600, and SRX5800)
- Juniper Agile Licensing Support (vSRX)

HARDWARE HIGHLIGHTS

- New EX4400 Switch for Large Branch Offices, Campus Wiring Closets, and Data Centers
- Features Supported on MPC10E and MPC11E on MX Series Routers
- Support for JNP-100G-DAC-1M, JNP-100G-DAC-3M, and JNP-100G-DAC-5M DACs (QFX10002-60C)
- Support for the JNP-QSFP-100G-BXSR and the JNP-QSFP-40G-BXSR bidirectional transceivers

Day One+

- Use this new setup tool to get your Junos OS up and running in three quick steps.

Table of Contents

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, cRPD, cSRX, EX Series, JRRSeries, JuniperSecureConnect,Junos Fusion Enterprise,Junos Fusion ProviderEdge, MX Series, NFXSeries, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

These release notes accompany Junos OS Release21.1R1for the ACX Series, Containerized Routing Protocol Process (cRPD), cSRX Container Firewall (cSRX), EX Series, JRR Series, Juniper Secure Connect, Junos Fusion Enterprise,Junos Fusion Provider Edge, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, virtual MX Series router (vMX), Virtual Route Reflector (vRR), and vSRX Virtual Firewall (vSRX).They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Key Features in Junos OS Release 21.1

Start here to learn about the key features in Junos OS Release 21.1. For more information about a feature, click the link in the feature description.

- **Enhanced monitoring and troubleshooting of the flow session (SRX Series)**—Starting in Junos OS Release 21.1R1, we've introduced additional filters to the show security flow session operational command. The additional filters allow you to generate specified outputs in a list so that you can easily monitor the flow session. We've also introduced the show security flow session pretty and show security flow session plugins operational commands to view detailed information about the flow session.

  You can also trace the packet-drop information without committing the configuration using the monitor security packet-drop operational command. This command output is displayed on the screen until you press Ctrl+c or until the security device collects the requested number of packet drops. The command includes various filters to generate the output fields per your requirement.

  [See show security flow session, show security flow session pretty, show security flow session plugins, and monitor security packet-drop.]

- **EVPN-VXLAN tunnel inspection (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 21.1R1, we've introduced the following enhancements to the VXLAN support for SRX Series devices:

  - Support for SRX5000 line of devices in addition to the SRX4000 line and vSRX

  - Enhancements to tunnel inspection for VXLAN-encapsulated traffic by applying Layer 4 or Layer 7 security services to the tunnel traffic. The supported services are:

- Application identification
- IDP
- Juniper Advanced Threat Prevention (ATP Cloud)
- Unified threat management (UTM)

Layer 7 security services provide application-level security and protect users from security threats through VXLAN tunnel.

[See Configuring Tunnel Traffic Inspection.]

- **IS-IS link delay measurement and advertising (MX Series)**—Starting in Junos OS Release 21.1R1, you can measure and advertise various performance metrics in IP networks with scalability, by using several IS-IS probe messages. These metrics can then be used to make path-selection decisions based on network performance.

  [See How to Enable Link Delay Measurement and Advertising in IS-IS, delay-measurement, and delay-metric.]

- **LLDP on routed and reth interfaces (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 21.1R1, you can enable LLDP on all physical interfaces, including routed and redundant Ethernet (reth) interfaces. LLDP is a link-layer protocol used by network devices to advertise capabilities, identity, and other information to a LAN.

  [See LLDP Overview.]

- **MVPN live-live solution support (MX Series)**—Starting in Junos OS Release 21.1R1, we've added support to enable the MVPN live-live feature in next-generation multicast VPN (MVPN) with multicast LDP point-to-multipoint (P2MP) provider tunnel. This feature helps to keep your network live all the time.

  To enable the MVPN live-live solution:

  - Configure the **sender-based-rpf** option by running the **set routing-instances** ***routing-instance-name*** **protocols mvpn sender-based-rpf** command. This option is disabled by default.
  - Configure the **hot-root-standby** option by running the **set routing-instances** ***routing-instance-name*** **protocols mvpn hot-root-standby** command. You can configure this option only if sender-based RPF is enabled.

  When you enable this configuration, the receiving PE automatically switches over to the backup path if it encounters any failure while forwarding the traffic from the primary path to the customer network. The transition from primary path to backup path happens in less than 50 milliseconds.

  For previous Junos OS releases, we provided support only for RSVP-TE and IR provider tunnels.

  [See sender-based-rpf and hot-root-standby.]

- **New transport class-based architecture to facilitate service mapping over colored tunnels (ACX Series, PTX Series, MX Series)**—Starting in Junos OS Release 21.1R1, you can classify colored transport tunnels (RSVP, IS-IS flexible algorithm) in your network into transport classes and map service routes over an intended transport class. You can also extend the transport tunnels to span across multiple domains (ASs or IGP areas) by using the new BGP transport address family called BGP Classful Transport (BGP CT).

  This feature lays the foundation for network slicing and allows the different domains to interoperate irrespective of the transport signaling protocols used in each domain.

  [See https://www.juniper.net/documentation/us/en/software/junos/mpls/topics/topic-map/mpls-traffic-engineering-configuration.html#id_pjt_vxq_2pb.]

- **Packet-based ECMP support for Express Path (SRX5400, SRX5600, and SRX5800)**—In earlier releases, Express Path supported only session-based ECMP traffic. Starting in Junos OS Release 21.1R1, Express Path also supports packet-based ECMP traffic from different network processors of the SRX Series device. In the packet-based ECMP mode, the SPU creates multiple network processor sessions on multiple network processors at a time. This feature is enabled by default.

  [See Express Path.]

- **Support for BGP unnumbered neighbor (MX Series, PTX1000, PTX10008, QFX5120-32C, QFX5200, QFX5210, and QFX10008)** —Starting in Junos OS Release 21.1R1, we support the BGP unnumbered neighbor feature using the IPv6 Neighbor Discovery Protocol (NDP). This feature allows BGP to automatically create peer neighbor sessions using link local IPv6 addresses of directly connected neighbor routers using IPv6 NDP.

- **Support for BGP MVPN (Junos fusion for provider edge)**—Starting in Junos OS Release 21.1R1, Junos fusion for provider edge supports BGP multicast VPN (MVPN). BGP MVPN is a method for implementing multiprotocol multicast services over a BGP MPLS Layer 3 VPN. Junos fusion for provider edge supports the connection of a BGP-based MVPN customer edge (CE) device on the extended ports of the satellite device in Junos fusion for provider edge.

  [See Junos Fusion Provider Edge Supported Protocols.]

- **Support for configuring multiple independent IGP instances of IS-IS (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.1R1, you can configure and run multiple independent IGP instances of IS-IS simultaneously on a router.

  > **NOTE**: Junos OS does not support configuring the same logical interface in multiple IGP instances of IS-IS.

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

- **Support for displaying the timestamp in syslog (MX Series routers with MS-MPC, MS-MIC, and MX-SPC3)**—Starting in Junos OS Release 21.1R1, you can enable system log (syslog) timestamps in local system timestamp format or UTC format.

  On routers with MS-MPC, you can override the default UTC timestamp to local system timestamp format by configuring the new statement, **syslog-local-system-timestamp**, at the **edit interfaces *ms-interface\ams-interface*services-options** hierarchy level.

  On routers with MX-SPC3 cards, you can override the default local system timestamp in syslog to UTC format by configuring the existing statement,**utc-timestamp**, at the **edit interfaces *vms-interface\ams-interface*services-options** hierarchy level or at the **[edit services *service-set-name*syslog** hierarchy level.

  For the routers with MX-SPC3 cards, starting in Release 21.1R1 you can configure the **utc-timestamp** statement at the **edit interfaces *vms-interface\ams-interface*services-options** hierarchy level. In earlier releases, we support this statement at the **[edit services *service-set-name*syslog** hierarchy level.

  [See syslog (Services Service Set).]

- **Support for EVPN-MPLS (Junos fusion for provider edge)**—Starting in Junos OS Release 21.1R1, Junos fusion for provider edge supports EVPN-MPLS. EVPN-MPLS is a solution that extends Layer 2 VPN services over an MPLS network. Junos fusion for provider edge supports the connection of a customer edge (CE) device on the extended port of the satellite device in an EVPN-MPLS network.

  [See Junos Fusion Provider Edge Supported Protocols.]

- **Support for microsegmentation on VLANs and VXLANs (QFX5110 and QFX5120)**—Starting in Junos OS Release 21.1R1, you can configure egress filters with Layer 2 and Layer 3 match conditions in both VLAN and VXLAN deployments. Junos OS already supports filtering in Layer 2 match conditions in the ingress direction.

  To use egress filters for microsegmentation in a VXLAN, enable the **epacl-firewall-optimization** statement at the **[edit chassis]** level of the hierarchy and create the firewall rules with the match conditions that you want to filter on. For egress filtering on VLANs, you don't need to enable **epacl-firewall-optimization**. Both the QFX5110 and QFX5120 support egress filtering, for VLANs and VXLANs, with the following match conditions:

  - **ip-source-address**
  - **ip-destination-address**
  - **destination-port**
  - **destination-mac-address**
  - **user-vlan-id**

- **ip-protocol**

- **source-mac-address**

Valid actions for these rules are **accept**, **count**, and **discard**.

[See Overview of Firewall Filters (QFX Series) and Understanding Firewall Filter Match Conditions.]

- **Support for flexible algorithm in OSPFv2 for segment routing traffic engineering (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.1R1, you can thin-slice a network by defining flexible algorithms that compute paths using different parameters and link constraints based on your requirements. For example, you can define a flexible algorithm that computes a path to minimize IGP metric and define another flexible algorithm to compute a path based on traffic engineering metric to divide the network into separate planes. This feature allows networks without a controller to configure traffic engineering and utilize segment routing capability of a device.

  To define a flexible algorithm, include the **flex-algorithm** statement at the **[edit routing-options]** hierarchy level.

  To configure a device to participate in a flexible algorithm, include the **flex-algorithm** statement at the **[edit protocols ospf source-packet-routing]** hierarchy level.

  [See How to Configure Flexible Algorithms in OSPF for Segment Routing Traffic Engineering.]

- **Support for interprovider and carrier-of-carrier VPNs (Junos fusion for provider edge)**—Starting in Junos OS Release 21.1R1, Junos fusion for provider edge supports Interprovider and Carrier-of-Carrier VPNs. The Carrier-of-Carrier VPN service describes a hierarchical VPN (also known as a recursive VPN) model where one carrier (VPN service customer) transports its VPN traffic inside another carrier's VPN (VPN service provider). Junos fusion for provider edge currently supports provider edge (PE) routers for VPN service customers. In Junos OS Release 21.1R1, we introduce support for PE routers for VPN service providers along with VPN service customers.

  Interprovider VPNs provide connectivity between different service providers that are using separate autonomous systems (ASs) or one service provider that is using different ASs for different geographic locations. For Interprovider VPNs, Junos fusion for provider edge supports only intra-AS connection on an AS boundary router (ASBR) to the extended port.

  [See Junos Fusion Provider Edge Supported Protocols.]

- **Support for PWHT (over EVPN-VPWS, on a transport logical interface) with subscriber management (BNG) service logical interfaces (MX Series routers)**—Starting in Junos OS Release 21.1R1, you can deploy broadband network gateways (BNGs) that are connected to aggregation networks running EVPN-VPWS. You configure pseudowire headend termination (PWHT) on a transport logical interface that is on the pseudowire subscriber interface. The BNG pops the EVPN and VPWS headers and terminates subscribers at Layer 2.

  This feature includes support for:

  - All broadband features available on PWHT on MX Series routers
  - Single-homed EVPN-VPWS with the pseudowire subscriber interface anchored to a logical tunnel (LT) interface
  - Choice of whether or not to use a control word

- **Support for Snort IPS signatures (SRX Series and NFX Series)**—Starting in Junos OS Release 21.1R1, Juniper Networks IDP supports Snort IPS signatures. IDP secures your network by using signatures that help to detect attacks. Snort is an open-source intrusion prevention system (IPS). You can convert the Snort IPS rules into Juniper IDP custom attack signatures using the Juniper Integration of Snort Tool (JIST). These rules help detect malicious attacks.

  - JIST is included in Junos OS by default. The tool supports Snort version 2 and version 3 rules.
  - JIST converts the Snort rules with snort-ids into equivalent custom attack signatures on Junos OS with respective snort-ids as the custom attack names.
  - When you run the **request** command with Snort IPS rules, JIST generates **set** commands equivalent to the Snort IPS rules. Use the **request security idp jist-conversion** command to generate the **set** commands as CLI output. To load the **set** commands, use the **load set terminal** statement or copy and paste the commands in the configuration mode, and then commit. You can then configure the existing IDP policy with the converted custom attack signatures.
  - All the Snort IPS rule files that didn't get converted are written to **/tmp/jist-failed.rules**. The error log files generated during the conversion are written to **/tmp/jist-error.log**.
  - To view the jist-package version, use the **show security idp jist-package-version** command.

  [See Understanding Snort IPS Signatures, request security idp jist-conversion , and show security idp jist-package-version .]

- **Support for strict SPF and IGP shortcut (ACX710, MX960, MX10008, MX2020, PTX5000, and PTX1000)**—Starting in Junos OS Release 21.1R1, you can configure segment routing algorithm 1 (strict SPF) and advertise its SIDs in IS-IS link-state PDU (LSPDU) and use these SIDs to create SR-TE tunnels to forward the traffic by using the shortest IGP path to reach the tunnel endpoint while avoiding loops. You can also specify a set of prefixes in the import policy, based on which the tunnel can redirect the traffic to a certain destination. You can use algorithm 1 (strict SPF) along with algorithm 0 (default SPF) by default when Source Packet Routing in Networking (SPRING) is enabled.

  [See How to Enable Strict SPF SIDs and IGP Shortcut, prefix-segment, and source-packet-routing.]

- **Support for VRRP (PTX1000, PTX10002, PTX10008, and PTX10016)**—Starting in Junos OS Release 21.1R1, PTX1000, PTX10002, PTX10008, and PTX10016 routers support VRRP. However, these routers do not support the following VRRP features:

  - VRRP on IRB

- Dual tagging
- GRES
- VRRP on logical tunnel (LT) interfaces
- Layer 2 VRRP

  [See Understanding VRRP.]

- **Policy-based threat profiling (SRX Series devices and vSRX)**—Starting in Junos OS Release 21.1R1, you can add the user source identity (username) to a security policy to generate security feeds.

  Juniper ATP Cloud service consolidates the generated feeds from SRX Series device and shares the duplicated results back with that security device. The security device uses the feeds to perform actions against the designated traffic. You can enable the security device to use the feeds by configuring security policies with the feeds as matching criteria. When traffic matches policy conditions, the device applies policy actions.

  [See Threat Profiling Support in Security Policy.]

Junos OS Release Notes for ACX Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for the ACX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

What's New in 21.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for the ACX Series.

EVPN

- **Support for EVPN E-Tree service (ACX5448)**—Starting with Junos OS Release 21.1R1, you can configure an EVPN Ethernet Tree (E-Tree) service on ACX5448 routers.

  [See EVPN-ETREE Overview.]

- **Support for inter-DC connectivity over a Layer 3 network (ACX5448)**—Starting with Junos OS Release 21.1R1, you can configure the ACX5448 router to support IRB interfaces in an EVPN-MPLS network. This feature supports EVPN Type 2 (MAC/IP advertisement) and EVPN Type 5 (IP prefix) routes.

  [See EVPN with IRB Solution Overview.]

- **Support for single-active multihoming redundancy in EVPN-VPWS with flexible cross-connect support (ACX5448)**—Starting with Junos OS Release 21.1R1, you can configure the interfaces on the ACX5448 router in an Ethernet VPN–virtual private wire service (EVPN-VPWS) network with flexible cross-connect (FXC) or legacy cross-connect (non-FXC) service to support single-active multihoming redundancy for traffic that flows from customer edge devices to the core. EVPN-VPWS also supports load balancing with equal-cost multipath (ECMP) fast reroutes (FRR) on IGP and over BGP multipaths that face the core.

  [See Overview of Flexible Cross-Connect Support on VPWS with EVPN and Configuring EVPN Active-Standby Multihoming.]

- **Tunnel endpoint in the PMSI tunnel attribute field for EVPN Type 3 routes (ACX5448, EX4600, EX4650, EX9200, and QFX10002)**—Starting in Junos OS Release 21.1R1, you can set the tunnel endpoint in the provider multicast service interface (PMSI) tunnel attribute field to use the ingress router's secondary loopback address. When you configure multiple loopback IP addresses on the local provider edge (PE) router and the primary router ID is not part of the MPLS network, the remote PE router cannot set up a PMSI tunnel route back to the ingress router.

  To configure the router to use a secondary IP address that is part of the MPLS network, include the **pmsi-tunnel-endpoint*pmsi-tunnel-endpoint*** statement at the **[edit routing-instances *routing-instance-name* protocols evpn]** hierarchy level for both EVPN and virtual-switch instance types.

  [See EVPN.]

- **Aliasing for all-active multihoming with EVPN-MPLS (ACX5448)**—Starting in Junos OS Release 21.1R1, ACX5448 routers support aliasing for EVPN-MPLS all-active multihoming with ELAN services. Aliasing enables remote provider edge (PE) devices to load balance Layer 2 traffic toward a multihomed customer edge (CE) device among the PEs that have the same EVPN segment ID (ESI) for that CE device.

  You enable aliasing when you configure the **load-balance per-packet** routing policy statement at the **[edit policy-options policy-statement]** hierarchy and **export** the policy statement at the **[edit routing-options forwarding-table]** hierarchy. This feature is supported in routing instances of type **evpn** with VLAN-based and VLAN bundle services.

  [See EVPN Multihoming Overview.]

MPLS

- **New transport class-based architecture to facilitate service mapping over colored tunnels (ACX Series, PTX Series, MX Series)**—Starting in Junos OS Release 21.1R1, you can classify colored transport tunnels (RSVP, IS-IS flexible algorithm) in your network into transport classes and map service routes over an intended transport class. You can also extend the transport tunnels to span across multiple domains (ASs or IGP areas) by using the new BGP transport address family called BGP Classful Transport (BGP CT).

This feature lays the foundation for network slicing and allows the different domains to interoperate irrespective of the transport signaling protocols used in each domain.

[See https://www.juniper.net/documentation/us/en/software/junos/mpls/topics/topic-map/mpls-traffic-engineering-configuration.html#id_pjt_vxq_2pb.]

Network Management and Monitoring

- **Operational command RPCs support returning JSON and XML output in minified format in NETCONF sessions (ACX1000, ACX1100, ACX2100, ACX4000, ACX5048, ACX5096, ACX5448, EX2300, EX2500, EX3400, EX4300, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48P, EX4400-48T, EX4600, EX4650, EX9200, MX104, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10001, PTX10002, PTX10008, PTX10016, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX10002, QFX10002-60C, QFX10008, QFX10016, SRX550, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, operational command RPCs, including the **<get-configuration>** RPC, support the **format="json-minified"** and **format="xml-minified"** attributes in NETCONF sessions to return JSON or XML output in minified format. Minified format removes any characters that are not required for computer processing—for example, unnecessary spaces, tabs, and newlines. Minified format decreases the size of the data, and as a result, can reduce transport costs as well as data delivery and processing times.

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

Routing Protocols

- **Support for configuring multiple independent IGP instances of IS-IS (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.1R1, you can configure and run multiple independent IGP instances of IS-IS simultaneously on a router.

  > **NOTE**: Junos OS does not support configuring the same logical interface in multiple IGP instances of IS-IS.

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

- **Support for flexible algorithms in IS-IS for segment routing–traffic engineering (SR-TE) (ACX Series)**—Starting in Junos OS Release 21.1R1, you can thin-slice a network by defining flexible algorithms that compute paths using different parameters and link constraints based on your requirements. For example, you can define a flexible algorithm that computes a path to minimize the IGP metric and another flexible algorithm to compute a path based on the traffic engineering metric to divide the network into separate planes. This feature enables networks without a controller to configure traffic engineering and utilize the segment routing capability of a device.

To define a flexible algorithm, include the **flex-algorithm** statement at the **[edit routing-options]** hierarchy level. To configure a device to participate in a flexible algorithm, include the **flex-algorithm** statement at the **[edit protocols isis segment routing]** hierarchy level.

[See Understanding IS-IS Flexible Algorithm for Segment Routing.]

Segment Routing

- **Support for flexible algorithm in OSPFv2 for segment routing traffic engineering (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.1R1, you can thin-slice a network by defining flexible algorithms that compute paths using different parameters and link constraints based on your requirements. For example, you can define a flexible algorithm that computes a path to minimize IGP metric and define another flexible algorithm to compute a path based on traffic engineering metric to divide the network into separate planes. This feature allows networks without a controller to configure traffic engineering and utilize segment routing capability of a device.

  To define a flexible algorithm, include the **flex-algorithm** statement at the **[edit routing-options]** hierarchy level.

  To configure a device to participate in a flexible algorithm, include the **flex-algorithm** statement at the **[edit protocols ospf source-packet-routing]** hierarchy level.

  [See How to Configure Flexible Algorithms in OSPF for Segment Routing Traffic Engineering.]

- **Support for strict SPF and IGP shortcut (ACX710, MX960, MX10008, MX2020, PTX5000, and PTX1000)**—Starting in Junos OS Release 21.1R1, you can configure segment routing algorithm 1 (strict SPF) and advertise its SIDs in IS-IS link-state PDU (LSPDU) and use these SIDs to create SR-TE tunnels to forward the traffic by using the shortest IGP path to reach the tunnel endpoint while avoiding loops. You can also specify a set of prefixes in the import policy, based on which the tunnel can redirect the traffic to a certain destination. You can use algorithm 1 (strict SPF) along with algorithm 0 (default SPF) by default when Source Packet Routing in Networking (SPRING) is enabled.

  [See How to Enable Strict SPF SIDs and IGP Shortcut, prefix-segment, and source-packet-routing.]

What's Changed

IN THIS SECTION

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

What's Changed in Release 21.1R1

IN THIS SECTION

General Routing

Support for unicast ARP request on table entry expiration—You can configure the device to send a unicast ARP request instead of the default broadcast request when an ARP table entry is about to expire. The retry requests are unicast at intervals of 5 seconds. Without this option, the retry requests are broadcast at intervals of 800 milliseconds. This behavior reduces ARP overall broadcast traffic. It also supports the use case where access nodes are configured not to forward broadcast ARP requests toward customer CPEs for security reasons and to instead translate ARP broadcasts to unicast requests. To confirm whether this is configured, you can issue the following command: **show configuration system arp | grep unicast-mode-on-expire**.

[See arp.]

Junos XML API and Scripting

- **The jcs:invoke() function supports suppression of root login and logout events in system log files for SLAX commit scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The **jcs:invoke()** extension function supports the **no-login-logout** parameter in SLAX commit scripts. If you include the parameter, the function does not generate and log **UI_LOGIN_EVENT** and **UI_LOGOUT_EVENT** messages when the script logs in as root to execute the specified remote procedure call (RPC). If you omit the parameter, the function behaves as in earlier Junos OS releases in which the root **UI_LOGIN_EVENT** and **UI_LOGOUT_EVENT** messages are included in system log files.

  [See invoke() Function (SLAX and XSLT).]

- **The jcs:invoke() function supports suppression of root login and logout events in system log files for SLAX event scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The

jcs:invoke() extension function supports the **no-login-logout** parameter in SLAX event scripts. If you include the parameter, the function does not generate and log **UI_LOGIN_EVENT** and **UI_LOGOUT_EVENT** messages when the script logs in as root to execute the specified remote procedure call (RPC). If you omit the parameter, the function behaves as in earlier releases in which the root **UI_LOGIN_EVENT** and **UI_LOGOUT_EVENT** messages are included in system log files.

[See invoke() Function (SLAX and XSLT).]

- **Python 2.7 deprecation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, devices running Junos OS no longer support Python 2.7. We've deprecated the corresponding **language python** statement at the **[edit system scripts]** hierarchy level. To execute Python scripts, configure the **language python3** statement at the **[edit system scripts]** hierarchy level to execute the scripts using Python 3.

  [See Understanding Python Automation Scripts for Devices Running Junos OS.]

Network Management and Monitoring

- **Support for specifying the YANG modules to advertise in the NETCONF capabilities and supported schema list (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—You can configure devices to advertise third-party, standard, and Junos OS native YANG modules in the capabilities exchange of a NETCONF session by configuring the appropriate statements at the **[edit system services netconf hello-message yang-module-capabilities]** hierarchy level. In addition, you can specify the YANG schemas that the NETCONF server should include in its list of supported schemas by configuring the appropriate statements at the **[edit system services netconf netconf-monitoring netconf-state-schemas]** hierarchy level.

  [See hello-message and netconf-monitoring.]

- **Support for disconnecting unresponsive NETCONF-over-SSH clients (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—You can enable devices to automatically disconnect unresponsive NETCONF-over-SSH clients by configuring the **client-alive-interval** and **client-alive-count-max** statements at the **[edit system services netconf ssh]** hierarchy level. The **client-alive-interval** statement specifies the timeout interval in seconds, after which, if no data has been received from the client, the device requests a response. The **client-alive-count-max** statement specifies the threshold of missed client-alive responses that triggers the device to disconnect the client, thereby terminating the NETCONF session.

  [See ssh (NETCONF).]

User Interface and Configuration

Verbose format option to export JSON configuration data (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)—The Junos OS CLI exposes the **verbose** statement at the **[edit system**

export-format json] hierarchy level. We changed the default format to export configuration data in JSON from **verbose** to **ietf** starting in Junos OS Release 16.1R1. You can explicitly specify the default export format for JSON configuration data by configuring the appropriate statement at the **[edit system export-format json]** hierarchy level. Although the **verbose** statement is exposed in the Junos OS CLI as of the current release, you can configure this statement starting in Junos OS Release 16.1R1.

[See export-format.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for ACX Series routers.

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

General Routing

- On the ACX710 router, the PTP Servo status shows holdover during transition between virtual port and PTP. PR1510880
- On the ACX710 router, the SyncE to 1PPS transient test results do not meet G.8273.2 SyncE to 1PPS transient metric. PR1522796
- On the ACX710 router, T1 or T4 cTE should be tuned closer to two-way CTE. PR1527347
- On the ACX5448 router, there is a two-way time error and CTE for 1PPS does not meet the class A metrics. PR1535434
- On the ACX710 router, changing the PTP profile type from g.8275.1 to g.8275.2 requires the Packet Forwarding Engine to reboot and the clksyncd process to restart. As a workaround, you must reboot the Packet Forwarding Engine and restart the clocking process before you change the profile. PR1546614

- On the ACX710 router, the clock parameters are incorrect in certain scenarios when the Servo is in the **FREERUN** state. PR1548192
- The ACX5448 router as TWAMP server delays the start session acknowledgment by 10 seconds. PR1556829
- On the ACX5048 router, the ISSU upgrade fails due to the Packet Forwarding Engine restart issue . PR1554915

Open Issues

IN THIS SECTION

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

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

General Routing

- On the ACX5448 router, latency is observed for the host-generated ICMP traffic. PR1380145
- Tx power cannot be configured using the **+** sign. PR1383980
- The vpls-oam sessions are detected with error (RDI sent by some MEP) after changing VLANs. PR1478346
- In ZTP DHCP, option012 or option host-name does not work as expected. PR1503958
- On the ACX710 router, an alarm is not raised when booting the system using the recovery snapshot. PR1517221

- Even though enhanced-ip is active, the following alarm is observed during ISSU:

```
RE0 network-service mode mismatch between configuration and kernel setting.
```

  PR1546002

- In the Layer 3 VPN scenario, the CE device traffic drops on ingress PE device while resolving using default route in VRF. PR1551063

- On the ACX5448 router, you cannot downgrade to Junos OS Release 18.4 code-base. PR1556377

- On the ACX5048 routers, entry for MAC address from which no traffic is seen for MAC age timer does not age out if there is active traffic destined for this MAC address. PR1565642

- On the ACX5448 routers, the untagged traffic is being incorrectly queued and marked. PR1570899

- On the ACX5448 routers, single rate three color policer does not work. PR1559665

- On the ACX500 routers, service MIC does not work. PR1569103

- Packets might get tagged with the default VLAN-ID and dropped at the peer under Layer 2 circuits local switching scenario. PR1574623

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for ACX Series routers.

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

Resolved Issues: 21.1R1

IN THIS SECTION

Forwarding and Sampling

- VLAN-ID-based firewall match conditions might not work for the VPLS service. PR1542092

General Routing

- Memory utilization enhancement is needed. PR1481151
- The ACX1100, ACX2100, ACX2200, ACX2000, and ACX4000 routers might stop forwarding transit and control traffic. PR1508534
- On the ACX5448 routers, transit DHCP packets drop are observed. PR1517420
- On the ACX500-I router, the **show services session count** command does not work as expected. PR1520305
- PTP to 1PPS noise transfer test fails for frequency 1.985 Hz. PR1522666
- Interface does not come up with the auto-negotiation setting between the ACX1100 router and the other ACX Series routers, MX Series routers, and QFX Series switches as the other end. PR1523418
- On the ACX710 routers, PIR or CIR Hqos behaviour is inconsistent. PR1525789
- With the ACX5448 router with 1000 CFM, the CCM state does not go in the **Ok** state after loading the configuration or restarting the Packet Forwarding Engine. PR1526626
- The l2cpd process might leak memory with the aggregated Ethernet interface flap. PR1527853
- The FEC field is not displayed when the interface is down. PR1530755
- Unable to switch profile between G.8275.1 and G.8275.2. PR1533263
- Upon classifying the Layer 3 packets, DSCP is not preserved and is lost at the egress due to the limitations of a chipset. PR1535876

- The clksyncd process generates core file on Junos OS Release 20.3R1.3 image. PR1537107
- The rpd process generates a core file at **l2ckt_vc_adv_recv, l2ckt_adv_rt_flash (taskptr=0x4363b80, rtt=0x4418100, rtl=< optimized out>, data=< optimized out>, opcode=< optimized out>) at ../../../../../../../../../src/junos/usr.sbin/rpd/l2vpn/l2ckt.c:7982.** PR1537546
- Management Ethernet link down alarm is seen while verifying the system alarms in a Virtual Chassis setup. PR1538674
- On the ACX5448 router, the BGPV6LU traffic drop is observed when the node is deployed in ingress. PR1538819
- On the ACX5448 router, unexpected behavior of the **show chassis network-services** command is observed. PR1538869
- The following error message is observed while deleting the remote stream 0 0 0 0 0 0 along with feb core file at **0x00ae6484 in bcmdnx_queue_assert (queue=0xc599b60)** at **../../../../../src/pfe/common/drivers/bcmdnx/bcmdnx_sdk_ukern_layer.c**:

  ```
  Err] clksync_mimic_delete_clock_entry Unexpected error.
  ```

  PR1539953
- The announcement or synchronization interval rate range is not as expected. PR1542516
- Synchronization Ethernet goes in the **Holdover** state and comes back to the **Locked** state when the PTP configuration is deleted. PR1546681
- The ACX5448 router as transit for the BGP labeled unicast drops traffic. PR1547713
- IP addresses other than IPv4 and IPv6 must not be forwarded. PR1550748
- Multicast traffic is stopped when HQoS with multicast configurations is applied. PR1551248
- Verifying multiple PD synchronizations with relay deletes and adds configurations. PR1554647
- The ARP packets from the CE device are added with VLAN tag if the VLAN-ID is configured in the EVPN routing instance. PR1555679
- On the ACX710 router, the T-BC-P switch-over performance fails beyond the standard mask and servo moves to multiple **Holdover-in** state, **Acquiring** state, and **Holdover-out** state. PR1556087
- On the ACX5448 router, you cannot downgrade to Junos OS Release 18.4 code-base. PR1556377
- On the ACX5448 router, the unicast packets from the CE devices might be forwarded by the PE devices with an additional VLAN tag if IRB is used. PR1559084

- On the ACX5048 router, the fxpc process generates a core file on the analyzer configuration. PR1559690

- On the ACX2100 routers, laser-output-power is observed after the interface is disabled and then rebooted. PR1560501

- On the ACX5448 router, the following syslog message is reported every 30 seconds:

```
ACX_DFW_CFG_FAILED: ACX Error (dfw):dnx_dfw_dyn_entry_counter_get : Entry is
invalid. <url
```

  PR1562323

- Expected entries are not observed while verifying the physical logical interface status with the Layer 3 traffic. PR1572211

- The aggregated Ethernet interface might not come up with LFM configured after reboot. PR1526283

Layer 2 Features

- On the ACX5448 routers, VPLS traffic statistics are not displayed when the **show vpls statistics** command is executed. PR1506981

Documentation Updates

There are no errata and changes in Junos OS Release 21.1R1 for the ACX Series documentation.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

For information about software installation and upgrade, see the https://www.juniper.net/documentation/en_US/junos/information-products/pathway-pages/software-installation-and-upgrade/software-installation-and-upgrade.html Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19,4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.1.

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

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

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

Junos OS Release Notes for cRPD

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for the containerized routing protocol process (cRPD) container. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

What's New in 21.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for cRPD.

Platform and Infrastructure

- **Authentication, authorization, and accounting**—Starting in cRPD Release 21.1R1, you can configure local and remote authorizations on RADIUS and TACPLUS servers at the **[edit system services ssh]** hierarchy level. We support the following features:

- Local authentication and local authorization
- TACACS+ authentication, authorization and accounting
- User template support
- Support for operational commands and regular expressions
- Local authentication and remote authorization

[See password-options, tacplus, and radius (System).]

- **SRv6 network programming in IS-IS**—Starting in cRPD Release 21.1R1, you can configure to enable basic segment routing functionalities in a core IPv6 network for both route reflector role and host routing roles.

  You can enable SRv6 network programming in an IPv6 network at the **[edit source-packet-routing]** hierarchy level.

  > **NOTE**: The support for flavor (specifies end sid behavior) and flexible algorithm options is not available for configuring end sids.

  [See source-packet-routing].

- **Increase ECMP next-hop limit**—Starting in cRPD Release 21.1R1, you can specify the multipath next-hop limit at the **[edit routing-options maximum-ecmp]** hierarchy level. This helps to load-balance the traffic over multiple paths. The default ECMP next-hop limit is 16.

  [See routing-options-max-ecmp and Hash Field Selection for ECMP Load Balancing on Linux].

- **EVPN Type 5 with VXLAN** —Starting in cRPD Release 21.1R1, we support EVPN Type 5 Route over VXLAN for both IPv4 and IPv6 prefix advertisements.

  [See EVPN Type-5 Route with VXLAN encapsulation for EVPN-VXLAN].

- **Support for multiple KRT channels in SONiC**—cRPD in SONiC supports multiple Kernel Routing Table (KRT) channels to download route table information to forwarding table (FIB). The KRT channels supported are NetLink-based native Linux kernel FIB and FpmSyncd-based SONiC FIB.

  [See cRPD Multi-channel KRT Support in SONiC].

What's Changed

IN THIS SECTION

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

What's Changed in Release 21.1R1

IN THIS SECTION

Junos Telemetry Interface

- **Support for JTI over TLS similar to Junos OS (cRPD)**—cRPD supports local (server-side) certificate validation for gRPC and Junos Telemetry Interface (JTI) similar to Junos OS. cRPD doesn't support bidirectional authentication for gRPC and JTI.

  [See Configuring gRPC for the Junos Telemetry Interface and Importing SSL Certificates for Junos XML Protocol Support.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for cRPD.

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

General Routing

- Removing the FPMSYNCD FIB download channel under the routing-options forwarding table doesn't remove the active routes that are already downloaded from REDISDB on SONiC. PR1549365

Open Issues

There are no open issues for cRPD in Junos OS Release 21.1R1.

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

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for cRPD.

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

Resolved Issues: 21.1R1

There are no resolved issues for cSRX in Junos OS Release 21.1R1.

Junos OS Release Notes for cSRX

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for the cSRX Container Firewall, a containerized version of the SRX Series Services Gateway. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

What's New in 21.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for cSRX.

Authentication and Access Control

- **Configure client information to connect to the JIMS server (cSRX, SRX300, SRX340, SRX345, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting with Junos OS Release 21.1R1, you can configure which specifc interface, source IP address or routing instance SRX should use for connecting to a JIMS server.
  [See Configuring the Connection to an SRX Series Device.]

What's Changed

IN THIS SECTION

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

What's Changed in Release 21.1R1

There are no changes in behavior or syntax for cSRX in Junos OS Release 21.1R1.

Known Limitations

There are no known limitations for cSRX in Junos OS Release 21.1R1.

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

Open Issues

There are no open issues for cSRX in Junos OS Release 21.1R1.

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

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for cSRX.

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

Resolved Issues: 21.1R1

There are no resolved issues for cSRX in Junos OS Release 21.1R1.

Junos OS Release Notes for EX Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

What's New in 21.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for EX Series Switches.

Hardware

- **New EX4400 switch (EX Series)**—In Junos OS Release 21.1R1, we introduce the EX4400 switch, which provides connectivity for high-density environments and scalability for growing networks. The switch is available in the following models: EX4400-24T, EX4400-24P, EX4400-48T, EX4400-48P, and EX4400-48F.

  EX4400 switches support both manual and auto-channelization, but manual CLI channelization always takes precedence (see Port Settings).

  To install the EX4400 switch hardware and perform initial software configuration, routine maintenance, and troubleshooting, see EX4400 Switch Hardware Guide. See Feature Explorer for the complete list of features for any platform.

  Table 1: Feature Support on the EX4400

Feature	Description
Class of service	Support for CoS configuration with the following limitations: • If you apply strict-high priority schedulers to queues 0 through 3, then the strict-high priority schedulers are also applied to queues 8 through 11. Therefore, we recommend that you apply strict-high priority schedulers only to queues 4 through 7. • The EX4400 doesn't support the **excess-rate** configuration for schedulers. [See schedulers (CoS).]

Table 1: Feature Support on the EX4400 *(Continued)*

Feature	Description
EVPN	Support for Layer 2 VXLAN gateway services in an EVPN-VXLAN network: • 802.1X authentication, accounting, CWA authentication, and captive portal • CoS • DHCPv4 and DHCPv6 snooping, dynamc ARP inspection (DAI), neighbor discovery inspection, IP source guard and IPv6 source guard, and router advertisement (RA) guard (no multihoming) • Firewall filters and policing • Storm control, port mirroring, and MAC filtering [See EVPN Feature Guide.]
	Support for the following Layer 2 VXLAN gateway features in an EVPN-VXLAN network: • Active/active multihoming • Proxy ARP use and ARP suppression, and Neighbor Discovery Protocol (NDP) use and NDP suppression on non-IRB interfaces • Ingress node replication for broadcast, unknown unicast, and multicast (BUM) traffic forwarding [See EVPN Feature Guide.]

Table 1: Feature Support on the EX4400 *(Continued)*

Feature	Description
	Layer 3 VXLAN gateway in EVPN-VXLAN centrally routed bridging overlay or edge-routed bridging overlay networks, supported on standalone switches or Virtual Chassis and including the following features: • Default gateway using IRB interfaces to route traffic between VLANs. [See Using a Default Layer 3 Gateway to Route Traffic in an EVPN-VXLAN Overlay Network.] • IPv6 data traffic routed through an EVPN-VXLAN overlay network with an IPv4 underlay. [See Routing IPv6 Data Traffic through an EVPN-VXLAN Network with an IPv4 Underlay.] • EVPN pure Type 5 routes. [See Understanding EVPN Pure Type-5 Routes.] The Virtual Chassis doesn't support EVPN-VXLAN multihoming, but you can use the standalone switch as an EVPN-VXLAN provider edge device in multihoming use cases.
	Support for VXLAN Group Based Policy (VXLAN-GBP). EX4400 switches support the use of existing Layer 3 VXLAN network identifiers (VNI) in conjunction with firewall filter policies to provide microsegmentation at the device or tag level, independent of the underlying network topology. IoT devices, for example, typically only need access to specific applications on the network. GBP keeps this traffic isolated by automatically applying security policies without the need for L2 or L3 lookups, or access control lists (ACLs). [See Firewall Filter Match Conditions, Actions, and Action Modifiers for EX Series Switches.]
High availability (HA) and resiliency	High availability includes NSSU, GRES, NSB, and NSR. [See High Availability User Guide.]

Table 1: Feature Support on the EX4400 *(Continued)*

Feature	Description
Interfaces and chassis	EX4400-24T and EX4400-24P models have 24 RJ-45 ports and 2 QSFP28 ports. EX4400-48T and EX4400-48P models have 48 RJ-45 ports and 2 QSFP28 ports. The EX4400-48F model has 36 1GbE SFP ports, 12 10GbE SFP+ ports, and 2 100GbE QSFP28 ports. You can channelize the QSFP28 ports into four 25-Gbps or four 10-Gbps interfaces. [See Port Settings.]
	Support for the IEEE 802.3bt standard for Power over Ethernet (PoE) and fast PoE. With fast PoE enabled, the switch saves PoE power settings across a reboot and powers on the powered device (PD) at the initial stage of the boot (within a few seconds of switching on power) before the complete switch is booted. To configure fast PoE, use the command **set poe fast-poe**. [See Understanding PoE on EX Series Switches.]

Table 1: Feature Support on the EX4400 *(Continued)*

Feature	Description
Junos telemetry interface (JTI)	JTI Packet Forwarding Engine and Routing Engine sensor support. Use the Junos telemetry interface (JTI) and remote procedure calls (gRPC) to stream statistics from the switches to an outside collector. The following Routing Engine statistics are supported: • LACP state export • Chassis environmentals export • Network discovery chassis and components • LLDP export and LLDP model • BGP peer information (RPD) • RPD task memory utilization export • Network discovery ARP table state • Network discovery NDP table state The following Packet Forwarding Engine statistics are supported: • Congestion and latency monitoring • Logical interface • Filter • Physical interface • NPU/LC memory • Network discovery NDP table state To provision a sensor to export data through gRPC, use the **telemetrySubscribe** RPC to specify telemetry parameters. [See Configuring a Junos Telemetry Interface Sensor (CLI Procedure), Configure a NETCONF Proxy Telemetry Sensor in Junos, and Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface).]

Table 1: Feature Support on the EX4400 *(Continued)*

Feature	Description
Junos XML API and scripting	Support for Python, SLAX, and XSLT scripting languages and for commit scripts and macros, event policy and event scripts, op scripts, and SNMP scripts. [See Automation Scripting User Guide.]
Layer 2 features	Support for Ethernet ring protection switching version 2 (ERPSv2), which reliably achieves carrier-class network requirements for Ethernet topologies to form a closed loop. [See Example: Configuring Ethernet Ring Protection Switching on QFX Series and EX Series Switches Supporting ELS.]

Table 1: Feature Support on the EX4400 *(Continued)*

Feature	Description
Layer 2 unicast features	• Bridge protocol data unit (BPDU) protection • Ethernet ring protection switching (ERPS) • IEEE 802.1p • LAG resilient hashing • Layer 3 VLAN-tagged subinterfaces • LLDP (IEEE 802.1AB) • Loop protection • MAC address aging • MAC address filtering • Disable MAC learning • Multiple Spanning Tree Protocol (MSTP) (IEEE 802.1s) • Multiple VLAN Registration Protocol (MVRP) (IEEE 802.1ak) • Persistent MAC (sticky MAC) • Per VLAN MAC learning (limit) • Port-based VLAN • Proxy ARP • Redundant trunk group (RTG) • Root protection • Routed VLAN interface (RVI) • Rapid Spanning Tree Protocol (RSTP) (IEEE 802.1w) • Static and dynamic link aggregation with LACP (fast and slow LACP) • Static MAC address assignment for interface

Table 1: Feature Support on the EX4400 *(Continued)*

Feature	Description
	• Storm control • STP (IEEE 802.1D) • Uplink failure detection • VLAN • VLAN—IEEE 802.1Q VLAN trunking • VSTP [See Ethernet Switching User Guide, Security Services Administration Guide, and Spanning-Tree Protocols User Guide.]

Table 1: Feature Support on the EX4400 *(Continued)*

Feature	Description
Layer 3 unicast features	• 32-way equal-cost multipath (ECMP) • BFD (for RIP, OSPF, IS-IS, BGP, and PIM) • BGP 4-byte ASN support • BGP Add Path (BGP-AP) • Filter based forwarding (FBF) • IP directed broadcast traffic forwarding • IPv4 BGP • IPv4 multiprotocol BGP (MBGP) • IPv4 over GRE • IPv6 BGP • IPv6 CoS (BA, classification and rewrite, scheduling based on traffic class) • IPv6 IS-IS • IPv6 Neighbor Discovery Protocol (NDP) • IPv6 OSPFv3 • IPv6 ping • IPv6 stateless auto-configuration • IPv6 static routing • IPv6 traceroute • IS-IS • OSPFv2 • Path MTU discovery • RIPv2

Table 1: Feature Support on the EX4400 *(Continued)*

Feature	Description
	• Static routing • Unicast reverse path forwarding (unicast RPF) • Virtual router for IS-IS, RIP, OSPF, and BGP • Virtual Router Redundancy Protocol (VRRP) • VRRPv3 [See High Availability User Guide, BGP User Guide, Routing Policies, Firewall Filters, and Traffic Policers User Guide, IS-IS User Guide, Security Services Administration Guide, and OSPF User Guide.]
Licensing	You need a license to use the software features on the EX4400-24T, EX4400-24P, EX4400-48T, EX4400-48P, and EX4400-48F switches. To learn about the features supported on this device. [See EX Series Switches Support for the Juniper Flex Program.] [To add, delete, and manage licenses, see Managing Licenses.]
Multicast	• IGMP snooping • IGMP: version 1, version 2, version 3 • Multicast Listener Discovery (MLD) snooping • PIM-SM, PIM-SSM, PIM-DM [See Multicast Protocols User Guide.]
Network management and monitoring	Chef support for EX4400-48F. [See Chef for Junos OS Getting Started Guide.]

Table 1: Feature Support on the EX4400 *(Continued)*

Feature	Description
	EX4400 switches support the following Ethernet OAM link fault management (LFM) and connectivity fault management (CFM) features: • Monitor faults, using the continuity check messages (CCM) protocol to discover and maintain adjacencies at the VLAN or link level. • Discover paths and verify faults, using the Link Trace Message protocol (LTM protocol) to map the path taken to a destination MAC address. • Isolate faults, using loopback messages The EX4400 supports the following Ethernet switching events: • **adjacency loss** • **connection-protection-tlv** • **interface-status-tlv** • **port-status-tlv** EX Series switches support the **interface-down** action. [See Ethernet OAM and CFM for Switches and OAM Link Fault Management.]
	• Local and remote port mirroring, and remote port mirroring to an IP address (GRE encapsulation). [See Port Mirroring and Analyzers.] • sFlow network monitoring technology. [See sFlow Monitoring Technology.]
	Support for Puppet for Junos OS. [See Puppet for Junos OS Administration Guide.]
	Support for adding nonnative YANG modules to the Junos OS schema. [See Understanding the Management of Nonnative YANG Modules on Devices Running Junos OS.]

Table 1: Feature Support on the EX4400 *(Continued)*

Feature	Description
	Support for configuring the ephemeral database using the NETCONF and Junos XML protocols. [See Understanding the Ephemeral Configuration Database.]
	Support for Juniper Mist Wired Assurance. You can automatically onboard and provision Juniper Networks EX4400 switches to the Juniper Mist cloud using a single activation code. Juniper Mist Wired Assurance provides automated operations and enables the use of service-level expectations (SLEs) for IoT devices, Juniper access points driven by Mist AI, and other network devices. [For an overview of Juniper Mist Wired Assurance and deployment instructions, see Juniper AI-Driven Enterprise and Overview of EX Series Switches and the Juniper Mist Cloud.]
Routing policy and firewall filters	Firewall filters and policers. [See Firewall Filters Overview.]
Security	Support for distributed denial-of-service (DDoS) protection. [See Control Plane Distributed Denial-of-Service (DDoS) Protection Overview.]
	Support for the following port security features: • DHCP snooping (IPv4 and IPv6) • Dynamic ARP inspection (DAI) • IPv6 neighbor discovery inspection [See Security Services Administration Guide.]
	Support for Media Access Control security with 256-bit cipher suite. [See Understanding Media Access Control Security (MACsec).]

Table 1: Feature Support on the EX4400 *(Continued)*

Feature	Description
Services applications	Flow-based telemetry (FBT) enables per-flow-level analytics, using inline monitoring services to create flows and collect them. A flow is a sequence of packets that have the same source IP, destination IP, source port, destination port, or protocol on an interface. For each flow, various parameters are collected and sent to a collector using the open-standard IPFIX template to organize the flow. You configure FBT by configuring the **template** statement at the **[edit services inline-monitoring**] hierarchy level, and including the **flow-monitoring** option. [See Inline Monitoring Services Configuration and template (Inline Monitoring).]
Software installation and upgrade	Support for secure boot. The implementation is based on the UEFI 2.4 standard. [See Software Installation and Upgrade Guide.]
Virtual Chassis	Virtual Chassis support for up to ten EX4400 switches interconnected and managed as a single device. The Virtual Chassis also supports NSSU to upgrade all member devices with a single command. You configure and operate an EX4400 Virtual Chassis the same way as you do other EX Series and QFX Series Virtual Chassis. However, there are a few platform-specific VCP differences, including the following: • By default, the two rear-panel 100GbE QSFP28 ports operate as four logical 50-Gbps VCP interfaces to connect the member switches. You can’t use any other ports as VCPs. • These ports are in PIC slot 1, so the VCP ports on a switch are always named vcp-255/1/x, where x is a port number from 0 through 3. [See Virtual Chassis Overview for Switches.]

Authentication and Access Control

- **FQDN support in RADIUS configuration (EX2300, EX3400, EX4300, and EX4300-48P switches)**—Starting in Junos OS Release 21.1R1, RADIUS server configuration supports fully qualified domain names (FQDNs) that resolve to one or more IP addresses. This feature can be used in a cloud-managed architecture where the server name could translate to more than one IP address. RADIUS requests can be distributed across multiple servers without explicitly configuring each server IP address. Load distribution can be achieved by configuring the round-robin algorithm at the [**edit access profile profile-name radius options**] hierarchy level.

[See Specifying RADIUS Server Connections on Switches.]

EVPN

- **Tunnel endpoint in the PMSI tunnel attribute field for EVPN Type 3 routes (ACX5448, EX4600, EX4650, EX9200, and QFX10002)**—Starting in Junos OS Release 21.1R1, you can set the tunnel endpoint in the provider multicast service interface (PMSI) tunnel attribute field to use the ingress router's secondary loopback address. When you configure multiple loopback IP addresses on the local provider edge (PE) router and the primary router ID is not part of the MPLS network, the remote PE router cannot set up a PMSI tunnel route back to the ingress router.

  To configure the router to use a secondary IP address that is part of the MPLS network, include the **pmsi-tunnel-endpoint*pmsi-tunnel-endpoint*** statement at the **[edit routing-instances *routing-instance-name* protocols evpn]** hierarchy level for both EVPN and virtual-switch instance types.

  [See EVPN.]

- **Flow-aware transport pseudowire support for EVPN-VPWS (MX Series routers and EX9200 switches)**—Starting in Junos OS Release 21.1R1, you can statically configure provider edge (PE) devices to use flow-aware transport (FAT) pseudowire labels in an EVPN virtual private wire service (VPWS) routing instance with an IP/MPLS underlay fabric. PE devices use these labels to load-balance EVPN-MPLS packets across ECMP paths or link aggregation groups (LAGs) without needing to do deep packet inspection of the payload.

  To enable FAT pseudowire load balancing in an **evpn-vpws** routing instance:

  - Configure **flow-label-transmit-static** on PE devices to insert FAT flow labels into VPWS pseudowire packets sent to remote PE devices.

  - Configure **flow-label-receive-static** on PE devices to remove FAT flow labels from VPWS pseudowire packets received from remote PE devices.

  You can configure these statements for all pseudowires in the routing instance or for pseudowires associated with a specific interface in the routing instance.

  [See FAT Flow Labels in EVPN-VPWS Routing Instances, flow-label-receive-static, and flow-label-transmit-static.]

- **EVPN-VXLAN fabric (EX9200 switches with MPC10 and MPC11 line cards)**—Starting in Junos OS Release 21.1R1, EX9200 switches with MPC10 and MPC11 line cards support the following features in an EVPN-VXLAN fabric:

  - Layer 2 VXLAN

  - Multihoming in active/active mode, an Ethernet segment identifier (ESI) per interface, and preference-based designated forwarder (DF) election
  - MAC pinning, MAC move, MAC limiting, and MAC aging
  - QoS
  - DHCP and DHCP relay
  - Prevention of broadcast, unknown unicast, and multicast (BUM) traffic loops when a leaf device is multihomed to more than one spine device
- Layer 3 VXLAN
  - IRB interfaces
  - IPv6 over IRB interfaces
  - Support for OSPF, IS-IS, BGP, and static routing over IRB interfaces
  - Proxy ARP and ARP suppression, and proxy NDP and NDP suppression with and without IRB interfaces
  - IPv6 underlay
  - Virtual machine traffic optimization (VMTO) for ingress traffic
- Data Center Interconnect (DCI)
  - Pure EVPN Type 5 routes only
- High availability
  - Nonstop active routing (NSR)
  - GRES
  - Graceful restart from a routing process restart or Routing Engine switchover without NSR enabled
- Operations and management
  - Core isolation feature
  - Ping over EVPN Type 5 tunnel
- Static VXLAN
  - Overlay ping and traceroute

[See EVPN User Guide.]

- **Loop detection for EVPN-VXLAN fabrics (EX4300-48MP)**—Starting in Junos OS Release 21.1R1, you can configure loop detection on the server-facing Layer 2 interfaces on EX4300-48MP leaf devices in an EVPN-VXLAN fabric. This feature can detect the following types of Ethernet loops:

  - A loop between two interfaces with different Ethernet segment identifiers (ESIs), usually caused if you miswire fabric components.

  - A loop between two interfaces with the same ESI, usually caused if you miswire a third-party switch to the fabric.

  After you enable loop detection, the interfaces periodically send multicast loop-detection protocol data units (PDUs). If a loop detection-enabled interface receives a PDU, the device detects a loop, which triggers the configured action to break the loop. For example, if you configure the **interface-down** action, the device brings down the interface. After the **revert-interval** timer expires, the device reverts the action and brings the interface back up again.

  [See loop-detect.]

- **Explicit congestion notification (ECN) over VXLAN tunnels (EX4650 and QFX5120)**—Starting in Junos OS Release 21.1R1, by default, standalone EX4650 and QFX5120 switches support explicit congestion notification (ECN) for packets that are encapsulated across VXLAN tunnels, as follows:

  - During VXLAN encapsulation at the source virtual tunnel endpoint (VTEP), the switch copies the ECN bits of the Type-of-Service (ToS) field from the original packet IP header to the outer VXLAN encapsulation IP header.

  - During VXLAN de-encapsulation at the remote VTEP, the switch copies the ECN bits of the ToS field from the outer VXLAN encapsulation IP header to the original packet IP header.

  You can configure the **vxlan-disable-copy-tos-encap** statement or the **vxlan-disable-copy-tos-decap** statement at the **[set forwarding-options]** hierarchy on the encapsulation or de-encapsulation ends of the tunnel, respectively, to disable the ECN copy operation.

  > **NOTE**: These switches also copy the differentiated services code point (DSCP) bits in the ToS field of the IP header upon VXLAN encapsulation and de-encapsulation by default, and the same statements disable copying both the DSCP and ECN bits.

  [See vxlan-disable-copy-tos-encap and vxlan-disable-copy-tos-decap.]

Forwarding Options

- **Storm control support in EVPN-VXLAN overlay networks (EX4650 switches)**—Starting in Junos OS Release 21.1R1, EX4650 switches support storm control in an EVPN-VXLAN overlay network. Storm control enables the switch to monitor traffic levels and to drop broadcast, unknown unicast, and multicast (BUM) packets before they cause a traffic storm.

[See Understanding Storm Control.]

High Availability

- **Support for VRRP on EX9200-SF3 and EX9200-15C (EX9200)**—Starting in Junos OS Release 21.1R1, the EX9200-SF3 Switch Fabric module and the EX9200-15C line card support VRRP. All VRRP features are supported.

  [See Understanding VRRP.]

Licensing

- **Juniper Agile Licensing (EX2300, EX2300-MP, EX2300-C, EX3400, EX4300, EX4300-MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48P, and EX4400-48T)**—Starting in Junos OS Release 21.1R1, the listed EX Series switches support Juniper Agile Licensing.

  Juniper Agile Licensing provides simplified and centralized license administration and deployment. You can use Juniper Agile Licensing to install and manage licenses for hardware and software features.

  Juniper Agile Licensing supports soft enforcement and hard enforcement of hardware and software feature licenses.

  - With soft enforcement, if you configure a feature without a license, Junos OS displays a warning when you commit the configuration. However, the feature remains operational. In addition, Junos OS generates periodic alarms indicating that you need the license to use the feature. You can see the list of alarms at System Log Explorer.

  - With hard enforcement, if you configure a feature without a license, Junos OS displays a warning when you commit the configuration. The feature is not operational until the license is installed. In addition, Junos OS generates periodic alarms indicating that you need the license to use the feature. You can see the list of alarms at System Log Explorer.

  "Table 2" on page 46 describes the licensing support for soft-enforced features on EX2300 switches.

Table 2: Licensed Features on EX2300 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	• Layer 2 and Layer 3 filters • Layer 2 (*x*STP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operation, Administration, and Maintenance (OAM) link fault management (LFM) • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis*

Table 2: Licensed Features on EX2300 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • IPv6 routing protocols: Multicast Listener Discovery (MLD) version 1 and MLD version 2, OSPF version 3, PIM multicast, VRRP version 3 • Multicast Source Discovery protocol (MSDP) • OAM and Maintenance CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • VRRP

Virtual Chassis*—We've included Virtual Chassis license in the Standard license model on EX2300-C 12-port switches. However, we don't include the Virtual Chassis license on EX2300 24-port and 48-port switch models. You need to purchase the license separately.

"Table 3" on page 48 describes the licensing support for soft-enforced features on EX3400 switches.

Table 3: Licensed Features on EX3400 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	• Layer 2 and Layer 3 filters • Layer 2 (*x*STP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operations, Administration, and Maintenance (OAM) link fault management (LFM) • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis

Table 3: Licensed Features on EX3400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • IPv6 routing protocols: Multicast Listener Discovery (MLD) version 1 and MLD version 2, OSPF version 3, PIM multicast, VRRP version 3 • Multicast Source Discovery protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP

Table 3: Licensed Features on EX3400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Premium	Campus and access Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • IPv6 routing protocols: Multicast Listener Discovery (MLD) version 1 and MLD version 2, OSPF version 3, PIM multicast, VRRPv3, virtual router support for unicast and filter-based forwarding (FBF) • Multicast Source Discovery Protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP • BGP and multiprotocol BGP (MBGP) • IS-IS

"Table 4" on page 51 describes the licensing support for soft-enforced features on EX4300 switches.

Table 4: Licensed Features on EX4300 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	• Layer 2 and Layer 3 filters • Layer 2 (*x*STP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operations, Administration, and Maintenance (OAM) link fault management (LFM) • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis

Table 4: Licensed Features on EX4300 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP

Table 4: Licensed Features on EX4300 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List

Premium	Campus and access Layer 3	• Bidirectional Forwarding Detection (BFD)
		• CFM (IEEE 802.1ag)
		• IGMP version 1, IGMP version 2, and IGMP version 3
		• Multicast Source Discovery Protocol (MSDP)
		• OAM CFM
		• OSPF version 2 or OSPF version 3
		• Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode
		• Real-time performance monitoring (RPM)
		• RIP IPv6 (RIPng)
		• Unicast reverse-path forwarding (unicast RPF)
		• Virtual router
		• VRRP
		• BGP and multiprotocol BGP (MBGP)
		• IS-IS
		• EVPN-VXLAN
		    • Supported only on EX4300-48MP switch.
		    • Requires the BGP for configuration.

"Table 5" on page 54 describes the licensing support for soft-enforced features on EX4400 switches.

Table 5: Licensed Features on EX4400 switches

License Model	Use Case Examples or Solutions	Feature List
Standard	Campus and access Layer 2 or Layer 3	• Layer 2 and Layer 3 filters • Layer 2 (*x*STP, 802.1Q, and LAG) • Layer 2 and Layer 3 QoS • Layer 3 (static) • IGMP snooping • Operations, Administration, and Maintenance (OAM) link fault management (LFM) • sFlow • SNMP • Junos telemetry interface (JTI) • Virtual Chassis

Table 5: Licensed Features on EX4400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Advanced	Campus and access Layer 2 or Layer 3	• Bidirectional Forwarding Detection (BFD) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP

Table 5: Licensed Features on EX4400 switches *(Continued)*

License Model	Use Case Examples or Solutions	Feature List
Premium	Campus and access Layer 3	• Bidirectional Forwarding Detection (BFD) • CFM (IEEE 802.1ag) • IGMP version 1, IGMP version 2, and IGMP version 3 • Multicast Source Discovery Protocol (MSDP) • OAM CFM • OSPF version 2 or OSPF version 3 • Protocol Independent Multicast (PIM) dense mode, PIM source-specific mode, PIM sparse mode • Real-time performance monitoring (RPM) • RIP IPv6 (RIPng) • Unicast reverse-path forwarding (unicast RPF) • Virtual router • VRRP • BGP and multiprotocol BGP (MBGP) • IS-IS • EVPN-VXLAN • Requires the BGP for configuration.

On EX4400 switch, the flow-based telemetry and MACsec features are hard-enforced. You'll need a license to use these features.

[See Supported Features on EX2300, EX2300-MP, EX2300-C, EX3400, EX4300, EX4300-MP, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48P, and EX4400-48T devices, Juniper Agile Licensing Guide, and Configuring Licenses in Junos OS.]

Network Management and Monitoring

- **Ephemeral configuration database support for load update operations (EX4300-MP, EX9200, MX5, MX10, MX80, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 21.1R1, NETCONF and Junos XML protocol client applications can configure the ephemeral configuration database using a load update operation. To perform a load update operation, set the **<load-configuration> action** attribute to **update**.

  [See <load-configuration>.]

- **Operational command RPCs support returning JSON and XML output in minified format in NETCONF sessions (ACX1000, ACX1100, ACX2100, ACX4000, ACX5048, ACX5096, ACX5448, EX2300, EX2500, EX3400, EX4300, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48P, EX4400-48T, EX4600, EX4650, EX9200, MX104, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10001, PTX10002, PTX10008, PTX10016, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX10002, QFX10002-60C, QFX10008, QFX10016, SRX550, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, operational command RPCs, including the **<get-configuration>** RPC, support the **format="json-minified"** and **format="xml-minified"** attributes in NETCONF sessions to return JSON or XML output in minified format. Minified format removes any characters that are not required for computer processing—for example, unnecessary spaces, tabs, and newlines. Minified format decreases the size of the data, and as a result, can reduce transport costs as well as data delivery and processing times.

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

- **Remote port mirroring to IPv6 address (GRE encapsulation)(EX4650, EX4650-48Y-VC, QFX5120, QFX5120-32C, QFX511120-48T, QFX5120-48T-VC, QFX5120-48Y, and QFX5120-48YM)**—Starting in Junos OS Release 21.1R1, you can use remote port mirroring to copy packets entering a port or VLAN and sends the copies to the IPv6 address of a device running an analyzer application on a remote network (sometimes referred to as “extended port mirroring”). When you use remote port mirroring the mirrored packets are GRE-encapsulated.

  Add the address you would like to have the copied packets sent to in the CLI hierarchy. For example, **set forwarding-options analyzer ff output ipv6-address 2000::1**.

  [See Understanding Port Mirroring and Analyzers.]

Software Installation and Upgrade

- **Support for bootstrapping using HTTP proxy server in phone-home client (EX2300, EX2300-VC, EX3400, EX3400-VC, EX4400-24T, EX4400-48F, EX4400-48T, and EX4600)**—Starting in Junos OS Release 21.1R1, when the phone-home client (PHC) receives information regarding the HTTP proxy server through either DHCP option 43 suboption 8 or DHCP option 17 suboption 8, it creates an HTTPS transparent tunnel with the proxy server. After the tunnel is established, the PHC uses the tunnel as a proxy for the phone-home server or redirect server. The phone-home client downloads the software image and configuration file through the tunnel onto the device. When bootstrapping is complete, the device reboots and the tunnel quits.

  [See Obtaining Configurations and Software Image Without User Intervention Using Phone-Home Client.]

- **Support for DHCP option 43 suboption 8 to provide proxy server information in phone-home client (EX2300, EX2300-VC, EX3400, EX3400-VC, EX4400-24T, EX4400-48F, EX4400-48T, and EX4600)**—Starting in Junos OS Release 21.1R1, during the bootstrapping process, the phone-home client (PHC) can access the redirect server or the phone-home server through a proxy server. The DHCP server uses DHCP option 43 suboption 8 or DHCP option 17 suboption 8 to deliver the details of both IPv4 and IPv6 proxy servers to the PHC. The DHCP daemon running on the target switch learns about the proxy servers in the initial DHCP cycle and then populates either the phc_vendor_specific_info.xml files or the phc_v6_vendor-specific_info.xml files located in the **/var/etc/** directory with the vendor-specific information.

  [See Obtaining Configurations and Software Image Without User Intervention Using Phone-Home Client.]

- **Support for phone-home client (EX4400 Virtual Chassis)**—Starting in Junos OS Release 21.1R1, the phone-home client (PHC) can securely provision an EX4400 Virtual Chassis without requiring user interaction. You only need to:

  - Ensure that the Virtual Chassis members have the factory-default configuration.
  - Interconnect the member switches using dedicated or default-configured Virtual Chassis ports.
  - Connect the Virtual Chassis management port or any network port to the network.
  - Power on the Virtual Chassis members.

  The PHC automatically starts up on the Virtual Chassis and connects to the phone-home server (PHS). The PHS responds with bootstrapping information, including the Virtual Chassis topology, software image, and configuration. The PHC upgrades each Virtual Chassis member with the new image and applies the configuration, and the Virtual Chassis is ready to go.

  [See Provision a Virtual Chassis Using the Phone-Home Client.]

What's Changed

IN THIS SECTION

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

What's Changed in Release 21.1R1

General Routing

- **Support for unicast ARP request on table entry expiration**—You can configure the device to send a unicast ARP request instead of the default broadcast request when an ARP table entry is about to expire. The retry requests are unicast at intervals of 5 seconds. Without this option, the retry requests are broadcast at intervals of 800 milliseconds. This behavior reduces ARP overall broadcast traffic. It also supports the use case where access nodes are configured not to forward broadcast ARP requests toward customer CPEs for security reasons and instead translate ARP broadcasts to unicast requests. To confirm whether this is configured, you can issue the following command: **show configuration system arp | grep unicast-mode-on-expire**.

  [See arp..]

- **Change in license bandwidth command on vMX virtual routers**—Starting in Junos OS, to use the available license bandwidth, explicitly set the license bandwidth using the **set chassis license bandwidth in mbps** command.

  [See Configuring Licenses on vMX Virtual Routers.]

- **Configure internal IPsec authentication algorithm (EX Series)**—You can configure the algorithm **hmac-sha-256-128** at the **edit security ipsec internal security-association manual direction bidirectional authentication algorithm** hierarchy level for internal IP security (IPsec) authentication. In earlier releases, you could configure the algorithm **hmac-sha-256-128** for MX Series devices only.

Junos XML API and Scripting

- **The jcs:invoke() function supports suppression of root login and logout events in system log files for SLAX commit scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The **jcs:invoke()** extension function supports the **no-login-logout** parameter in SLAX commit scripts. If you include the parameter, the function does not generate and log UI_LOGIN_EVENT and

UI_LOGOUT_EVENT messages when the script logs in as root to execute the specified remote procedure call (RPC). If you omit the parameter, the function behaves as in earlier releases in which the root UI_LOGIN_EVENT and UI_LOGOUT_EVENT messages are included in system log files.

[See invoke() Function (SLAX and XSLT).]

- **The jcs:invoke() function supports suppression of root login and logout events in system log files for SLAX event scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The **jcs:invoke()** extension function supports the **no-login-logout** parameter in SLAX event scripts. If you include the parameter, the function does not generate and log UI_LOGIN_EVENT and UI_LOGOUT_EVENT messages when the script logs in as root to execute the specified remote procedure call (RPC). If you omit the parameter, the function behaves as in earlier releases in which the root UI_LOGIN_EVENT and UI_LOGOUT_EVENT messages are included in system log files.

  [See invoke() Function (SLAX and XSLT).]

- **Python 2.7 deprecation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, devices running Junos OS no longer support Python 2.7. We've deprecated the corresponding **language python** statement at the **[edit system scripts]** hierarchy level. To execute Python scripts, configure the **language python3** statement at the **[edit system scripts]** hierarchy level to execute the scripts using Python 3.

  [See Understanding Python Automation Scripts for Devices Running Junos OS.]

Layer 2 Ethernet Services

- **Modification to sync-reset command (All JUNOS and EVO platforms)**—Starting from this release, the sync-reset command is disabled by default on all Junos and EVO platforms. Sync-reset command enables the device to send the sync bit in the LACP packets on minimum-link failure. Previously the sync-reset command was enabled by default on QFX and EX series, while it was by default disabled on MX, PTX and ACX series.

  [See sync-reset.]

Network Management and Monitoring

- **Support for disconnecting unresponsive NETCONF-over-SSH clients (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—You can enable devices to automatically disconnect unresponsive NETCONF-over-SSH clients by configuring the **client-alive-interval** and **client-alive-count-max** statements at the **[edit system services netconf ssh]** hierarchy level. The **client-alive-interval** statement specifies the timeout interval in seconds, after which, if no data has been received from the client, the device requests a response. The **client-alive-count-max** statement specifies the threshold of missed client-alive responses that triggers the device to disconnect the client, thereby terminating the NETCONF session.

[See ssh (NETCONF).]

- **Support for specifying the YANG modules to advertise in the NETCONF capabilities and supported schema list (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—You can configure devices to emit third-party, standard, and Junos OS native YANG modules in the capabilities exchange of a NETCONF session by configuring the appropriate statements at the **[edit system services netconf hello-message yang-module-capabilities]** hierarchy level. In addition, you can specify the YANG schemas that the NETCONF server should include in its list of supported schemas by configuring the appropriate statements at the **[edit system services netconf netconf-monitoring netconf-state-schemas]** hierarchy level.

  [See hello-message and netconf-monitoring.]

User Interface and Configuration

- **Verbose format option to export JSON configuration data (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The Junos OS CLI exposes the **verbose** statement at the **[edit system export-format json]** hierarchy level. We changed the default format to export configuration data in JavaScript Object Notation (JSON) from **verbose** to **ietf** starting in Junos OS Release 16.1R1. You can explicitly specify the default export format for JSON configuration data by configuring the appropriate statement at the **[edit system export-format json]** hierarchy level. Although the **verbose** statement is exposed in the Junos OS CLI as of the current release, you can configure this statement starting in Junos OS Release 16.1R1.

  [See export-format.]

Known Limitations

Learn about known limitations in this release for EX Series switches.

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

EVPN

- After a reboot during recovery process, the ESI LAGs come up before the BGP sessions, and routes or ARP entries are not synchronized. PR1487112

General Routing

- On all platforms running Junos OS or Junos OS Evolved, in a Q-in-Q environment, if xSTP is enabled on an interface that has a logical interface with vlan-id-list configured, then, it will only run on those logical interfaces whose vlan-id range includes native-vlan-id configured. All other xSTP will be in discarding state. This might lead to traffic drop. PR1532992

- Tail drop is seen in WRED configuration statistics. PR1549910

Interfaces and Chassis

- **Support for low power idle mode (EX4400-48T, EX4400-48P, EX4400-24T, and EX4400-24P)**—Starting in Junos OS Release 21.1R1, the 1-Gbps or 100-Mpbs port switches to low power idle (LPI) mode based on the following conditions:.

  - When a port operates at 1-Gbps speed and no traffic is either received or transmitted, then the port enters LPI mode. If the 1-Gbps port transfers unidirectional or bidirectional traffic, then the port will not enter LPI mode.

  - When a port operates at 100-Mbps speed, the port switches to LPI mode, based on the direction of the traffic. The **show interfaces interface-name extensive** command displays **RX LPI** when there is no RX traffic and **TX LPI** when there is no TX traffic.

  You can view the interface that is in LPI mode by executing the **show interfaces interface-name extensive** command. The output field **IEEE 802.3az Energy Efficient Ethernet** displays the status of the LPI mode.

  [See show interfaces extensive .]

User Interface and Configuration

- Unsupported options can be seen under "restart" command. PR1545558

- Python script is not supported in ZTP workflow. Python can run (during ZTP) only in few QFX Series based flex images. PR1547557

Open Issues

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

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

General Routing

- On the EX9214 device, if the MACsec-enabled link flaps after reboot, the error "errorlib_set_error_log(): err_id(-1718026239)" is observed. PR1448368

- A delay of 35 seconds is added in reboot time in Junos OS Release 20.2R1 compared to Junos OS Release 19.4R2. PR1514364

- Traffic does not get load balanced by EX4300-VC platforms over ESI links with EVPN_VXLAN configured. PR1550305

- "Resource deadlock avoided" messages are observed during software add on EX4400. No functionality impact seen. PR1557468

- When dot1x server-fail-voip vlan-name is configured, ensure that both server-fail-voip vlan-name and voip vlan are configured using vlan-name and not by using vlan-id. PR1561323

- RPD core file is generated when the device reboots and daemon restarts. Daemon recovers and there is no service impact on routing protocol usage. PR1567043

- When a MACsec session is down and the physical interface is up, traffic might continue to pass over the interface unencrypted. PR1569650

Infrastructure

- On EX Series switches, If you are configuring a large-scale number of firewall filters on some interfaces, the FPC might crash and generate core files. PR1434927

- "IFDE: Null uint32 set vector, ifd and IFFPC: 'IFD Ether uint32 set' (opcode 151) error message is observed continuously in AD with base configurations. PR1485038

Layer 2 Features

- The memory leak might happen due to eswd daemon on EX Series platforms. A message like the following is displayed in the system log: eswd[1330]: JTASK_OS_MEMHIGH: Using 212353 KB of memory, 158 percent of available /kernel: KERNEL_MEMORY_CRITICAL: System low on free memory, notifying init (#2). /kernel: Process (1254,eswd) has exceeded 85% of RLIMIT_DATA: used 114700 KB Max 131072 KB. PR1262563

Platform and Infrastructure

- Upgrading satellite devices might lead to some SDs in SyncWait state. Cascade port flap is not causing the issue. PR1556850

- On all EX9200 line of switches with EVPN-VXLAN configured, the next-hop memory leak in Trio ASIC happens whenever there is a route churn for remote MAC-IP entries learned bound to the IRB interface in EVPN-VXLAN routing-instance. When the ASIC's NH memory partition exhausted the FPC might reboot. PR1571439

Routing Policy and Firewall Filters

- On all Junos OS platforms with "set policy-options rtf-prefix-list" configured, if you upgrade to a specific version, the device might fail to validate its configuration, which eventually causes the rpd to crash unexpectedly due to a software fault. PR1538172

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 21.1R1

General Routing

- While verifying the Last-change op-state value through XML, the rpc-reply message is inappropriate. PR1492449
- The mge interface might still stay up while the far end of the link goes down. PR1502467
- SNMP POE MIB walk produces either no results or sometimes results from the master Virtual Chassis whenever one of the Virtual Chassis is renamed. PR1503985
- The DHCP traffic might not be forwarded correctly when DHCP sends unicast packets. PR1512175
- Traffic loss might be observed on interfaces in a VXLAN environment. PR1524955
- On the EX2300, the following PoE message is observed: poe_get_dev_class: Failed to get PD class info. PR1536408
- EX4300-48MP : sFlow: dcpfe core file is generated when you use the **request chassis fpc slot slot_num restart** command. PR1536997

- On EX4300 platforms, the LLDP neighborship with the Voice over Internet Protocol (VoIP) phones cannot be established when LLDP is configured on the Power over Ethernet (PoE) enabled port on EX4300 and connects to the VoIP phone. PR1538482
- On the EX3400 and EX2300 switches, the upgrade fails due to the lack of available storage. PR1539293
- DHCP discover packet might be dropped if DHCP inform packet is received first. PR1542400
- The Slaac-Snoopd child process generates a core file upon multiple switchovers on the Routing Engine. PR1543181
- In every software upgrade, host needs to get upgraded. PR1543890
- [Supportability] Improve Junos CLI outputs to display the host OS and kernel version in an easier and human-readable way. This enhancement is needed for all VMhost and Linux platforms. PR1543901
- The chip FPC might crash during the system booting. PR1545455
- **show system software rollback** is not supported on EX4400-48F. PR1546605
- **show pfe route summary hw** shows random high free and 'Used' column for 'IPv6 LPM(< 64)' routes. PR1552623
- The configuration statement **action-shutdown** of storm control does not work for ARP broadcast packets. PR1552815
- On the EX9200 device, SF3 Fabric OIR issues is observed with Junos OS Release 23.1R1.8. PR1555727
- Traffic might be dropped when a firewall filter rule uses the then VLAN action. PR1556198
- On the EX4300 device, script fails while committing the IPsec authentication configuration as the algorithm statement is missing. PR1557216
- Observing error Opening configuration database: Could not open configuration database during usb upgrading. PR1561741
- The client authentication fails after GRES. PR1563431
- QinQ should not be licensed on EX2300, EX3400, EX4300, EX4300MP, and EX4400. PR1573179

Infrastructure

- On the EX4600 and EX4300 Virtual Chassis or Virtual Chassis Fabric, the VSTP configurations device goes unreachable and becomes nonresponsive after commit. PR1520351

- Error message during USB install: g_vfs_done():da0p1[READ(offset=65536, length=8192)]error = 5. PR1544736
- EX4300 Virtual Chassis or Virtual Chassis Fabric: Observing HEAP malloc(0) detected. PR1546036
- Traffic related to IRB interface might be dropped when mac-persistence-timer expires. PR1557229

Platform and Infrastructure

- DHCP binding does not happen after GRES. PR1515234
- lldp-receive-packet-count is not getting exchanged properly in l2pt operation for LLDP after configuring protocols. PR1532721
- On the EX4300 device, the LLDP neighborship might not come up with the non-aggregated Ethernet interfaces. PR1538401
- The targeted-broadcast feature might not work after a reboot. PR1548858
- The BGP session replication might fail to start after the session crashes on the backup Routing Engine. PR1552603
- The targeted-broadcast feature might send out duplicate packets. PR1553070

Routing Protocols

- The OSPF neighborship gets stuck in the Start state after configuring the EVPN-VXLAN. PR1519244
- The OSPFv3 adjacency is not be established when IPsec authentication is enabled. PR1525870
- DCPFE crash might be observed while updating VRF for multicast routes during irb uninit. PR1546745
- The untagged packets might not work on QFX5000 platforms. PR1568533

User Interface and Configuration

- Removing the Flash component from the Monitor > Interfaces and DHCP pages removes other flash pages. PR1553176
- J-Web application package cannot be automatically updated for all the supported EX Series devices PR1563588

Migration, Upgrade, and Downgrade Instructions

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19,4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.1.

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

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

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

Junos OS Release Notes for JRR Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for the JRR Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

What's New in 21.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for JRR Series Route Reflectors.

Routing Protocols

- **Support for SR-IOV virtualization (JRR200)**—Starting in Junos OS Release 21.1R1, the JRR200 route reflector uses single-root I/O virtualization (SR-IOV) instead of full virtualization (emulated I/O) for network ports. SR-IOV helps to maximize the I/O throughput on the 10GbE SFP+ ports.

  SR-IOV improves:

  - BGP convergence in a scaled environment.
  - Throughput performance for BGP RIB sharding.

  [See BGP sharding overview, rib-sharding, and update-threading.]

What's Changed

IN THIS SECTION

Learn about what changed in Junos OS main and maintenance releases for JRR Series Route Reflectors.

What's Changed in Release 21.1R1

There are no changes in behavior and syntax in Junos OS Release 21.1R1 for JRR Series Route Reflectors.

Known Limitations

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 21.1R1 for JRR Series Route Reflectors.

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

Open Issues

There are no open issues in Junos OS 21.1R1 Release for JRR Series Route Reflectors.

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

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 21.1R1

IN THIS SECTION

General Routing

- The **request system power-off** and **request system halt** commands do not work as expected on JRR200. PR1534795
- Optics information of physical interfaces is not available for JRR200 on Junos OS. PR1537261

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

For information about software installation and upgrade, see the JRR200 Route Reflector Quick Start and Installation and Upgrade Guide.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19,4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.1.

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

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

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

Junos OS Release Notes for Juniper Secure Connect

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for Juniper Secure Connect. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for Juniper Secure Connect.

What's New in 21.1R1

There are no new features for Juniper Secure Connect in Junos OS Release 21.1R1.

What's Changed

IN THIS SECTION

Learn about what changed in Junos OS main and maintenance releases for Juniper Secure Connect.

What's Changed in Release 21.1R1

There are no changes in behavior or syntax for Juniper Secure Connect in Junos OS Release 21.1R1.

Known Limitations

There are no known limitations for Juniper Secure Connect in Junos OS Release 21.1R1.

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

Open Issues

There are no open issues for Juniper Secure Connect in Junos OS Release 21.1R1.

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

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for Juniper Secure Connect.

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

Resolved Issues: 21.1R1

There are no resolved issues for Juniper Secure Connect in Junos OS Release 21.1R1.

Junos OS Release Notes for Junos Fusion for Enterprise

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for the Junos Fusion for enterprise. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for Junos fusion for enterprise.

What's New in 21.1R1

There are no new features or enhancements to existing features in Junos OS Release 21.1R1 for Junos fusion for enterprise.

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for Junos Fusion for enterprise.

What’s Changed in Release 21.1R1

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 21.1R1 for Junos fusion for enterprise.

Known Limitations

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 21.1R1 for Junos fusion for enterprise.

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

Open Issues

There are no known issues in hardware and software in Junos OS Release for 21.1R1 Junos fusion for enterprise.

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

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for Junos Fusion for enterprise.

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

Resolved Issues: 21.1R1

There are no resolved issues in Junos OS Release 21.1R1 for documentation for Junos fusion for enterprise.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Basic Procedure for Upgrading Junos OS on an Aggregation Device

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

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

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

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

To download and install Junos OS:

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

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

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

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

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

5. Select the **Software** tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

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

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

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

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

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

    ```
    user@host> request system software add validate reboot source/package-name.n-limited.tgz
    ```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

Preparing the Switch for Satellite Device Conversion

There are multiple methods to upgrade or downgrade satellite software in your Junos fusion for enterprise. See Configuring or Expanding a Junos fusion for enterprise.

For satellite device hardware and software requirements, see Understanding Junos fusion for enterprise Software and Hardware Requirements.

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

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

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

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

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

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

2. Clear the device:

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Switch

If you need to convert a satellite device to a standalone device, you must install a new Junos OS software package on the satellite device and remove it from the Junos fusion topology. For more information, see Converting a Satellite Device to a Standalone Device.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

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

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

Downgrading Junos OS

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

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

To downgrade a Junos fusion for enterprise, follow the procedure for upgrading, but replace the **junos-install** package with one that corresponds to the appropriate release.

Junos OS Release Notes for Junos Fusion for Provider Edge

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for Junos Fusion for provider edge. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

Learn about new features introduced in the Junos OS main and maintenance releases for Junos Fusion for Enterprise.

What's New in 21.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for Junos Fusion for Provider Edge.

EVPN

- **Support for EVPN-MPLS (Junos fusion for provider edge)**—Starting in Junos OS Release 21.1R1, Junos fusion for provider edge supports EVPN-MPLS. EVPN-MPLS is a solution that extends Layer 2 VPN services over an MPLS network. Junos fusion for provider edge supports the connection of a customer edge (CE) device on the extended port of the satellite device in an EVPN-MPLS network.

  [See Junos Fusion Provider Edge Supported Protocols.]

VPNs

- **Support for BGP MVPN (Junos fusion for provider edge)**—Starting in Junos OS Release 21.1R1, Junos fusion for provider edge supports BGP multicast VPN (MVPN). BGP MVPN is a method for implementing multiprotocol multicast services over a BGP MPLS Layer 3 VPN. Junos fusion for provider edge supports the connection of a BGP-based MVPN customer edge (CE) device on the extended ports of the satellite device in Junos fusion for provider edge.

  [See Junos Fusion Provider Edge Supported Protocols.]

- **Support for interprovider and carrier-of-carrier VPNs (Junos fusion for provider edge)**—Starting in Junos OS Release 21.1R1, Junos fusion for provider edge supports Interprovider and Carrier-of-Carrier VPNs. The Carrier-of-Carrier VPN service describes a hierarchical VPN (also known as a recursive VPN) model where one carrier (VPN service customer) transports its VPN traffic inside another carrier's VPN (VPN service provider). Junos fusion for provider edge currently supports provider edge (PE) routers for VPN service customers. In Junos OS Release 21.1R1, we introduce support for PE routers for VPN service providers along with VPN service customers.

  Interprovider VPNs provide connectivity between different service providers that are using separate autonomous systems (ASs) or one service provider that is using different ASs for different geographic locations. For Interprovider VPNs, Junos fusion for provider edge supports only intra-AS connection on an AS boundary router (ASBR) to the extended port.

  [See Junos Fusion Provider Edge Supported Protocols.]

What's Changed

IN THIS SECTION

Learn about what changed in the Junos OS main and maintenance releases for Junos Fusion for provider edge.

What's Changed in Release 21.1R1

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

Known Limitations

There are no known behaviors, system maximums, and limitations in hardware and software in Junos OS Release 21.1R1 for Junos fusion for provider edge.

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

Open Issues

There are no open issues in the Junos OS Release 21.1R1 for Junos fusion for provider edge.

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

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for Junos fusion for provider edge.

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

Resolved Issues: 21.1R1

There are no fixed issues in the Junos OS Release 21.1R1 for Junos fusion for provider edge.

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for Junos fusion for provider edge. Upgrading or downgrading Junos OS might take several hours, depending on the size and configuration of the network.

Basic Procedure for Upgrading an Aggregation Device

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

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

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

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

The download and installation process for Junos OS Release 21.1R1 is different from that for earlier Junos OS releases.

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

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

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

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

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

5. Select the **Software** tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

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

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

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

    - For 64-bit software:

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

```
user@host> request system software add validate reboot source/jinstall64-21.1R1.SPIN-domestic-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.1R1.SPIN-domestic-signed.tgz
```

All other customers, use the following commands.

- For 64-bit software:

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

```
user@host> request system software add validate reboot source/jinstall64-21.1R1.SPIN-export-signed.tgz
```

- For 32-bit software:

```
user@host> request system software add validate reboot source/jinstall-21.1R1.SPIN-export-signed.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 21.1R1 **jinstall** package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

Upgrading an Aggregation Device with Redundant Routing Engines

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

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine and save the configuration change to both Routing Engines.

2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.

3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.

4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

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

Preparing the Switch for Satellite Device Conversion

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

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

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

Customers with EX4300 switches, use the following command:

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

Customers with QFX5100 switches, use the following command:

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

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

1. Log in to the device by using the console port.
2. Clear the device:

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

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

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

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

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

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

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

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

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

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

Converting a Satellite Device to a Standalone Device

If you need to convert a satellite device to a standalone device, you must install a new Junos OS software package on the satellite device and remove the satellite device from the Junos fusion topology.

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

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

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

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

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

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

4. Select the Junos OS Release 14.1X53-D30 software image for your platform.

5. Review and accept the End User License Agreement.

6. Download the software to a local host.

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

8. Remove the satellite device from the automatic satellite conversion configuration.

   If automatic satellite conversion is enabled for the satellite device's member number, remove the member number from the automatic satellite conversion configuration. The satellite device's member number is the same as the FPC slot ID.

   ```
   [edit]
   user@aggregation-device# delete chassis satellite-management auto-satellite-conversion
   satellite member-number
   ```

   For example, to remove member number 101 from Junos fusion:

   ```
   [edit]
   user@aggregation-device# delete chassis satellite-management auto-satellite-conversion
   satellite 101
   ```

   You can check the automatic satellite conversion configuration by entering the **show** command at the **[edit chassis satellite-management auto-satellite-conversion]** hierarchy level.

9. Commit the configuration.

   To commit the configuration to both Routing Engines:

   ```
   [edit]
   user@aggregation-device# commit synchronize
   ```

Otherwise, commit the configuration to a single Routing Engine:

```
[edit]
user@aggregation-device# commit
```

10. Install the Junos OS software on the satellite device to convert the device to a standalone device.

```
[edit]
user@aggregation-device> request chassis satellite install URL-to-software-package fpc-slot
member-number
```

For example, to install a PXE software package stored in the **/var/tmp** directory on the aggregation device onto a QFX5100 switch acting as the satellite device using FPC slot 101:

```
[edit]
user@aggregation-device> request chassis satellite install /var/tmp/install-media-pxe-
qfx-5-14.1X53-D43.3-signed.tgz fpc-slot 101
```

For example, to install a software package stored in the **var/tmp** directory on the aggregation device onto an EX4300 switch acting as the satellite device using FPC slot 101:

```
[edit]
user@aggregation-device> request chassis satellite install /var/tmp/jinstall-ex-4300-14.1X53-
D30.3-domestic-signed.tgz fpc-slot 101
```

The satellite device stops participating in the Junos fusion topology after the software installation starts. The software upgrade starts after this command is entered.

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

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

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

Upgrading an Aggregation Device

When you upgrade an aggregation device to Junos OS Release 21.1R1, you must also upgrade your satellite device to Satellite Device Software version 3.1R1.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

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

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

Downgrading from Junos OS Release 21.1

To downgrade from Release 21.1 to another supported release, follow the procedure for upgrading, but replace the 21.1 **jinstall** package with one that corresponds to the appropriate release.

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

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for MX Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for the MX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

What's New in 21.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for the MX Series routers.

Hardware

- We've added the following features to the MPC10E (MPC10E-15C-MRATE and MPC10E-10C-MRATE) and MPC11E (MX2K-MPC11E) in Junos OS Release 21.1.

Table 6: Feature Support on MPC10E and MPC11E on MX Series Routers

Feature	Description
EVPN	• Configure inner source MAC address for flexible VXLAN tunnels—Use the Juniper Extension Toolkit (JET) RIB Service API to configure the source MAC address used in IPv4 and IPv6 flexible VXLAN tunnel encapsulation profiles. If you don't specify a source MAC address, the default source MAC address 00:00:5e:00:52:01 is used to encapsulate IPv4 and IPv6 flexible VXLAN tunnels. [See Understanding Programmable Flexible VXLAN Tunnels and Juniper Extension Toolkit (JET).] • Support for auto-derived route targets on EVPN-MPLS.Junos OS supports the automatic derivation of route targets on EVPN-MPLS in an MPC10E line card on an MX Series router. When you enable the auto-derived route target feature, route targets are automatically derived from the VLAN ID for EVPN Type 2 and EVPN Type 3 routes and can be imported to the EVPN routing instance table. To enable the auto-derived route targets option, include the **auto** statement at the [**edit routing-instances routing-instance-name protocols evpn vrf-target**] hierarchy level. [See Auto-derived Route targets.] • Support for IPv4 unicast VXLAN encapsulation optimization on MPC10E and MPC11E line cards running on MX240, MX480, MX960, MX2008, MX2010, and MX2020 routers. By default, these routers optimize VXLAN-encapsulated throughput for IPv4 unicast packets that are 512 through 1500 bytes in size over the following VXLAN tunnel types: • PIM-based VXLAN • EVPN-VXLAN • Static VXLAN

Table 6: Feature Support on MPC10E and MPC11E on MX Series Routers *(Continued)*

Feature	Description
	This feature doesn’t provide additional optimization over EVPN Type 5 tunnels (which are already optimized), and is not supported with forwarding table filters. [See Understanding VXLANs.]
Hardware	• Support for QDD-400G-LR4-10, QDD-4x100G-LR, and QSFP-100G-LR transceivers (MX240, MX480, and MX960 with MPC10E line cards). [See Hardware Compatibility Tool.]
High availability (HA) andresiliency	• MX Series Virtual Chassis (MX-VC) support for MPC10E-10C-MRATE and MPC10E-15C-MRATE (MX240, MX480, and MX960)— You can operate the MPC10E-10C-MRATE and MPC10E-15C-MRATE line cards in a router in an MX Series Virtual Chassis. The MPC10E support in MX-VC is only for uplink usage. [See Virtual Chassis Components Overview.]
Juniper Extension Toolkit (JET)	• Support for static backup paths with IP-in-IP tunnel encapsulation and provisioning APIs (MX240, MX480, MX960, MX2010 and MX2020)—We've enhanced Juniper Extension Toolkit (JET) APIs to enable a controller to set up underlay network backup paths that use IP-in-IP tunnels with IPv4 encapsulation. [See Juniper Extension Toolkit (JET).]

Table 6: Feature Support on MPC10E and MPC11E on MX Series Routers *(Continued)*

<table>
<tr><th>Feature</th><th>Description</th></tr>
<tr><td>Layer 2 features</td><td>

- Support for MAC statistics (MX-Series)— You can enable MAC statistics for Layer 2 traffic on MPC10E-15C-MRATE, MPC10E-10C-MRATE, and MX2K-MPC11E MPC line cards.

  To enable MAC statistics at the bridge domain, include the **mac-statistics** configuration statement at the [**edit bridge-domains <bridge-domain name> bridge-options**] hierarchy level.

  To enable MAC statistics at the global level, you need to include the **global-mac-statistics** configuration statement at the [**edit protocols l2-learning**] hierarchy level.

  [See mac-statistics and global-mac-statistics.]

- Support for Multiple VLAN Registration Protocol (MVRP) and Ethernet ring protection switching (ERPS).

  [See Understanding Multiple VLAN Registration Protocol (MVRP) for Dynamic VLAN Registration and Ethernet Ring Protection Switching Overview.]

</td></tr>
<tr><td>Port security</td><td>

- Support for Media Access Control Security (MACsec) on logical interfaces (MPC10E and MPC11E). VLAN tags are transmitted in clear text, which allows intermediate switches that are MACsec-unaware to switch the packets based on the VLAN tags.

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

</td></tr>
</table>

Table 6: Feature Support on MPC10E and MPC11E on MX Series Routers *(Continued)*

Feature	Description

Services applications	• Support for Mapping of Address and Port with Encapsulation (MAP-E) and inline 6rd (MPC10E and MX2K-MPC11E)— You can configure MAP-E and inline IPv6 rapid deployment (inline 6rd) on the following MPCs:
	  ◦ MPC10E-15C-MRATE and MPC10E-10C-MRATE on MX240, MX480, and MX960 routers
	  ◦ MX2K-MPC11E on MX2010 and MX2020 routers
	[See Configuring Mapping of Address and Port with Encapsulation (MAP-E) and Configuring Inline 6rd.]
	• Support for tunnel interfaces on the MPC10E line card—Junos OS supports three tunnel interfaces on the MPC10E line card: generic routing encapsulation (GRE) tunnel, logical tunnel (LT), and virtual tunnel (VT).
	  ◦ The GRE tunnel interface supports the **tunnel** statement with these options: **destination**, **key**, **source**, **traffic-class** and **ttl**. The **copy-tos-to-outer-ip-header** statement is also supported.
	  ◦ The LT interface supports the family **inet**, **inet6**, and **iso** options. The **encapsulation** statement supports the Ethernet and VLAN physical interface options only.
	  ◦ The VT interface supports the family **inet** option only.
	[See Tunnel Services Overview].
	• AMS support (MX240, MX480, MX960, MX2010, and MX2020 routers)—Junos OS supports aggregated multiservices (AMS) interfaces on the MPC10E and MX2K-MPC11E line cards to provide load balancing and high availability features for stateful firewall and NAT services. You can configure AMS interfaces with next-hop style service sets and with MS-MPC or MS-MIC only.
	[See Understanding Aggregated Multiservices Interfaces.]

Table 6: Feature Support on MPC10E and MPC11E on MX Series Routers *(Continued)*

Feature	Description
System management	• Support for Synchronous Ethernet over link aggregation group interfaces (MX240, MX480, and MX960)—MPC10E line cards support Synchronous Ethernet over a link aggregation group (LAG). [See Synchronous Ethernet Overview.] • Support for PTP over Ethernet, hybrid mode, and G.8275.1 profile (MX240, MX480, and MX960)—MPC10E line cards support Precision Time Protocol (PTP) over Ethernet, G.8275.1 profile, and hybrid mode. [See Precison Time Protocol Overview and Understanding Hybrid Mode.] • Support for PTP over Ethernet and hybrid mode over link aggregation group interfaces (MX240, MX480, and MX960)—MPC10E line cards support Precision Time Protocol (PTP) over Ethernet and hybrid mode over a link aggregation group (LAG). [See Understanding Hybrid Mode and Precison Time Protocol Overview.]

Dynamic Host Configuration Protocol

- **Include DHCP option 61 in Radius Access Request (MX240, MX480, and MX960 routers)**—Starting in Junos OS Release 21.1R1, you can configure DHCP to use the client identifier (DHCP Option 61) in the username that is passed to the external AAA authentication service when the DHCP client logs in. You can also configure options to exclude headers and to use automatic ASCII hex encoding to obtain the preferred string for authentication. This feature is supported for DHCP server and relay in DHCPv4, DHCPv6, and dual stack.

  [See Creating Unique Usernames for DHCP Clients.]

EVPN

- **Flow-aware transport pseudowire support for EVPN-VPWS (MX Series routers and EX9200 switches)**—Starting in Junos OS Release 21.1R1, you can statically configure provider edge (PE) devices to use flow-aware transport (FAT) pseudowire labels in an EVPN virtual private wire service (VPWS) routing instance with an IP/MPLS underlay fabric. PE devices use these labels to load-balance EVPN-MPLS packets across ECMP paths or link aggregation groups (LAGs) without needing to do deep packet inspection of the payload.

To enable FAT pseudowire load balancing in an **evpn-vpws** routing instance:

- Configure **flow-label-transmit-static** on PE devices to insert FAT flow labels into VPWS pseudowire packets sent to remote PE devices.

- Configure **flow-label-receive-static** on PE devices to remove FAT flow labels from VPWS pseudowire packets received from remote PE devices.

You can configure these statements for all pseudowires in the routing instance or for pseudowires associated with a specific interface in the routing instance.

[See FAT Flow Labels in EVPN-VPWS Routing Instances, flow-label-receive-static, and flow-label-transmit-static.]

Interfaces

- **Support for QSFP56-DD-400G-LR4-10 and QSFP56-DD-4X100G-LR optics on MPC11E line card (MX2010 and MX2020)**—Starting in Junos OS Release 21.1R1, you can use the QSFP56-DD-400G-LR4-10 and QSFP56-DD-4X100G-LR 400GE optics on the MPC11E line card in the MX2010 and MX2020 routers.

  [See Hardware Compatibility Tool.]

- **Support for DDOS telemetry (MX Series)**–Starting in Junos OS Release 21.1R1, you can get the DDOS telemetry statistics with the help of Jvision from MPC1, MPC2, MPC3, MPC5, MPC6, MPC7, MPC8, and MPC9 line cards. Use configuration statements:

  - **[show services analytics sensor ddos]** - to see the DDOS configuration

  - **[show agent sensors]** - to see the details about configured sensors

  [See sensor (Junos Telemetry Interface), Guidelines for gRPC and gNMI Sensors (Junos Telemetry Interface), show agent sensors, and show configuration services analytics sensor ddos.]

Junos Telemetry Interface

- **VCP interchassis link port statistics and optimized queue statistics for aggregated Ethernet bundle support with JTI (MX5, MX10, MX40, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX100016, and vMX)**—Starting in Junos OS Release 21.1R1, you can use Junos telemetry interface (JTI) with remote procedure call (gRPC) services to export Virtual Chassis port (VCP) interchassis link statistics and queue statistics. A Virtual Chassis operator can subscribe to supported sensors to monitor the health of MX-VC interchassis links and be able to diagnose and solve issues that may arise when links become unhealthy. This feature also optimizes queue statistics collection, limiting the data and statistical polling to queues that are part of an interface set for which there is an active telemetry subscription. Doing so reduces resources and creates a more stable operating environment.

The supported new sensors are:

- Virtual Chassis port sensor, which provides interchassis links basic error and operational state for the interface (resource path **/junos/system/mxvc/members/member[memberID=<ID>]/virtual-chassis-ports/virtual-chassis-port[vcp-interface-name=<vcp-interface-port-string>]**). This sensor collects the same data displayed when using the operational mode command **show interfaces vcp-*x*/*x*/*x* extensive** and **show virtual-chassis vc-port**.

- Virtual Chassis heartbeat sensor, which provides insight into the overall link health of the Virtual Chassis system (resource path **/junos/system/mxvc/members/member[memberID=<ID>]/heartbeat**). The Virtual Chassis heartbeat sensor, when active, periodically sends and receives information between the chassis to keep track of the connection state. This sensor collects the same data displayed when using the operational mode command **show virtual-chassis heartbeat detail**.

- Virtual Chassis high/low DDoS queue statistics sensor (resource path **/junos/system/mxvc/members/member[memberID=<ID>]/ddos-protocols/ddos-protocol[packetType=<packet_type>]/**). This sensor tracks high and low statistics used in distributed denial-of-service (DDoS) protection. This sensor is available on the global primary chassis. No sensor output is collected for a backup chassis. This sensor collects the same data displayed when using the operational mode command **show ddos-protection protocols virtual-chassis statistics terse**.

- Timestamp sensor (resource path **/junos/system/subscriber-management/dynamic-interfaces/interface-sets/queue-statistics/interface-set[container-index=<container-index>]/fpcs/fpc[slot=<slot>]/last-update-time** and **/junos/system/subscriber-management/dynamic-interfaces/interfaces/queue-statistics/interface[sid=<session-identifier>]/fpcs/fpc[slot=<slot>]/last-update-time**). The timestamp sensor keeps track of when the FPC calculated the queue statistics for a given FPC leg. This provides a better way to track the validity of the data and is a basis for more accurate rate calculations.

The enhanced sensors are:

- Per-subscriber queue statistics sensor (resource path **/junos/system/subscriber-management/dynamic-interfaces/interfaces/queue-statistics/interface[sid=<session-identifier>]/fpcs/fpc[slot=<slot>]/queues/queue[queue-no=<queue-index>]** and **/junos/system/subscriber-management/dynamic-interfaces/interface-sets/queue-statistics/interface-set[container-index=<container-index>]/fpcs/fpc[slot=<slot>]/queues/queue[queue-no=<queue-index>]**). This sensor can include the additional leafs **current-polling-interfaces** and **current-polling-**

interface-sets. When you provide a corresponding index (SID for interface or container ID for interface set), polling for queue statistics is enabled only for that corresponding index. If no index is specified, polling all indexes queue statistics is enabled.

[See Junos Telemetry Interface User Guide.]

- **Optimized chassis sensor support with JTI (MX2010 and MX2020 with MPC11E and MPC9E line cards)**—Starting in Junos OS Release 21.1R1, you can use Junos telemetry interface (JTI) with remote procedure call (gRPC) services to export additional chassis sensors from an MX2010 or MX2020 router to an outside collector.

  For network debugging, there are system-generated logs and SNMP traps available. However, some parameters, such as power entry module (PEM) voltage and PEM supply failure, have not been available in telemetry. We've now introduced these additional system parameters through chassis sensors that support messages logged as part of the SNMP traps for a field-replaceable unit (FRU), fan, PEM, or plane.

  Use the resource path **/components/component/properties/property** in subscriptions for these additional chassis sensors:

  - power-supply-failed
  - chassisd-pem-breaker-trip
  - chassisd-pem-voltage
  - fan-blower-removed
  - pem-not-powered
  - chassisd-zone-blowers-speed-type
  - chassisd-zone-blowers-speed
  - temprature-back-to-normal
  - over-temprature
  - fru-failed
  - plane-fru-check
  - plane-online

  [See Junos Telemetry Interface User Guide.]

MPLS

- **Nonstop active routing (NSR) support for controller-initiated RSVP label-switched paths (LSPs) (MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.1R1, we support NSR for controller-initiated RSVP-based point-to-point (P2P) and point-to-multipoint (P2MP) LSPs. The primary Routing Engine synchronizes all RSVP LSPs initiated by Path Computation Elements (PCEs), including multicast flow specifications for any PCE-initiated P2MP LSPs, with the backup Routing Engine. This ensures zero traffic loss for the traffic carried over PCE-initiated RSVP LSPs during Routing Engine switchovers. This feature is enabled when NSR is configured.

  [See PCEP Configuration.]

- **New transport class-based architecture to facilitate service mapping over colored tunnels (ACX Series, PTX Series, MX Series)**—Starting in Junos OS Release 21.1R1, you can classify colored transport tunnels (RSVP, IS-IS flexible algorithm) in your network into transport classes and map service routes over an intended transport class. You can also extend the transport tunnels to span across multiple domains (ASs or IGP areas) by using the new BGP transport address family called BGP Classful Transport (BGP CT).

  This feature lays the foundation for network slicing and allows the different domains to interoperate irrespective of the transport signaling protocols used in each domain.

  [See https://www.juniper.net/documentation/us/en/software/junos/mpls/topics/topic-map/mpls-traffic-engineering-configuration.html#id_pjt_vxq_2pb.]

- **Install prefixes for RSVP-TE LSPs using PCEP (MX Series, PTX Series, QFX Series)**–Starting in Junos OS Release 21.1R1, you can configure different prefixes for Path Computation Element (PCE)-initiated and PCE-delegated RSVP-TE LSPs using the Path Computation Element Protocol (PCEP). Prior to this feature, for PCE-initiated LSPs, you could install prefixes as routes through templates and map the templates to the LSPs. For Path Computation Client (PCC)-configured LSPs, although you could install prefixes on the device, this information was not reported to the PCE.

  With this feature, you can install prefixes for external RSVP-TE LSPs through PCEP communication, and enable the PCC to report installed prefixes for all local RSVP-TE LSPs to the PCE . This support provides you better traffic engineering capabilities and allows Junos OS to interoperate with other vendor's PCC or PCE.

  [See https://www.juniper.net/documentation/en_US/junos/topics/topic-map/pcep-configuration.html#id-support-of-the-path-computation-element-protocol-for-rsvp-te-overview.]

Multicast

- **MVPN live-live solution support (MX Series)**—Starting in Junos OS Release 21.1R1, we’ve added support to enable the MVPN live-live feature in next-generation multicast VPN (MVPN) with multicast LDP point-to-multipoint (P2MP) provider tunnel. This feature helps to keep your network live all the time.

To enable the MVPN live-live solution:

- Configure the **sender-based-rpf** option by running the **set routing-instances *routing-instance-name* protocols mvpn sender-based-rpf** command. This option is disabled by default.

- Configure the **hot-root-standby** option by running the **set routing-instances *routing-instance-name* protocols mvpn hot-root-standby** command. You can configure this option only if sender-based RPF is enabled.

When you enable this configuration, the receiving PE automatically switches over to the backup path if it encounters any failure while forwarding the traffic from the primary path to the customer network. The transition from primary path to backup path happens in less than 50 milliseconds.

For previous Junos OS releases, we provided support only for RSVP-TE and IR provider tunnels.

[See sender-based-rpf and hot-root-standby.]

Network Management and Monitoring

- **Ephemeral configuration database support for load update operations (EX4300-MP, EX9200, MX5, MX10, MX80, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, and vMX)**—Starting in Junos OS Release 21.1R1, NETCONF and Junos XML protocol client applications can configure the ephemeral configuration database using a load update operation. To perform a load update operation, set the **<load-configuration> action** attribute to **update**.

  [See <load-configuration>.]

- **Ephemeral configuration database support for synchronous commit synchronize operations (MX Series)**—Starting in Junos OS Release 21.1R1, you can configure the ephemeral database to execute commit synchronize operations using a synchronous commit model on dual Routing Engine devices or MX Series Virtual Chassis. The synchronous commit model enables you to reliably use the ephemeral database on devices that have graceful Routing Engine switchover (GRES) or non-stop routing (NSR) enabled. To use the synchronous commit model for the ephemeral database, configure the **commit-synchronize-model synchronous** statement at the **[edit system configuration-database ephemeral]** hierarchy level.
  [See Understanding the Ephemeral Configuration Database.]

- **Operational command RPCs support returning JSON and XML output in minified format in NETCONF sessions (ACX1000, ACX1100, ACX2100, ACX4000, ACX5048, ACX5096, ACX5448, EX2300, EX2500, EX3400, EX4300, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48P, EX4400-48T, EX4600, EX4650, EX9200, MX104, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10001, PTX10002,**

PTX10008, PTX10016, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX10002, QFX10002-60C, QFX10008, QFX10016, SRX550, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)—Starting in Junos OS Release 21.1R1, operational command RPCs, including the **<get-configuration>** RPC, support the **format="json-minified"** and **format="xml-minified"** attributes in NETCONF sessions to return JSON or XML output in minified format. Minified format removes any characters that are not required for computer processing—for example, unnecessary spaces, tabs, and newlines. Minified format decreases the size of the data, and as a result, can reduce transport costs as well as data delivery and processing times.

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

- **SNMP support for carrier-grade NAT PBA monitoring (MX Series)**—Starting in Junos OS Release 21.1R1, you can get port block allocation (PBA) information about MS-MPC and unified services framework (USF)MX-SPC3 - related aspects using two new MIB objects and two new MIB tables:

  - New MIB object jnxNatSrcNumAddressMapped under the MIB table jnxSrcNatStatsTable, and a new MIB table jnxNatPbaStatsTable to get information about MS-MPC-PIC and MS-MIC

  and

  - New MIB object jnxJsNatSrcNumAddressMapped under the MIB table jnxJsSrcNatStatsTable,and a new MIB table jnxJsNatPbaStatsTable to get information about MX-SPC3.

  [See SNMP MIBs and Traps Supported by Junos.]

- **sFlow support for IP-IP traffic (MX240, MX480, and MX960)**—Starting in Junos OS Release 21.1R1, you can use sFlow technology to sample egress sFlow for IP over IP (IP-IP) traffic at the tunnel entry point, transit device, and tunnel endpoint on a physical port. sFlow sampling is supported for IP-IP tunnels with an IPv4 outer header that carry IPv4 or IPv6 traffic. Tunnel header encapsulation is done by either dynamic tunnel or FTI (Flexible Tunnel Interface). You can use sFlow monitoring technology to randomly sample network packets from IP-IP tunnels and to send the samples to a destination collector for monitoring.

  [See Overview of sFlow Technology and Configuring IP Tunnel Interfaces.]

- **HMAC-SHA-2 authentication protocol support for users of SNMPv3 USM (MX Series and SRX Series)**—Starting in Junos OS Release 21.1R1, you can configure HMAC-SHA-2 authentication protocols for users of the SNMPv3 user-based security model (USM) with the following new CLI configuration statements:

  - authentication-sha224
  - authentication-sha256
  - authentication-sha384
  - authentication-sha512

We've introduced these statements for local-engine users at **[edit snmp v3 usm local-engine user username]** and for remote-engine users at **[set snmp v3 usm remote-engine engine-id user user-name]**.

[See authentication-sha224, authentication-sha256, authentication-sha348, and authentication-sha512.]

OpenConfig

- **OpenConfig support for VLAN interfaces (MX240)**—Junos OS Release 21.1R1 supports the following OpenConfig Data Model openconfig-interfaces.yang version 2.4.3 files for VLAN interfaces:

  - **/interfaces/interface/subinterfaces/subinterface/oc-vlan:vlan/oc-vlan:match/oc-vlan:single-tagged/oc-vlan:config/oc-vlan:vlan-id**

  - **/interfaces/interface/subinterfaces/subinterface/oc-vlan:vlan/oc-vlan:match/oc-vlan:double-tagged/oc-vlan:config/oc-vlan:inner-vlan-id**

  - **/interfaces/interface/subinterfaces/subinterface/oc-vlan:vlan/oc-vlan:match/oc-vlan:double-tagged/oc-vlan:config/oc-vlan:outer-vlan-id**

  [See Mapping OpenConfig VLAN Commands to Junos Configuration.]

- **OpenConfig support for GRE tunnel interfaces (MX5, MX10, MX40, MX150, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, and vMX)**—Junos OS Release 21.1R1 supports the following OpenConfig Data Model openconfig-if-tunnel.yang version 0.1.1 sensors:

  - **/interfaces/interface/oc-tun:tunnel/oc-tun:config/oc-tun:src**

  - **/interfaces/interface/oc-tun:tunnel/oc-tun:config/oc-tun:dst**

  - **/interfaces/interface/oc-tun:tunnel/oc-tun:config/oc-tun:ttl**

  - **/interfaces/interface/oc-tun:tunnel/oc-tun:ipv4/oc-tun:addresses/oc-tun:address/oc-tun:config/oc-tun:ip**

  - **/interfaces/interface/oc-tun:tunnel/oc-tun:ipv4/oc-tun:addresses/oc-tun:address/oc-tun:config/oc-tun:prefix-length**

  - **/interfaces/interface/oc-tun:tunnel/oc-tun:ipv4/oc-tun:config/oc-tun:mtu**

  - **/interfaces/interface/oc-tun:tunnel/oc-tun:config/oc-tun:gre-key**

  This feature includes converting OpenConfig configuration schemas to Junos OS configuration schemas. For example, the OpenConfig command**set openconfig-interfaces:interfaces interface gr-0/0/0 openconfig-if-tunnel:tunnel config src 1.1.1.1** maps to the Junos OS command **set interfaces gr-0/0/0 unit 0 tunnel source 1.1.1.1**.

[See OpenConfig User Guide.]

Platform and Infrastructure

- **Next Gen Services (MX240, MX480, and MX960 with MX-SPC3)**— Starting in Junos OS Release 21.1R1, we support IPsec (a Next Gen Services component) on the listed MX Series routers with the MX-SPC3 services card installed. To configure IPsec on MX Series routers with MX-SPC3, use the CLI configuration statements at the [**edit security**] hierarchy level. On MX Series routers with MS-MPC/MS-MIC line cards, you configure the feature at the [**edit services**] hierarchy level.

  > **NOTE**: MX240, MX480, and MX960 routers with MS-MPC/MS-MIC and MX-SPC3 support Next Gen Services. We introduced this support in Junos OS Release 19.3R2.

  See Next Gen Services Overview

- **Table 7: Next Gen Services Supported on MX-SPC3**

Feature	Description
MX-SPC3 IPsec VPN Feature License	You require a valid license to use the IPsec VPN feature on your MX Series devices with the MX-SPC3 services card. This is a binary license. The **show system license** command output displays the license count as 0 when no license is installed and 1 when a valid license is installed. You won't be able to establish IPsec VPN tunnels if you don't have a valid license to use the feature. However, tunnels that are currently active will continue to stay up if your license expires. You cannot reestablish IPsec VPN tunnels that go down after the expiry of the license until you install a valid license. See Managing Licenses.
IPsec VPN	The MX-SPC3 services card provides consistent IPsec VPN capability across security and routing platforms. You configure IPsec for the MX-SPC3 at the [**edit security**] hierarchy level. See Next Gen Services Overview

Table 7: Next Gen Services Supported on MX-SPC3 *(Continued)*

Feature	Description
AutoVPN preshared key (PSK) on MX-SPC3	To allow different IKE preshared keys used by the VPN gateway to authenticate the remote peer, use our new CLI statements **seeded-pre-shared-key ascii-text** or **seeded-pre-shared-key hexadecimal** at the **[edit security ike gateway *gateway_name*]** hierarchy level. To allow the same IKE preshared key used by the VPN gateway to authenticate the remote peer, use the existing CLI command **pre-shared-key ascii-text** or **pre-shared-key hexadecimal**. During authentication of the remote peer, use the **general-ikeid** statement at the **[edit security ike gateway *gateway_name* dynamic]** hierarchy level to bypass the IKE-ID validation. See AutoVPN on Hub-and-Spoke Devices.
Add new members to existing aggregated multiservice (AMS) bundle for IPsec service	To add new members to an AMS bundle (for IPsec services) without impacting the traffic on the existing AMS bundle, configure the **no-bundle-flap** statement under the **[edit interfaces *interface-name* load-balancing-options]** hierarchy in non-HA mode. During the configuration change, the existing members in the AMS bundle don't flap. See Understanding Aggregated Multiservices Interfaces for Next Gen Services.

Table 7: Next Gen Services Supported on MX-SPC3 *(Continued)*

Feature	Description
PowerMode IPsec	The MX-SPC3 card supports PowerMode IPsec (PMI) with vector packet processing (VPP) and Intel Advanced Encryption Standard New Instructions (AES-NI), leading to IPsec performance improvements. You can enable PMI processing by using the **set security flow power-mode-ipsec** command. To disable PMI processing, use the **delete security flow power-mode-ipsec** command. MX-SPC3 also supports the fat tunnel feature that improves the performance of a single tunnel. If one of the tunnels is loaded with traffic and other tunnels have less traffic, the resources are shared within the fat group. This results in an even CPU utilization of the resources. To enable this feature, configure the **fat-core** statement at the [**edit security distribution-profile**] hierarchy level. You must configure the PMI feature first to enable the fat tunnel feature. See Improving IPsec Performance with PowerMode IPsec, Understanding Symmetric Fat IPsec Tunnel, and power-mode-ipsec.
Support for mobility in CGNAT–XLAT464	We've upgraded the current dual-translation (464XLAT) feature by introducing **clat-ipv6-prefix-length** at the source NAT rule hierarchy level. You can use a single NAT rule with this configuration parameter in place of multiple source NAT rules with different source-address and customer-side translator (CLAT)-prefix values. This simplifies the configuration method for certain use case scenarios.
Support for time zones in carrier-grade NAT	Support for syslog timestamp (local system time stamp) using the **utc-timestamp** statement at the [**edit interfaces interface-name services-options**] hierarchy level.
Network Address Translation - Port Translation (NAT-PT)	We support NAT-PT with the DNS ALG service on the MX-SPC3 services card. See Configuring the DNS ALG.

Table 7: Next Gen Services Supported on MX-SPC3 *(Continued)*

Feature	Description
MPC10E interoperability	The MPC10E (MPC10E-15C-MRATE and MPC10E-10C-MRATE) line card interoperates with the MX-SPC3 services card to support the NAT and stateful firewall Layer 3 services. See Protocols and Applications Supported by MX-SPC3 Services Card

Port Security

MACsec bounded delay protection (MX10003 routers)—Starting in Junos OS Release 21.1R1, you can configure bounded delay protection on MX10003 routers. MACsec bounded delay protection prevents the delivery of a frame when the frame is delayed by two seconds or longer. This feature enables the detection of delayed MACsec frames that result from a man-in-the-middle attack.

Routing Protocols

- **IS-IS link delay measurement and advertising (MX Series)**—Starting in Junos OS Release 21.1R1, you can measure and advertise various performance metrics in IP networks with scalability, by using several IS-IS probe messages. These metrics can then be used to make path-selection decisions based on network performance.

  [See How to Enable Link Delay Measurement and Advertising in IS-IS, delay-measurement, and delay-metric.]

- **Support for configuring multiple independent IGP instances of IS-IS (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.1R1, you can configure and run multiple independent IGP instances of IS-IS simultaneously on a router.

  > **NOTE**: Junos OS does not support configuring the same logical interface in multiple IGP instances of IS-IS.

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

- **Avoid microloops in IS-IS-SRv6 networks (MX Series with MPC7E, MPC8E and MPC9E line cards)** — Starting in Junos OS Release 21.1R1, you can enable post-convergence path calculation on a device to avoid microloops if a link or metric changes in an SRv6 network. Note that microloop avoidance is not a replacement for local repair mechanisms such as topology-independent loop-free alternate (TI-LFA), which detects local failure very fast and activates a precomputed loop-free alternative path.

To configure microloop avoidance in an SRv6 network, include the **microloop avoidance post-convergence-path delay *milliseconds*** statement at the **[edit protocols isis spf-options]** hierarchy level.

[See How to Configure Microloop Avoidance for IS-IS in SRv6 Networks.]

- **SRv6 network programming in IS-IS (MX Series with MPC10 and MPC11 line cards)**—Starting in Junos OS Release 21.1R1, you can configure segment routing in a core IPv6 network without an MPLS data plane. This feature is useful for service providers whose networks are predominantly IPv6 and have not deployed MPLS. Such networks depend only on the IPv6 headers and header extensions for transmitting data. This feature also benefits networks that need to deploy segment routing traffic through transit routers that do not have segment routing capability yet. In such networks, the SRv6 network programming feature can provide the flexibility to leverage segment routing without deploying MPLS.

  To enable SRv6 network programming in an IPv6 domain, include the **srv6** statement at the**[edit routing-options 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.

  To configure a topology-independent loop-free alternate (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 BGP Auto-discovered Neighbor (MX Series, PTX1000, PTX10008, QFX5120-32C, QFX5200, QFX5210, and QFX10008)**—Starting in Junos OS Release 21.1R1, we support BGP auto-discovered neighbors using IPv6 Neighbor Discovery Protocol (ND). With this feature, you can enable BGP to create peer neighbor sessions using link-local IPv6 addresses of directly connected neighbor devices. You need not specify remote or local neighbor IP addresses.

  To enable peering for a given interface or set of interfaces without specifying the local or remote neighbor addresses, configure the **peer-auto-discovery** statement at the [**edit fabric protocols bgp group <*name*> dynamic-neighbor <*name*>**] hierarchy level.

  [See BGP Auto-Discovered Neighbors, and peer-auto-discovery.]

Segment Routing

- **Support for flexible algorithm in OSPFv2 for segment routing traffic engineering (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.1R1, you can thin-slice a network by defining flexible algorithms that compute paths using different parameters and link constraints based on your requirements. For example, you can define a flexible algorithm that computes a path to minimize IGP metric and define another flexible algorithm to compute a path based on traffic engineering metric to divide the network into separate planes. This feature allows networks without a controller to configure traffic engineering and utilize segment routing capability of a device.

To define a flexible algorithm, include the **flex-algorithm** statement at the **[edit routing-options]** hierarchy level.

To configure a device to participate in a flexible algorithm, include the **flex-algorithm** statement at the **[edit protocols ospf source-packet-routing]** hierarchy level.

[See How to Configure Flexible Algorithms in OSPF for Segment Routing Traffic Engineering.]

- **Support for strict SPF and IGP shortcut (ACX710, MX960, MX10008, MX2020, PTX5000, and PTX1000)**—Starting in Junos OS Release 21.1R1, you can configure segment routing algorithm 1 (strict SPF) and advertise its SIDs in IS-IS link-state PDU (LSPDU) and use these SIDs to create SR-TE tunnels to forward the traffic by using the shortest IGP path to reach the tunnel endpoint while avoiding loops. You can also specify a set of prefixes in the import policy, based on which the tunnel can redirect the traffic to a certain destination. You can use algorithm 1 (strict SPF) along with algorithm 0 (default SPF) by default when Source Packet Routing in Networking (SPRING) is enabled.

  [See How to Enable Strict SPF SIDs and IGP Shortcut, prefix-segment, and source-packet-routing.]

Services Applications

- **Support for displaying the timestamp in syslog (MX Series routers with MS-MPC, MS-MIC, and MX-SPC3)**—Starting in Junos OS Release 21.1R1, you can enable system log (syslog) timestamps in local system timestamp format or UTC format.

  On routers with MS-MPC, you can override the default UTC timestamp to local system timestamp format by configuring the new statement, **syslog-local-system-timestamp**, at the **edit interfaces *ms-interface\ams-interface*services-options** hierarchy level.

  On routers with MX-SPC3 cards, you can override the default local system timestamp in syslog to UTC format by configuring the existing statement,**utc-timestamp**, at the **edit interfaces *vms-interface\ams-interface*services-options** hierarchy level or at the **[edit services *service-set-name*syslog** hierarchy level.

  For the routers with MX-SPC3 cards, starting in Release 21.1R1 you can configure the **utc-timestamp** statement at the **edit interfaces *vms-interface\ams-interface*services-options** hierarchy level. In earlier releases, we support this statement at the **[edit services *service-set-name*syslog** hierarchy level.

  [See syslog (Services Service Set).]

- **Enhancements to DNS sinkhole feature (MX240, MX480, and MX960 routers with MS-MPC and MX-SPC3)**—Starting in Junos OS Release 21.1R1 as part of the DNS sinkhole feature enhancements, you can:

- Configure new actions for a DNS request for a disallowed domain-alert, accept, drop, and drop-no-log.
- Configure domain names and actions for multiple tenants such that domain feeds can be managed on a per tenant basis.
- Configure hierarchical domain feed management per profile, dns-filter-template or dns-filter-term.
- Exempt domain feeds at the IP, subnet, or CIDR level.

[See DNS Request Filtering for Disallowed Website Domains.]

- **TWAMP Light IPv4 support (MX Series)**—Starting in Junos OS Release 21.1R1, we support the Two-Way Active Measurement Protocol (TWAMP) Light, as defined in Appendix I of RFC 5357. TWAMP Light is a stateless version of TWAMP, where test parameters are predefined instead of negotiated. All test packets received by the server on a test port are reflected back and forgotten right away.

  [See twamp.]

- **Support for the any firewall filter family and the Layer 2 firewall filter families for inline monitoring services (MX Series)**—Starting in Junos OS Release 21.1R1, you can configure the **any**, **bridge**, **ccc**, **mpls**, or **vpls** family firewall filter with the term action **inline-monitoring-instance** ***inline-monitoring-instance-name***.

  [See Inline Monitoring Services Configuration .]

Software-Defined Networking (SDN)

- **Configure SLCs and assign them to GNFs (MX2010 and MX2020)**—Starting in Junos OS Release 21.1R1, in an external server-based Junos node slicing setup, you can additionally configure logical partitions (called sub line cards or SLCs) of the MX2K-MPC11E line card and assign each partition to different guest network functions (GNFs). See Sub Line Card Overview for details. You can create two SLCs on an MX2K-MPC11E. An SLC functions like an independent line card.

  In Junos OS Release 21.1R1, SLCs do not support handling of failures of links between Control Boards and the server, graceful Routing Engine switchover on BSYS and GNF, and unified in-service software upgrade.

  > **NOTE**: In Junos OS Release 21.1R1, Junos node slicing is not multi-version interoperable with previous releases of Junos OS (whether or not SLCs are configured). So, for any GNF in a node-sliced system to run Junos OS Release 21.1R1, all other GNFs and BSYS must also run Junos OS Release 21.1R1.

  [See Configuring Sub Line Cards and Assigning Them to GNFs.]

- **Support for ECMP on multiple flexible routes (MX Series routers with MPC10 and MPC11 line cards)**—Starting in Junos OS Release 21.1R1, MX Series routers with MCP10 or MPC11 line cards support traffic load balancing over multiple flexible routes with 64-way ECMP. A flexible route is a static route with a tunnel encapsulation profile that has the flexible tunnel interface (FTI) attribute. Multiple flexible routes can go through the same logical interface. You can install flexible routes on Juniper gateway devices using Juniper Extension Toolkit (JET) APIs.

  When the router receives a packet with the flexible route as the destination address, it processes the packet using the profile associated with a flexible route, and load-balances the traffic across multiple flexible routes based on the traffic priority.

  Use the **show route** and **show route extensive** CLI commands or the **get-route-information** RPC/NETCONF command to view details about a flexible route for a destination address.

  [See Understanding Programmable Flexible VXLAN Tunnels.]

Software Installation and Upgrade

- **Support for signed third-party application installation (MX10003, MX10008, QFX5210, QFX10002, and QFX10008 routers with VM host architecture)**—Starting in Junos OS Release 21.1R1, you can install signed third-party application installation and carry over the application between upgrades.

  The backup of third-party package occurs during upgrade. Hence, the package is restored even if the installed package is deleted or uninstalled before a reboot. However, as the third party package restoration depends on the contents saved on the disk during upgrade and the configuration to allow the package to be installed, restoration is not possible when

  - Configuration is removed after upgrade

  - Content is removed due to deletion by configuring **request vmost zeroize** command

  On platforms where jinstall-host.tgz images are installed, the minimum space required for the backup is 250MB. After backup, if the free space available is less than 200MB, the backup would be deleted to make space for upgrade. On platforms where junos-vmhost images are installed, the minimum space required for backup of third party unbundled packages is 1200MB. After the backup, if the free space is less than 512MB, the backup would be deleted to free up space for upgrade.

  [See Installing, Upgrading, Backing Up, and Recovery of VM Host.]

- **request system software status command (MX480, MX960, MX2010, MX2020, SRX1500, SRX4100, SRX4400, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, you can use the CLI command **request system software status** to view the status of the software package installation or uninstallation on the local Routing Engine.

Subscriber Management and Services

- **L2TP session lockout support (MX Series)**—Starting in Junos OS Release 21.1R1, you can specify the **lockout-result-code** and **lockout-error-code** options to control the L2TP access concentrator (LAC) behavior in the Layer 2 Tunneling Protocol (L2TP) session lockout state.

  [See lockout-timeout (L2TP Destination Lockout).]

- **Support for PWHT (over EVPN-VPWS, on a transport logical interface) with subscriber management (BNG) service logical interfaces (MX Series routers)**—Starting in Junos OS Release 21.1R1, you can deploy broadband network gateways (BNGs) that are connected to aggregation networks running EVPN-VPWS. You configure pseudowire headend termination (PWHT) on a transport logical interface that is on the pseudowire subscriber interface. The BNG pops the EVPN and VPWS headers and terminates subscribers at Layer 2.

  This feature includes support for:

  - All broadband features available on PWHT on MX Series routers
  - Single-homed EVPN-VPWS with the pseudowire subscriber interface anchored to a logical tunnel (LT) interface
  - Choice of whether or not to use a control word

What's Changed

IN THIS SECTION

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

What’s Changed in Release 21.1R1

IN THIS SECTION

General Routing

- **Updates to ON-CHANGE and periodic dynamic subscriber interface metadata sensors (MX Series routers and EX9200 line of switches)**—We've made the following updates to the **/junos/system/subscriber-management/dynamic-interfaces/interfaces/meta-data/interface<user-typing>sid='<variable>sid-value</variable>'</user-typing>/** sensor:

  - Notifications are sent when subscribers log in on either IP demux or VLAN demux interfaces. In earlier releases, login notifications are sent only for IP demux logins.

  - The *interface-set* end path has been added to the logical interface metadata. The interface-set field appears in both ON-CHANGE and periodic notifications. In earlier releases, this field is not included in the sensor metadata or notifications.

  [See gRPC Sensors for Subscriber Statistics and Queue Statistics for Dynamic Interfaces and Interface-Sets (Junos Telemetry Interface).]

- **New commit check for MC-LAG (MX Series)**—We've introduced a new commit check to check the values assigned to the redundancy group identification number on the MC-AE interface **(redundancy-group-id)** and ICCP peer **(redundancy-group-id-list)** when you configure multichassis link aggregation groups (MC-LAGs). If the values are different, the system reports a commit check error. In previous releases, if the configured values were different, the l2ald process would crash.

  [See iccp.]

- **Support for unicast ARP request on table entry expiration**—You can configure the device to send a unicast ARP request instead of the default broadcast request when an ARP table entry is about to expire. The retry requests are unicast at intervals of 5 seconds. Without this option, the retry requests are broadcast at intervals of 800 milliseconds. This behavior reduces ARP overall broadcast traffic. It also supports the use case where access nodes are configured not to forward broadcast ARP requests toward customer CPEs for security reasons and instead translate ARP broadcasts to unicast requests. To confirm whether the device is configured, you can issue the following command: **show configuration system arp | grep unicast-mode-on-expire**

  [See arp.]

- **Change in license bandwidth command on vMX virtual routers**—To use the available license bandwidth, explicitly set the license bandwidth by using the **set chassis license bandwidth *In Mbps*** command.

  [See Configuring Licenses on vMX Virtual Routers.]

Interfaces and Chassis

- **Hardware-assisted timestamping**—By default, hardware assistance is used for timestamping Ethernet frame delay frames on AFT-based MX Series line cards, even if **hardware-assisted-timestamping** is not configured.

  [See Enabling the Hardware-Assisted Timestamping Option.]

- **Change in range> XML tag (MX480)**—We've changed the **<range> string </range>** XML tag to **<transport-range> <transport-range-info> string </transport-range-info> <transport-range-suspect-flag> string </transport-range-suspect-flag> <transport-range-reason> string </transport-range-reason> </transport-range>** under the [**show interfaces transport pm optics current <interface> | display**] hierarchy in the XML output. Hence, the new XML tags that associate the values to the range-info, range-suspect-flag, and range-reason tags map the information to the given **show interfaces transport pm optics current interface | display** entry.

  [See Supported OTN Options on MX Series Routers.]

Junos XML API and Scripting

- **The jcs:invoke() function supports suppression of root login and logout events in system log files for SLAX commit scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The **jcs:invoke()** extension function supports the **no-login-logout** parameter in SLAX commit scripts. If you include the parameter, the function does not generate and log **UI_LOGIN_EVENT** and **UI_LOGOUT_EVENT** messages when the script logs in as root to execute the specified remote procedure call (RPC). If you omit the parameter, the function behaves as in earlier releases in which the root **UI_LOGIN_EVENT** and **UI_LOGOUT_EVENT** messages are included in system log files.

  [See invoke() Function (SLAX and XSLT).]

- **The jcs:invoke() function supports suppression of root login and logout events in system log files for SLAX event scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The **jcs:invoke()** extension function supports the **no-login-logout** parameter in SLAX event scripts. If you include the parameter, the function does not generate and log **UI_LOGIN_EVENT** and **UI_LOGOUT_EVENT** messages when the script logs in as root to execute the specified remote procedure call (RPC). If you omit the parameter, the function behaves as in earlier releases in which the root **UI_LOGIN_EVENT** and **UI_LOGOUT_EVENT** messages are included in system log files.

  [See invoke() Function (SLAX and XSLT).]

- **Python 2.7 deprecation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, devices running Junos OS no longer support Python 2.7. We've deprecated the corresponding **language python** statement at the **[edit system scripts]** hierarchy level. To execute Python scripts, configure the **language python3** statement at the **[edit system scripts]** hierarchy level to execute the scripts using Python 3.

  [See Understanding Python Automation Scripts for Devices Running Junos OS.]

Layer 2 Ethernet Services

Active leasequery-based bulk leasequery (MX Series)—The **overrides always-write-option-82** and **relay-option-82 circuit-id** configuration at the [**edit forwarding-options dhcp-relay**] hierarchy level is not mandatory for active leasequery-based bulk leasequery. In releases before Junos OS Release 21.1R1, the **overrides always-write-option-82** and **circuit-id** configurations are mandatory for active leasequery-based bulk leasequery. For regular bulk leasequery between relay and server without any active leasequery, the **overrides always-write-option-82** and **relay-option-82 circuit-id** configurations are mandatory.

[See bulk-leasequery (DHCP Relay Agent).]

Network Management and Monitoring

- **Support for specifying the YANG modules to advertise in the NETCONF capabilities and supported schema list (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—You can configure devices to emit third-party, standard, and Junos OS native YANG modules in the capabilities exchange of a NETCONF session by configuring the appropriate statements at the **[edit system services netconf hello-message yang-module-capabilities]** hierarchy level. In addition, you can specify the YANG schemas that the NETCONF server should include in its list of supported schemas by configuring the appropriate statements at the **[edit system services netconf netconf-monitoring netconf-state-schemas]** hierarchy level.

  [See hello-message and netconf-monitoring.]

- **Support for disconnecting unresponsive NETCONF-over-SSH clients (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—You can enable devices to automatically disconnect unresponsive NETCONF-over-SSH clients by configuring the **client-alive-interval** and **client-alive-count-max** statements at the **[edit system services netconf ssh]** hierarchy level. The **client-alive-interval** statement specifies the timeout interval in seconds, after which, if no data has been received from the client, the device requests a response. The **client-alive-count-max** statement specifies the threshold of missed client-alive responses that triggers the device to disconnect the client, thereby terminating the NETCONF session.

  [See ssh (NETCONF).]

User Interface and Configuration

Verbose format option to export JSON configuration data (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)—The Junos OS CLI exposes the **verbose** statement at the **[edit system export-format json]** hierarchy level. We changed the default format to export configuration data in JavaScript Object Notation (JSON) from **verbose** to **ietf** starting in Junos OS Release 16.1R1. You can explicitly specify the default export format for JSON configuration data by configuring the appropriate statement at the **[edit system export-format json]** hierarchy level. Although the **verbose** statement is exposed in the Junos OS CLI as of the current release, you can configure this statement starting in Junos OS Release 16.1R1.

[See export-format.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for MX Series routers.

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

General Routing

- On the MX104 router, scheduler slip is observed when configuration changes are committed. PR1361250

- Traffic stops after the volume limit is reached but the traffic resumes after an aggregated Packet Forwarding Engine interface fails. PR1463723

- For two tunnels with same TS, all traffic is forwarded on the tunnel that comes up later. PR1467364

- The BGP neighbor flaps during the primary NG-RE reboot, although GRES or NSR is enabled. PR1524791

- The NPC process continuously generates core files at **Trinity_Ktree::Trinity_FourWayBlock, Trinity_Ktree::walkSubTree** due to the next-hop memory exhaustion with the next-hop explosion. The rpd and srrd processes start hogging and the system becomes unstable. PR1538029

- Guidelines are needed for enabling or restarting fib-streaming in low-memory conditions. PR1540478

- On the MX10003 routers, after a subscriber logs in, the subscriber is allowed to delete the entire AGF service stanza and commit the configurations, leaving the subscribers stuck in the **Active** state permanently. The user must not be allowed to delete the AGF Service configurations with active UEs. PR1555031

- On the MPC11E line cards, the following error message is observed:

  ```
  ppman - PPM:RPC - Error message <url
  ```

  PR1559434

- On the MPC11E line cards, the following error message is observed:

  ```
  l2tp-sfd[11852]: [Error] L2TP-SFD & CFMMAN & VBFMAN & RPC-SERVICE
  ```

  PR1559440

- The RPD process generates core file if the **use-for-shortcut** command is configured on an SRTE tunnel which uses an SR Algo 0 Prefix SID. PR1578994

Interfaces and Chassis

- For MC-LAG to work properly, the mc-ae interface should be configured on both the PE devices. A scenario where the mc-ae interface is deleted, deactivated, or not configured on one of the devices is a case of misconfiguration. Juniper Networks does not support such a scenario because it can lead to traffic loss and other unexpected behavior. PR1536831

- On the MPC10 line cards, DMRs or SLRs are not received with an EVPN up MEP on the aggregated Ethernet interface with normalization. PR1543641

MPLS

- The rpd process might crash. PR1461468

Network Management and Monitoring

- SNMP link up trap message is not observed after a line card reboots when scaled interfaces are present. PR1507780

Routing Protocol

Convergence time is high when the igmp snooping configuration is deleted. PR1550523

User Interface and Configuration

- Unsupported options are displayed under the **restart** commands. PR1545558

VPNs

- Traffic loss is observed on starting the traffic with PIM disabled under the ingress primary UMH. PR1562759

Open Issues

IN THIS SECTION

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

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

Class of Service (CoS)

- On the MPC7E line cards, the BPS counter of the egress queue displays wrong BPS value when the cell mode is configured on the static interface. PR1568192

EVPN

- The VXLAN OAM host-bound packets are not throttled with the DDoS policers. PR1435228
- The vmcore process generates core file at **rts_ifbd_get_parent, rts_ifstate_chk_if_interesting_int, rts_ifstate_chk_if_interesting_int_with_stats**. PR1542037
- Prefix added to the **mhevpn.evpn.0 output** route table triggers TC failure. PR1566429
- The mustd.core process generates core file during upgrading or committing a configuration. PR1577548
- On the MX480 routers, the vmcore process generates core file at **rts_ifbd_get_parent, rts_ifstate_chk_if_interesting_int, rts_ifstate_chk_if_interesting_int_with_stats**. PR1580313

Forwarding and Sampling

- Packet length for ICMPv6 is shown as **0** in the output of the **show firewall log detail** command. PR1184624
- After you restart routing, the remote mask (which indicates from which remote PE devices MAC-IP addresses are learned) that the routing daemon sends might be different from the existing remote mask that the Layer 2 learning daemon had before the restart. This causes a mismatch between Layer 2 learning and routing daemons' interpretation as to where the MAC-IP address entries are learned, either local or remote, leading to the MAC-IP table being out of synchronization. PR1452990

General Routing

- On the MX104 router, if you use **snmpbulkget** or **snmpbulkwalk** (for example, used by the SNMP server) on a chassisd-related component (for example, jnxOperatingEntry), high CPU usage and slow response of the chassis process (chassisd) might be observed because of a hardware limitation, which might also lead to a query timeout on the SNMP client. This issue might not be observed while using an SNMP query. PR1103870
- On the MPC7E line cards, the following log message might be seen on FPC with WINTEC mSATA SSD:

```
SMART ATA Error Log Structure error: invalid SMART checksum.
```

PR1354070

- Modifying the underlying interface on a demux0 interface with subscribers present on the underlying interface causes the FPC to generate core files. PR1396157

- Subscribers experience 100 percent CPU utilization of the FPC for 56 minutes after changing the service firewall filter configuration. PR1447003

- In the DNS filtering when the DNS request are sent from the server, implicit filters and routes to the service PIC are configured. This causes the DNS packets to loop. PR1468398

- A regression issue causes the WAN-PHY interface to continuously flap with the default hold-time down of 0. PR1508794

- LFM might flap during MX Virtual Chassis ISSU. PR1516744

- The RPD sensors generate core files during defer-continue case on the network churn. PR1526503

- Inconsistent **core.python2.7.mpc0** core file is seen with **stacktrace @ea_wi_precl,@ea_macsec_receive.**PR1534568

- The CFM sessions go down during FRU upgrade stage of ISSU in MX Virtual Chassis. PR1534628

- On the MX480 routers, sFlow log error message is seen when egress sampling is enabled in a dynamic IP-IP tunnel encapsulation scenario. PR1538863

- On the MX2020 router, the next hops are less than the total number of nhdb 4MPOST GRES. PR1539305

- Even though **enhanced-ip** is active, the following alarm is observed during ISSU:

  ```
  RE0 network-service mode mismatch between configuration and kernel setting.
  ```

  PR1546002

- Heap malloc(0) is detected for **jnh_unilist_adaptive_add** on loading the configurations. PR1547240

- Commit error is observed when **deactivate chassis synchronization source** and **esmc-transmit all** are configured. PR1549051

- Captive portal for phone-home bootstrap process is not supported. PR1555112

- On the MPC11E line cards in BSYS, commit goes through when ISSU is initiated in the GNF. PR1556544

- On the MX10008 routers, the GRE keepalive adjacency state is **Down** even though the GRE tunnel is in the **Up** state. PR1559200

- On the MPC11 line cards, error messages are not displayed while executing the **show log message** command with errors. PR1560920

- Core files are found at **MX104-ABB-0.gz.core.0.gz >clksync_geneva_delete_ptp_loc_entry> clksync_geneva_ptp_add_clock_entry> clksync_ptp_stream_proc_op> clksync_event_update> clksync_process_event.** PR1561004

- The session status gets stuck in the **Invalid** state after the core-facing link fails in the primary PE devices. PR1562387

- Fusion cascade ports must not be hosted on the VPN core-facing FPC. PR1567850

- On the MX480 routers, traffic loss is observed with scale 4000 tunnels 800 VRF test. PR1568414

- Sometimes part of the output of the **show ptp lock-status detail** command is missed while changing the interface configuration from the encapsulation Ethernet to the family inet. PR1572047

- PIM rib-group fails to be added in VRF. PR1574497

- Commit check for a validating the interface name is not available for the **show interface** command. PR1306191

- Changing the scaled firewall profiles on the fly does not release the TCAM resources as expected. PR1512242

- MACSEC PIC stays offline in new primary after ISSU is in GNF. PR1534225

- the ngmpc2 process generates core file at **bv_entry_active_here::bv_vector_op:: gmph_reevaluate_group:: gmph_destroy_client_group.** PR1537846

- During power cycle, 100G port down issue is observed occasionally on et-0/0/54 and et-0/0/55 with INNOLIGHT 100G-AOC cables. PR1548525

- On the MPC9E line card, core file is generated when SFB is online after ISSU of a GNF.

  PR1556627

- The core.python2.7.mpc0 core file is observed while trying to integrate script in vZT. PR1556719

- RIOT crashes with the following error message that causes aftd-trio crash: **FATAL:Failed to translate ucode instruction**. PR1559522

- IGMP joins where there are more than expected value while verifying the IGMP snooping membership in the CE router. PR1560588

- Some BFD sessions get stuck in the **Down** or **Init** state after the iterative operations triggers on DUT. PR1560772

- The traffic silently gets discarded on switching the rlt interface with both legs on subLC slices. PR1566198

- After loading the inline services configuration and loading the twamp configuration, the SLC reboots and AFT generates core files. PR1567313

- The mpc-2e-3e-ng core file is generated at **htimer_is_last_child htimer_relink_timer htimer_set_exptime_internal**. PR1567495

- The mspmand process might crash if the packet flow-control issue occurs on MS-MPC or MS-MIC. PR1569894

- PDB pull or synchronization does not occur in new primary during ISSU. PR1570841

- The toe_gld_toe0_ucode process generates core file at **prds_rt_ifl_ipv6_del_hndl_from_desc_list**.PR1571279

- The **show services mobile-edge sessions summary access-network-peers** command displays incorrect established subscriber output after the UPF Handover ENB step. PR1572520

- The **unplugged** message of the CFP is not logged in Junos OS Release 17.3 and later. PR1573209

- The rpd process on the transit node might crash while performing the MPLS traceroute on the ingress node. PR1573517

- From the regress user shell prompt, the vhclient access does not display the following error: **rcmd: socket: Operation not permitted**. PR1574240

- The MPC10E line cards generates the following error message: **user.err aftd-trio: [Error] Em: root: Insert entry failed, entry:parentToken:747441 entryMask:ffffffffffffffff index:52**. PR1575310

- On the MX150 routers, interfaces might take a long time to power down while rebooting, powering-off, halting, or upgrading. PR1575328

- The **show services service-sets statistics syslog** command returns the following error message as the service-set does not have the syslog configuration: **error: usp_ipc_client_recv_ 1237: ipc_pipe_read fails! error:No error: 0(0), tries:1**. PR1576044

- Verification of NAT POOL DETAIL fails while verifying the SIP and bi-directional mapping with the block-size configured as default. PR1576398

- On the MX10016 routers, when the **Fan X Failed** alarm is cleared in the Fan Tray 1, the **Fan/Blower OK** SNMP traps are generated for the Fan Tray 0 [Fan 31 - 41] and Fan Tray 1 [Fan 11 - 41]. PR1576521

- With sharding configuration enabled, the RPD process generates core file at **rsi_configipc_shardsprocess, rpd_shard_infra_recv_handler, (jp=< optimized out>)** at **../../../../../../../../src/junos/usr.sbin/rpd/lib/jipc-infra/rpd_jipc_infr a_ipc.c:813**.

PR1577193

- On the MPC11E line cards, system resource monitor does not list some of the available Packet Forwarding Engines. PR1579975
- On the MX480 routers, the SLIP messages are observed while testing the inline GRE reassembly feature with the GRE interface scaling. PR1581042
- In the NAT64 scenario during session creation, IPv6 atomic fragments are not processed correctly. PR1581348
- ISSU status displays errors with the reason of disconnection after ISSU and before switchover. PR1581380
- When the MX Series device is in the SAEGW-U mode, in rare cases of a double back-to-back failover involving GRES and Node Association release, some access-peers might not be freed (even after the sessions count associated with that peer reaches zero). PR1549689
- On the MX2010 and MX2020 devices, the following error message might be seen after switchover with GRES/NSR: **CHASSISD_IPC_FLUSH_ERROR**. PR1565223
- Core files are generated at **export_svc_set_nat_idl@nsd_calloc** while verifying the no-translation with destination-nat. PR1568997
- On the MX960 devices, the 400G and 4x100G optics laser restores after reboot despite **interface disable** being configured. PR1582418
- The rpd might crash due to a rare timing issue if both BGP Local-RIB and Adjacency-RIB-In route monitoring are enabled in BMP. PR1584560

Infrastructure

- The HSRPv2 IPv6 packets might get dropped if IGMP snooping is enabled. PR1232403
- The following error message is observed continuously in AD with base configurations:

```
IFDE:Null uint32 set vector, ifd and IFFPC: 'IFD Ether uint32 set' (opcode
151) failed.
```

  PR1485038
- User while loading the kernel displays the following error message: **GEOM: mmcsd0s.enh: corrupt or invalid GPT detected**. PR1549754

Interfaces and Chassis

- On the MX480 routers, the output of the **show interfaces transport pm otn current < interface>** command is not as expected. PR1560533
- On the MX2020 routers, the MM TXED is not the same as LMR RX due to packet loss with cycle time 100ms. PR1561397

Juniper Extension Toolkit (JET)

- Abrupt shutdown or closure of the collector port results in GRPC connection with the same client ID to fail till all the devices are disconnected. PR1549044

Layer 2 Ethernet Services

- The OSPF and OSPF3 adjacency uptime are more than expected after the NSSU, and outage is higher than expected. PR1551925

MPLS

- Extended-admin-groups on links are shown as the SRLG attribute in TED. PR1575060
- With the local reversion on, there is a possibility of the transit router not informing the headend of RSVP disabled link when the link flaps more than once. PR1576979
- The rpd process generates core file during GRES at **mpls_tunnel_selfID_update ,p2mp_branch_update_selfID ,rsvp_nhop_lookup ,rsvp_change_label_for_appl_p2mp_session**. PR1559022

Network Address Translation (NAT)

- Services NAT mappings and sessions are incorrect while checking the SIP sessions from public to private and RTP from private to public. PR1577922

Platform and Infrastructure

- The MX Series router might drop packets larger than the tunnel interface MTU as tail drops in an egress queue. PR1386350
- The vmxt_lnx process generates a core file at **KtreeSpace::FourWayLeftAttachedNode::getNextDirty Trinity_Ktree::walkSubTree Trinity_Ktree::walkSubTree.** PR1525594
- Upgrading satellite devices might lead to some SDs in the **SyncWait** state. PR1556850
- The BFD session goes down after ISSU switchover. PR1561306

Routing Policy and Firewall Filters

- When upgrading Junos OS to a specific version, the configuration validation might fail and the rpd process might crash. PR1538172

Routing Protocols

- On the MX960 router, the backup path fails to install in the LAN scenario and breaks the SR-MPLS for LAN when more than four end-x SIDs are configured on the interface.

  PR1512174
- The routes are not copied from the transport ribs (junos-rti-tc-200.inet.3) to bgp.transport.3 in the device with transport. PR1556632
- The BGP session flaps might be seen after the Routing Engine switchovers when the VRRP virtual address is used as the local address for the BGP session. PR1576959
- Possible RPD crash with the **routing-options transport-class** configuration during the restart routing is observed. PR1582081
- On the MX960 routers, the next-hop entries in table inet.0 are not as expected when testing the IS-IS policy LFA. PR1558581
- IS-IS adjacency is not as expected when testing the BGP community feature using VRR. PR1559079
- More ssh connections are allowed than the configured ssh connection limit. PR1559305
- The DHCP BFD subscriber session does not come up on the MPC Type 2 card and gets stuck in the **Down** state. PR1572577

Subscriber Access Management

- Subscriber might get stuck in the **Terminating** state if the **Access-Challenge** packet is received from the RADIUS server during the subscriber authentication. PR1583090

User Interface and Configuration

- Commit fails for the backup Routing Engine for the **deactivated mpls lsp priority** command. PR1519367

the

VPNs

- Traffic from the reverse direction might cause traffic loss for up to 1 second with NSR switchover. PR1558395

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for MX Series routers.

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

Resolved Issues: 21.1R1

IN THIS SECTION

EVPN

- **no-arp-suppression** is required for MAC learning across the EVPN domain on the static VTEP. PR1517591
- ARP replies from the CE device gets dropped incorrectly at the PE fdevice or the EVPN routes resolving through MPLS-over-UDP. PR1563802

  The l2ald process might crash under the VLAN-based EVPN-VxLAN scenario. PR1550109
- The BUM traffic might get dropped in the EVPN-VXLAN setup. PR1525888
- The route table shows additional paths for the same EVPN or VXLAN Type 5 destination after upgrading from Junos OS Release 18.4R2-S3 to 19.4R1-S2. PR1534021
- All the ARP reply packets toward some address are flooded across the entire fabric. PR1535515
- The GE LOS alarm logs on the change in **IFF_CCCDOWN** are not logged in the syslog message file. PR1539146

- The rpd memory might leak when the EVPN configuration is changed. PR1540788
- The l2ald process might generate a core file when the EVPN-VXLAN configuration is changed. PR1541904
- The rpd might crash after adding route-target on a dual-Routing Engine system under the EVPN multihoming scenario. PR1546992
- VLAN ID information is missed while installing the EVPN route from the BGP Type 2 Route after modifying a routing instance from instance type EVPN to instance type virtual-switch. PR1547275

Forwarding and Sampling

- The srrd process might crash in a high route churns scenario or if the process flaps. PR1517646
- The l2ald process might crash when a device configuration flaps frequently. PR1529706
- VLAN-ID-based firewall match conditions might not work for the VPLS service. PR1542092
- MAC learning issue might occur when EVPN-VXLAN is enabled. PR1546631
- All traffic is dropped on the aggregated Ethernet bundle without VLAN configuration if bandwidth-percent policer is configured. PR1547184
- The l2ald process might crash due to a next-hop issue in the EVPN-MPLS. PR1548124
- Configuration archive transfer-on-commit fails on Junos OS Release 18.2R3-S6.5. PR1563641

General Routing

- Dynamic tunnel summary displays a wrong count of up and total tunnels. PR1429949
- The riot might crash due to a rare issue if vMX run in the performance mode. PR1534145
- The BFD sessions might not come up in the VXLAN scenario. PR1538600

  </p>

- Unable to show to which shard a given route is hashed. PR1430460
- On the MPC11E line card, the number-of-sub-ports configuration on the 4x10GbE channelized ports might cause the channels to go down. PR1442439
- The MPC2E-NG or MPC3E-NG card with a specific MIC might crash after a high rate of interface flaps. PR1463859

- The following line-card errors are seen:

```
HALP-trinity_nh_dynamic_mcast_add_irb_topo:3520 snooping-error: invlaid IRB
topo/ IRB ifl zero in l2 nh 40495 add IRB.
```

  PR1472222

- Dynamic SR-TE tunnels do not get automatically re-created at the new primary Routing Engine after the Routing Engine switchovers. PR1474397
- Memory utilization enhancement is needed. PR1481151
- Subscribing to **/linecard/packet/usage** and triggering the UDP decoder, the hardware statistics are exported with improper hierarchy. PR1485739
- Prefix is not emitted for the **te-lsp-timers/state/cleanup-delay** sensor path for OCST. PR1500690
- Transit IPv4 traffic forwarding over BGP SR-TE might not work. PR1505592
- The log file to log the activities associated with the **request rift package activate** command is created with the permissions of the user. If multiple users run the command, the command might fail due to the write permission error. PR1514046
- On the MX960 routers, the **show interfaces redundancy rlt0** statement shows current status as **Primary down** as the FPC is still in the **Ready** state after RLT failover (restart FPC). PR1518543
- The BFD session status remains down at the non-anchor FPC even though BFD session is up after the anchor FPC reboots or panic. PR1523537
- The rpd process might crash when the routing-instances are deleted and recreated quickly. PR1562905
- FPC might not be recognized after the power cycle (hard reboot). PR1540107
- No response from the other Routing Engine for the last 2 seconds triggers the following SNMP trap message:

```
Fru Offline
```

  PR1524390

- Problem with static VLAN deletion with active subscribers, and the FPC might be stuck at the **Ready** state during restart. PR1525036

- The following error message is observed during GRES if an IRB interface is configured without a profile:

```
RPD_DYN_CFG_GET_PROF_NAME_FAILED.
```

  PR1526481

- The l2cpd process might crash when removing LLDP on an aggregated Ethernet interface. PR1528856

- The **speed** command cannot be configured under the interface hierarchy on an extended port when the MX204 or MX10003 router works as an aggregation device. PR1529028

- The SFP-LX or SFP-SX optics on MIC-3D-20GE-SFP-E/EH might show as unsupported after ISSU. PR1529844

- The following error message for port might be seen:

```
FAILED(-1) read of SFP eeprom
```

  PR1529939

- On the MX2010 routers, BiDi 1G SFP optics gives wrong value in JVision for **optics/laser_rx_power_*_thresholds**.

  PR1530120

- After performing ISSU with a high-scale bridge-domain configuration, less than 0.0254 percent of traffic loss is observed for a single bridge-domain interface. PR1531051

- On MX204 and MX10003 routers, PEM 0 always shows as absent or empty even if PEM 0 is present. PR1531190

- On the MX150 routers, configuring the **no-flow-control** statement under gigether-options does not work. PR1531983

- Wavelength unlocked alarm is **On** when using SFP+-10G-T-DWDM-ZR optics. PR1532593

- The interface with the **pic-mode 10GE** configuration might not come up if upgraded to Junos OS Release 18.4R3-S4 or later. PR1534281

- Some routes might get incorrectly programmed in the forwarding table in the kernel that are no longer present in rpd. PR1534455

- PTP slave might discard the PTP packets from primary when MPLS explicit-null is configured. PR1547901

- Packets drops might be seen after configuring the PTP transparent clock. PR1530862
- PTP slave might discard the PTP packets from primary when MPLS explicit-null is configured.PR1547901
- The log file of the lcklsyncd process shows empty.PR1567687
- On the ACX710 routers, continuous reboot due to configuration under auxiliary port s observed. PR1580016
- Multiple vmxt processes might generate core files. PR1534641
- The MPLS traffic that passes through the back-to-back PE device topology might match the wrong COS queue. PR1569715
- The following log message might be seen on VM host platform: **/tmp//mpci_info: No such file or directory :error[1]** PR1570135
- SNMP MIB walk for jnxSubscriber OIDs returns a general error message. PR1535754
- All SFBs might go offline due to fabric failure and fabric self-ping probes performing the **disable-pfe** action. PR1535787
- Enhancements are needed to debug l2ald. PR1536530
- The chassisd memory leak might cause traffic loss. PR1537194
- The following error message might be observed when the JAM packages for the MX204, MX10003, and MX10008 routers are installed:

  ```
  AM: Plugin installed for summit_xxx PIC
  ```

  PR1537389
- Version-alias gets missed for subscribers configured with dynamic profiles after ISSU. PR1537512
- Deactivating or activating PTP or SyncE in the upstream router causes the 100GbE links on the LC2103 to flap. PR1538122
- The The MPC10 and MPC11 Packet Forwarding Engine FPCs (MPC10 and MPC11 line cards) Packet Forwarding Engine **show jnh exceptions inst <inst-number>** command might cause the FPC to crash. PR1538138
- Traffic drop might be seen while executing the **request system reboot** command. PR1538252
- The accounting interim-updates for subscriber does not work after GRES and subsequent reboot of FPCs in the node-slicing setup. PR1539474

- The rpd memory might leak on the backup Routing Engine due to link flaps. PR1539601
- The mspmand process leaks memory in relation to the MX Series telemetry, reporting the following error message:

  ```
  RLIMIT_DATA exceed
  ```

  PR1540538
- With hold-time configuration, the ge interfaces remain down on reboot. PR1541382
- Subscriber might not come up on some dynamic VLAN ranges in a subscriber management environment. PR1541796
- The dcpfe process might crash and restart with a dcpfe core file created while running the Type5 EVPN-VXLAN with 2000 VLANs. 1556561
- Packets corruption on 100G or 40G interface is observed when configured with protocol PTP. PR1557758
- During ISSU, BNG losses the subscriber sessions without sending Session Stop but stay in authd. PR1554539
- The l2alm process high CPU utilization might be observed in the EVPN-VxLAN environment. PR1551025
- After changing addresses in the source pool, if the carrier-grade NAT traffic does not stop, the source pool cannot perform the NAT translation from the new pool. PR1542202
- The KRT queue might get stuck after the Routing Engine switchover. PR1542280
- Port mirroring with maximum-packet-length configuration does not work over the GRE interface. PR1542500
- The mspmand process might generate a core file on activating or deactivating the interface. PR1544794
- The riot forwarding daemon might crash on vMX-based platforms configured with an IRB interface. PR1544856
- Traffic loss might be observed when the Switch Fabric Board 3 and MPC8E 3D combination is used in the MX2010 or MX2020 router. PR1544953
- The FPC process might crash during the system booting. PR1545455
- RPD fails to program new routes, and continuous rpd errors might be observed. PR1545463

- Plane offline IPC of chassis-id might time out on MX Series devices with MPC11E line cards. PR1546449
- Unexpected log messages appear related to Neighbor Solicitation (NS) messages with multicast as source address. PR1546501
- Backup Routing Engine vmcore might be seen due to absence of next-hop acknowledgment Infra. PR1547164
- In the syslog output, the **sylog-local-tag** name is truncated as **SYSLOG_SF** when the **sylog-local-tag** name is configured as **SYSLOG_SFW**. PR1547505
- The nsd daemon might crash after configuring inline NAT in USF mode. PR1547647
- **SENSOR APP DWORD** leak is observed during the period of churn for routes bound to the sensor group. PR1547698
- SR-TE might stay up when the routes are deleted through policy. PR1547933
- Multicast traffic drop might be seen after ISSU. PR1548196
- Validation of OCSP certificate might not go through in case of certain CA servers. PR1548268
- Error messages are observed as the backup peer does not send marker acknowledgment for the last 360 seconds for vks 0 slave_ack=0 during ISSU. PR1550492
- The adapted sample rate might be reset to the configured sample rate without changing the sampling rate information in sFlow datagrams after enabling sFlow technology on a new interface. PR1550603
- The rpd might crash when BGP service route is resolved over color-only SR-TE policy. PR1550736
- The PPPoE subscribers might fail to log in. PR1551207
- Slow FPC heap memory might leak due to the flapping of the subscribers terminated over multiple pseudowires. PR1574383
- The Packet Forwarding Engine might get disabled when major CMERROR occurs due to the parity errors. PR1551353
- Disable-pfe with intermittent **ipc_pipe_get_packet(): packet_get()** failed error message and **CM_CMERROR_FABRIC_SELFPING failure** messages are observed. PR1554209

  </para>
- The following error message might be observed.

```
LCM Peer Absent
```

PR1551760

- Fixed Packet Forwarding Engine instance processing in JnhHandleReplicate to honor the Packet Forwarding Engine mask is observed. PR1553400
- Fabric errors are observed and the FPC processes might go offline with SCBE3, MPC3E-NG, or MPC3E line cards and MPC7 or MPC10 line card in the increased-bandwidth fabric mode. PR1553641
- Configuring HFRR (for example, link-protection) on an interface might cause rpd to crash. PR1555866
- Chassisid SNMP trap **Fru Offline** is not generated on MPC11E line card due to no power. PR1556090
- ISSU might be aborted on the MX Series devices for Junos OS Release 20.2R2-S1. PR1557413
- On the MX150 routers, the following continuous license error is observed:

```
[licinfra_set_usage_nextgen_async:1733] Invalid input parameters.
```

  PR1559361
- On the MX960 routers, mismatch between YANG schema and RPC output are observed. PR1559810
- When the system has only one plane (in the process of plane offline or online), the MPC10-10c line card displays a destination error. PR1560053
- The **request system software validate** command might corrupt installation of junos-openconfiguration package. PR1560234
- On the MX240 routers, R0 overlay ping fails. PR1560408
- The l2cpd process might generate a core file on reboot. PR1561235
- On the MX240 routers, the VIA headers do not change properly when the SIP ALG is enabled. PR1561312
- Traffic drop might occur on all platforms running Junos OS when a GRE-based dynamic tunnel is configured. PR1561721
- The rpd might crash during processing huge amount of PIM prune messages. PR1561984

- The following error message might be seen after ISSU:

  ```
  Turbotx process not running
  ```

  PR1564418

- The PPPoE service-name-tables do not correctly count active sessions matching the agent-specifier aci/ari used for delay. PR1565258

- The MX204 FPC might show high CPU utilization because the JGCI background thread runs for a long period. PR1567797

- On the MX150 routers, the **request system software add** command is disabled in Junos OS Release 19.4R3-S1, 20.1R2, and 20.4R1. PR1568273

- The rpd might crash while using BFD API to bring up BFD sessions. PR1569040

- The agent sensor **__default_fabric_sensor__** seems to be partly applied to some FPCs, which causes the following zero payload issue:

  ```
  AGENTD received empty payload for pfe sensor __default_fabric_sensor__
  ```

  PR1569167

- GRE OAM keepalive fails to start after the Packet Forwarding Engine reboots. PR1569790

- Fabric errors are observed on a system with MPC3E line cards and MPC4E or MPC5E line card with enhanced MX960 backplane. PR1573360

- DHCP discover packet might be dropped if the DHCP inform packet is received first. PR1542400

- The **show dynamic-profile session client-id** command displays only one IPv6 framed-route information. PR1555476

- On the MX2010 routers, many chassid and fabric related errors are observed after ZPL ISSU. PR1558626

- On the MX480 routers, the MPC10E line cards are restarted after performing GRES with scaled configurations. PR1561259

- On the MX2020 and MX960 routers, the PTP state gets stuck in the **Acquiring** state. PR1562267

- On the MX2010 routers, the aft-ulcd process crashes and generates core files continuously and SLC keeps restarting after upgrade. PR1578191

- On the MX480 routers, the expected DDoS Routing Engine violations are not observed on the MPC10E. PR1579319

- On the MX2020 routers, the **ISSU RECONNECT TIMEOUT** error message is observed on the MPC6E line crads due to which the dark window size is more than expected.PR1580658

- On the MX960 routers, the R0 overlay ping fails with the following error message: **tunnel-src 1.1.1.1 tunnel-dst 7.7.7.7 vni 1 count 1, invalid VNI: '1'**.PR1580918

- On the MX480 routers, the STP topology changes after ISSU with VSTP configuration. PR1581080

- The interface might not be added to BD after the VLAN change. PR1504374

Interfaces and Chassis

- The configuration might not be applied after deleting all existing logical interfaces and adding a new logical interface for a physical interface (IFD) in a single commit. PR1534787

- The following errors are generated during GRES: **VRRPMAN_PATRICIA_GROUP_ADD_FAIL: vrrp_ifcm_send_bulk: Failed to add group to patricia tree key** and **VRRPMAN_ENTRY_KEY_PRESENT: vrrp_ifcm_send_bulk: Already an entry present with the key**. PR1575689

- Inline Y.1731 SLM or DM does not work in the enhanced-cfm-mode for the EVPN up MEP scenario. PR1537381

- The following error message might be seen after commit for configuration under interface hierarchy:

  ```
  should have at least one member link on a different fpc.
  ```

  PR1539719

- The following commit error is observed while trying to delete unit 1 logical systems interfaces: ae2.1:

  ```
  Only unit 0 is valid for this encapsulation.
  ```

  PR1547853

- The startup-silent-period command might not work in Junos OS Release 20.3R1 or later. PR1548464

- The VCP port is marked as administratively down on the wrong MX-VC member. PR1552588

- The dcd process might leak memory on pushing the configuration to the ephemeral database. PR1553148

- On the MX960 routers, sessions are flapped after applying the action profile on the router. PR1561044

- The input errors counter on the monitor interface CLI does not work. PR1561065

- MAC address entry issue might be seen after the MC-LAG interface fails or falls back. PR1562535

- Traffic loss might be seen while verifying VRRP State Machine functionality. PR1564551

Juniper Extension Toolkit (JET)

- TCP connection might not be established while creating the default gRPC channel with **fw_channel** name. PR1559064.

Layer 2 Ethernet Services

- The copying of files to the RCB over WAN ports is slow. PR1496895

- The **show dhcp relay statistics** command displays **DHCPLEASEUNASSIGNED** instead of **DHCPLEASEUNASSINGED**, which is a spelling error. PR1512239

- DHCP packet might drop when DHCP relay is configured on the leaf device. PR1554992

- jnxJdhcpLocalServerMacAddress (.1.3.6.1.4.1.2636.3.61.61.1.4.3) returns incorrect format of MAC address. PR1565540

- The Option 82 information are incorrectly cleared by the DHCP Relay Agent. PR1568344

  </p>

MPLS

- Traffic loss might be observed due to rpd crash in the MPLS scenario. PR1528460

- MPLS LSP on transit has double entries. PR1533161

- The rpd process might crash when the LDP route with indirect next hop is deleted on the aggregated Ethernet interface. PR1538124

- Committing might trigger externally provisioned LSP MBB mechanism. PR1546824

- A new LSP might not be up even if the bypass LSP is up and **setup-protection** is configured. PR1555774

Network Management and Monitoring

- Commit error while deleting the routing instance when SNMP trap-group also has the same routing instance referred. PR1555563
- The trace-relay process generates core files. PR1556040
- After the l2cpd service is restarted, the context of registration from l2cpd to snmpd was failing due to incorrect reinitialization. Because of this, if an NMS polls the dot1dStp objects by prefixing the context might fail. As a workaround, restart snmpd or reconfigure the protocols hierarchy. PR1561736

Platform and Infrastructure

- PE-CE OAM CFM might have issues in the aggregated Ethernet interface. PR1501656
- The following major error might cause Packet Forwarding Engine(s) to disable: **XQ_CMERROR_SCHED_L3_PERR_ERR** PR1538960
- An internal timer on the backup Routing Engine might cause an ARP storm upon GRES switchover on the new primary Routing Engine. PR1547583
- The state of the flow detection configuration might not be displayed properly if DDoS-SCFD is configured globally. PR1519887
- The following error message is observed when the alarms resets after interface:

  ```
  7836 ifl 567 chan_index 8 NOENT & jnh_ifl_topo_handler_pfe(13015): ifl=567
  err=1 updating channel table nexthop.
  ```

  PR1525824
- The VXLAN encapsulation over IPv6 underlay might not work. PR1532144
- The PPE error messages or traps might be observed in the Layer 2 flooding scenarios. PR1533767
- The fpc process might crash when the next-hop memory of ASIC is exhausted in an EVPN-MPLS scenario. PR1533857
- The ISSU might fail on platforms running Junos OS with LU chip-based line cards. PR1535745
- Subscribers do not come up with VPLS on ps interface. PR1536043
- Packet loss might be observed when the RFC2544 egress reflector session is configured on the nonzero Packet Forwarding Ethernet interface. PR1538417

- The vmxt_lnx process generates a core file at **l2_metro_bd_host_inject_del bd_platform_delete bd_handle_msg**. PR1538516
- The rmopd process might leak memory if the TWAMP client is configured. PR1541808
- FPC might crash when the underlying Layer 2 interface for ARP over IRB interface is changed from the physical interface to the LSI interface. PR1542211
- ARP expired timer on the backup Routing Engine is not the same as on the primary Routing Engine if aging-timer is configured. PR1544398
- The kernel might crash if GRES is performed in either a new iteration or after swapping the Routing Engine and restoring the HA configuration. PR1549656
- The BGP session replication might fail to start after the session crashes on the backup Routing Engine. PR1552603
- Traffic is not forwarded over IRB to l2circuit on lt interfaces. PR1554908
- IPv4 EXP rewrite might not work properly when inet IPv6-VPN is enabled. PR1559018
- DHCPv4 request packets might be wrongly dropped during DDoS attacks. PR1562474
- The **enforce-strict-scale-limit-license** configuration enforces subscriber license incorrectly and the following error message is observed:

  ```
  / PADS:"AC-System-Error - No resources"
  ```

  PR1563975
- The BUM frame might be duplicated on an aggregate device if the extended-port on the Satellite device is an aggregated Ethernet interface. PR1560788
- The **IIF-LIST APP DWORD** leak is observed during the period of churn for the NGMVPN-MoFRR routes with sender-based-rpf enabled. PR1548806

Routing Policy and Firewall Filters

- For setting the IPv6 router ID, the **routing-options** statement is added. PR1523283
- The RPD process generates core file at **task_block_alloc_jemalloc isis_spring_stats_jobinfo_alloc isis_spring_stats_show_traffic_stats**. PR1579830
- The policy configuration might be mismatched between the rpd and mgd processes when deactivate policy-options prefix-list is involved in the configuration sequence. PR1523891

- The generated route goes into the **Hidden** state when the **protect core** statement is enabled. PR1562867

- Global variable policy_db_type do not set the correct value on failure. PR1561931

Routing Protocols

- The BFD session might get stuck in the **Init** or **Down** state after the BFD session flaps. PR1474521

- With BGP rib-sharding enabled, RPD memory might exhaust PR1546347

  </para>

- Traffic might be lost during mirror data transmit from the primary ppmd/bfdd. PR1570228

- VRF table does not get refreshed after changing to **maximum-prefixes** in the VRF. PR1564964

- Traffic loss might occur during VRF route resolution over indirect nexthop. PR1525363

- The rpd might crash with BGP RPKI enabled in a race condition. PR1487486

- The virtual-router option is not supported under a routing instance in a lean rpd image. PR1494029

- Some PIM join or prune packets might not be processed in the first attempt in the scale scenario where the PIM routers establish neighborship and immediately join the multicast group. PR1500125

- Traffic might be silently discarded when the clear bgp neighbor all command is executed on a router and also on the corresponding route reflector in succession. PR1514966

- The BGP session with VRRP virtual address might not come up after a flap. PR1523075

- The VRF label is not assigned at ASBR when the inter-AS is implemented. PR1523896

- The rpd process generates a core file at **is_srv6_delete_locator_end_sid_data isis_srv6_end_sid_local_data_delete isis_srv6_locator_config_check**. PR1531830

- Transit labels for Layer 3 VPN routes are pushed momentarily to the MPLS.0 table. PR1532414

- Configuring then next hop and then reject on a route policy for the same route might cause the rpd process to crash. PR1538491

- After the peer is moved out of the protection group, the path protection is not removed from the PE device. The multipath route is still present. PR1538956

- The rpd process generates a core file at **gp_rtarget_tsi_update,bgp_rtarget_flash_rt,bgp_rtarget_flash**. PR1541768

- Traffic loss might be seen in next-hop-based dynamic tunnels of the Layer 3 VPN scenario after changing the dynamic-tunnel preference. PR1542123

- Continuous rpd crash might be observed if a static group is added to the PIM protocol. PR1542573
- The metric of prefixes in intra-area-prefix LSA might be changed to 65535 when the metric of one of the OSPFv3 P2P interfaces is set to 65535. PR1543147
- IS-IS does not call ted_add_halflink for P2P IPv6-only links for traffic engineering topology. PR1548506
- Telemetry key value for transport or remote-address field for link-local IPv6 peer is incorrect, and logical interface is absent. PR1548754
- The BGP session neighbor shutdown configuration does not affect the non-established peer. PR1554569
- The changes are not effective when the values are set under static default hierarchy. PR1555187
- The BGP session might not come up if **extended-nexthop** is enabled by default on the other vendor remote peer. PR1555288
- Sending multicast traffic to downstream receiver on Virtual Chassis platforms might fail. PR1555518
- Six PE device prefixes might not be removed from the RIB upon reception of withdrawal from a BGP neighbor when RIB sharding is enabled. PR1556271
- Multipath information still shown for BGP route even after disabling interface for one path. PR1557604
- Extra node-spring-algorithm-type is displayed under the **show route table lsdist.0 te-node-iso <> extensive** command. PR1560003
- VPN routes learned from core were not advertised to the CE devices when BGP sharding is configured. PR1560661
- All Layer 3 VPN route ages reset when a VRF is added or deleted. PR1560827
- Duplicate LSP next hop is shown on inet.0, inet.3, and mpls.0 route table when OSPF traffic-engineering shortcuts and MPLS **bgp-igp-both-ribs** are enabled. PR1561207
- Wrong SPF calculation might be observed for OSPF with ldp-synchronization hold-time configured after interface flaps. PR1561414
- BGP routes might be stuck in routing table in the **Accepted DeletePending** state when the BGP peering session goes down. PR1562090
- The rpd might crash on the backup Routing Engine after rpd restart is triggered on the primary Routing Engine. PR1563350
- SNMP MIB OSPFv3NbrState returns a drifted value. PR1571473

Services Applications

- L2TP subscribers might fail to establish a session on the MX Series device if the CPE is a virtual host. PR1527343
- The following error message is observed:

```
SPD_CONN_OPEN_FAILURE: spd_pre_fetch_query: unable to open connection to
si-1/0/0.
```

  PR1550035

User Interface and Configuration

- The **verbose** command unexpectedly becomes hidden after Junos OS Release 16.1 for **set system export-format json**. PR1547693
- The **request system software validate on host** command does not validate the correct configuration file. PR1553577
- The configuration under groups stanza is not inherited properly. PR1529989
- Removing the flash component from Monitor > Interfaces and DHCP pages, removes the other flash pages. PR1553176
- The firewall filter for both IPv4 and IPv6 might not work when it is applied through apply-groups. PR1534858
- The JNH memory might leak on the Trio-based line cards. PR1542882

VPNs

- The PIM (S,G) join state might stay forever when there are no MC receivers and the source is inactive. PR1536903 <url
- MVPN multicast route entry might not be properly updated with the actual downstream interfaces list. PR1546739

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

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

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

Basic Procedure for Upgrading to Release 21.1R1

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

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

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

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

Procedure to Upgrade to FreeBSD 11.x-Based Junos OS

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

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

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

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

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

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

4. Select the Software tab.

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

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

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

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

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

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

    - For 32-bit Routing Engine version:

    ```
    user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-20.4R1.9-signed.tgz
    ```

    - For 64-bit Routing Engine version:

    ```
    user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-20.4R1.9-signed.tgz
    ```

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

    - For 32-bit Routing Engine version:

    ```
    user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-20.4R1.x-limited.tgz
    ```

    - For 64-bit Routing Engine version:

    ```
    user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-20.4R1.9-limited.tgz
    ```

    Replace source with one of the following values:

    - */pathname*—For a software package that is installed from a local directory on the router.

- For software packages that are downloaded and installed from a remote location:
  - **ftp://** ***hostname/ pathname***
  - **http://** ***hostname/ pathname***
  - **scp://** ***hostname/ pathname***

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

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

Rebooting occurs only if the upgrade is successful.

NOTE:

- You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the **request vmhost software add** command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.
- Starting in Junos OS Release 21.1R1, in order to install a VM host image based on Wind River Linux 9, you must upgrade the i40e NVM firmware on the following MX Series routers:
  - MX240, MX480, MX960, MX2010, MX2020, MX2008, MX10016, and MX10008

  [See https://kb.juniper.net/TSB17603.]

NOTE: After you install a Junos OS Release 21.1R1 jinstall package, you cannot return to the previously installed Junos OS (FreeBSD 6.x) software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add no-validate** command and specify the jinstall package that corresponds to the previously installed software.

NOTE: Most of the existing **request system** commands are not supported on routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. See the VM Host Software Administrative Commands in the Installation and Upgrade Guide.

Procedure to Upgrade to FreeBSD 6.x-Based Junos OS

Products impacted: MX5, MX10, MX40, MX80, MX104.

To download and install FreeBSD 6.x-based Junos OS:

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

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

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

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

4. Select the Software tab.

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

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

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

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

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

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

  ```
  user@host> request system software add validate reboot source/jinstall-ppc-20.4R1.9-signed.tgz
  ```

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

  ```
  user@host> request system software add validate reboot source/jinstall-ppc-20.4R1.9-limited-signed.tgz
  ```

Replace source with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 21.1R1 jinstall package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the jinstall package that corresponds to the previously installed software.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

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

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

Upgrading a Router with Redundant Routing Engines

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

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine, and save the configuration change to both Routing Engines.

2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.

3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.

4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

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

Downgrading from Release 21.1R1

To downgrade from Release 21.1R1 to another supported release, follow the procedure for upgrading, but replace the 21.1R1 jinstall package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases.

For more information, see the Installation and Upgrade Guide.

Junos OS Release Notes for NFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for the NFX Series Network Services Platforms. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

What's New in 21.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for the NFX Series.

Application Identification (AppID)

- **Application signature package enhancements (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 21.1R1, we've enhanced the application signature package by grouping all newly added signatures under the junos:all-new-apps group. When you download the application signature package on your device, the predefined application group is downloaded. You can use this application group in the security policy configuration.

  We've also introduced a list of application tags, based on attributes, in the application signature package. You can group similar applications based on these predefined tags. By doing so, you can consistently reuse the application groups when you define security policies.

  [See Predefined Application Signatures for Application Identification.]

- **Enhancements to packet capture of unknown applications (NFX Series, SRX Series, and vSRX)**—

Starting in Junos OS Release 21.1R1, your security device stores the packet capture of unknown

applications' details per session. As a result of this change, the packet capture (.pcap) file now includes the session ID in the filename. We now store the file in **destination-IP-address.destination-port.protocol.session-id.pcap** format in the **/var/log/pcap** location. (Previously, the packet capture file was saved in **destination-IP-address. destination-port.protocol.pcap** format.)

In addition, we've enhanced packet capture of unknown application functionality to capture unknown Server Name Indication (SNI) details.

[See Packet Capture of Unknown Application Traffic Overview.]

- **Application signature enhancements (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 21.1R1, we've introduced the following enhancements to application signatures:
  - Support for FTP data context propagation
  - Skipping of deep packet inspection (DPI) for the sessions offloaded by advanced policy-based routing (APBR) on application system cache (ASC) hit (when only APBR service is enabled).
  - Forceful installation of the application signature pack over the same version of signature pack.
  - Display (in the CLI command output) of the application signature pack release date.
  - Display (in the CLI command output) of the list of deprecated application signatures available in the installed signature pack.

  [See Predefined Application Signatures for Application Identification.]

Architecture

- **Custom mode (NFX250 NextGen and NFX350 devices)**—Starting in Junos OS Release 21.1R1, you can define and specify a custom-mode template for NFX250 NextGen and NFX350 devices. The custom mode provides an option to allocate resources to Layer 3 data plane and Network Functions Virtualization (NFV) backplane.
  [See NFX350 Overview and NFX250 NextGen Overview.]

Flow-Based and Packet-Based Processing

- **Support for PowerMode IPsec (PMI) solution (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800 with SPC3 cards, vSRX, and vSRX3.0) and GRE acceleration solution (SRX Series and NFX Series)**—Starting in Junos OS Release 21.1R1, we support the PMI and GRE acceleration solutions to improve the software-defined WAN (SD-WAN) performance.

Table 8: Solutions and Details

Solution	How to Enable?
PMI	Include the **power-mode-ipsec** and **gre-performance-acceleration** statements at the **[edit security flow]** hierarchy level. **NOTE**: PMI supports both IPsec and GRE. In this case, traffic flows through the PMI data path.
GRE acceleration	Include the **gre-performance-acceleration** statement at the **[edit security flow]** hierarchy level. **NOTE**: By default, **gre-performance-acceleration** is turned off. In this case, traffic flows through the GRE acceleration data path.

[See gre-performance-acceleration (Security Flow), flow (Security Flow), and show security flow status.]

Intrusion Detection and Prevention

- **Support for Perl-compatible regular expression (PCRE) version 8.40 (SRX Series and NFX Series)**—Starting in Junos OS Release 21.1R1, we've upgraded the codebase of intrusion detection and prevention (IDP) from PCRE version 5.40 to PCRE version 8.40. As PCRE version 8.40 supports new regex constructs, this upgrade enhances the capability of Junos OS IDP attack signatures to match regular expressions. With this upgrade, we've also addressed security vulnerabilities in the Junos OS PCRE codebase.

  [See pattern-pcre (Security IDP).]

- **Support for Snort IPS signatures (SRX Series and NFX Series)**—Starting in Junos OS Release 21.1R1, Juniper Networks IDP supports Snort IPS signatures. IDP secures your network by using signatures that help to detect attacks. Snort is an open-source intrusion prevention system (IPS). You can convert the Snort IPS rules into Juniper IDP custom attack signatures using the Juniper Integration of Snort Tool (JIST). These rules help detect malicious attacks.

  - JIST is included in Junos OS by default. The tool supports Snort version 2 and version 3 rules.

  - JIST converts the Snort rules with snort-ids into equivalent custom attack signatures on Junos OS with respective snort-ids as the custom attack names.

- When you run the **request** command with Snort IPS rules, JIST generates **set** commands equivalent to the Snort IPS rules. Use the **request security idp jist-conversion** command to generate the **set** commands as CLI output. To load the **set** commands, use the **load set terminal** statement or copy and paste the commands in the configuration mode, and then commit. You can then configure the existing IDP policy with the converted custom attack signatures.

- All the Snort IPS rule files that didn't get converted are written to **/tmp/jist-failed.rules**. The error log files generated during the conversion are written to **/tmp/jist-error.log**.

- To view the jist-package version, use the **show security idp jist-package-version** command.

[See Understanding Snort IPS Signatures, request security idp jist-conversion , and show security idp jist-package-version .]

Platform and Infrastructure

- **Transfer files from USB (NFX150, NFX250 NextGen, and NFX350 devices)**—Starting in Junos OS Release 21.1R1, you can transfer files from USB to NFX devices by enabling the USB pass-through feature. To enable this feature, use the **set system services usb-pass-through** command. Built-in LTE functionality does not work after you enable the USB pass-through feature.

  [See Supporting File Transfer from USB on NFX150 Devices, Supporting File Transfer from USB on NFX250 NextGen Devices, and Supporting File Transfer from USB on NFX350 Devices]

- **Virtual port peering (NFX250 NextGen and NFX350 devices)**—Starting in Junos OS Release 21.1R1, you can configure the virtual port peering (VPP) feature to map a physical port and an interface to a virtualized network function (VNF), so that if the physical interface becomes inactive, the corresponding virtual interface also becomes inactive and the status of the physical interface is communicated to the virtual interface.

  The VPP feature is supported only on the Network Functions Virtualization (NFV) backplane.

  [See Configuring VNFs on NFX350 Devices and Configuring VNFs on NFX250 NextGen Devices.]

What's Changed

IN THIS SECTION

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

What's Changed in Release 21.1R1

IN THIS SECTION

Network Management and Monitoring

- **Support for disconnecting unresponsive NETCONF-over-SSH clients (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—You can enable devices to automatically disconnect unresponsive NETCONF-over-SSH clients by configuring the **client-alive-interval** and **client-alive-count-max** statements at the **[edit system services netconf ssh]** hierarchy level. The **client-alive-interval** statement specifies the timeout interval in seconds, after which, if no data has been received from the client, the device requests a response. The **client-alive-count-max** statement specifies the threshold of missed client-alive responses that triggers the device to disconnect the client, thereby terminating the NETCONF session.

  [See ssh (NETCONF).]

Known Limitations

Learn about known limitations in this release for NFX Series devices.

There are no changes in behavior or syntax in Junos OS Release 21.1R1 for NFX Series devices.

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

Open Issues

IN THIS SECTION

Learn about open issues in this release for NFX Series devices.

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

High Availability

- On an NFX350 chassis cluster, when FPC0 (when node0 is primary) or FPC7 (when node1 is primary) is restarted by either using the **request chassis fpc slot *slot* restart node local** command or due to dcpfe core files on the primary, it restarts FPC1 or FPC8. This might break the preexisting TCP sessions and fail to restart the TCP sessions. The TCP sessions might require a manual restart. PR1557607

Interfaces

- When you run a **show interface** command on NFX150 devices to check the interface details, the system does not check whether the interface name provided is valid or invalid. The system does not generate an error message if the interface name is invalid. PR1306191
- On NFX350 devices, when you run the **show interfaces queue** command on the gr-1/0/0 interface, the **Egress queue statistics are not applicable to this interface.** error message appears. Due to this error, interface queue statistics might not be available for the gr-1/0/0 interface. PR1530855

Platform and Infrastructure

- On NFX150 devices, when J-Flow v5 is configured and the J-Flow v5 server is reachable through an IPsec tunnel, and the MTU size of this IPsec tunnel is configured as 1500, the J-Flow packets are not generated on NFX Series devices. As a workaround, use J-Flow v9 or IPFIX version, instead of J-Flow v5, to enable the J-Flow functionality on NFX Series devices. PR1539964

Virtual Network Functions (VNFs)

- On NFX150 devices, before reusing a VF to Layer 3 data plane interfaces (for example, ge-1/0/3), which was earlier allocated to a VNF, you must restart the system. PR1512331

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 21.1R1

IN THIS SECTION

High Availability

- On NFX150 devices, upgrade from Junos OS Release 19.4 to Junos OS Release 20.2 fails and the **/usr/sbin/boot_mgmt_fsm: line 40: echo: write error: No space left on device issue** message is displayed. PR1532334

Interfaces

- On NFX250 devices, a VNF interface is not brought down when the VNF interface is mapped to an already link down or disabled peer physical interface. PR1555193

- Analyzer on OVS fails to mirror packets after a system reboot on a DPDK-enabled device. PR1480290

- On NFX Series devices, the following error message for interfaces might be seen: **FAILED(-1) read of SFP eeprom.** PR1529939

Performance Modes

- A message is provided in syslog if reboot is required for the mode modification to take effect in custom mode. PR1555465

Platform and Infrastructure

- On NFX150, NFX250 NextGen, and NFX350 devices, the **EmulatorPin CPUSet** option does not get configured, which might result in vCPU running on a higher level up to 100%. PR1540564

- On NFX350 devices and the SRX5000 line of devices with SPC3 card, the DPD Gateway failover feature is not supported. PR1564715

- The l2cpd core files might be seen on reboot. PR1561235

- The DSL SFP firmware cannot finish upgrade successfully through vmhost reboot. PR1547540

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

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

Basic Procedure for Upgrading to Release 21.1

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

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

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

To download and install Junos OS Release 21.1R1:

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

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

2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the **Software** tab.
4. Select the release number (the number of the software version that you want to download) from the Version drop-down list to the right of the Download Software page.
5. In the Install Package section of the Software tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the device or to your internal software distribution site.
10. Install the new package on the device.

Junos OS Release Notes for PTX Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

What's New in 21.1R1

IN THIS SECTION

Learn about new features or enhancements to existing features in this release for the PTX Series.

High Availability

- **Support for VRRP (PTX1000, PTX10002, PTX10008, and PTX10016)**—Starting in Junos OS Release 21.1R1, PTX1000, PTX10002, PTX10008, and PTX10016 routers support VRRP. However, these routers do not support the following VRRP features:

  - VRRP on IRB
  - Dual tagging
  - GRES
  - VRRP on logical tunnel (LT) interfaces
  - Layer 2 VRRP

  [See Understanding VRRP.]

MPLS

- **Nonstop active routing (NSR) support for controller-initiated RSVP label-switched paths (LSPs) (MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.1R1, we support NSR for controller-initiated RSVP-based point-to-point (P2P) and point-to-multipoint (P2MP) LSPs. The primary Routing Engine synchronizes all RSVP LSPs initiated by Path Computation Elements (PCEs), including multicast flow specifications for any PCE-initiated P2MP LSPs, with the backup Routing Engine. This ensures zero traffic loss for the traffic carried over PCE-initiated RSVP LSPs during Routing Engine switchovers. This feature is enabled when NSR is configured.

  [See PCEP Configuration.]

- **New transport class-based architecture to facilitate service mapping over colored tunnels (ACX Series, PTX Series, MX Series)**—Starting in Junos OS Release 21.1R1, you can classify colored transport tunnels (RSVP, IS-IS flexible algorithm) in your network into transport classes and map service routes over an intended transport class. You can also extend the transport tunnels to span across multiple domains (ASs or IGP areas) by using the new BGP transport address family called BGP Classful Transport (BGP CT).

  This feature lays the foundation for network slicing and allows the different domains to interoperate irrespective of the transport signaling protocols used in each domain.

  [See https://www.juniper.net/documentation/us/en/software/junos/mpls/topics/topic-map/mpls-traffic-engineering-configuration.html#id_pjt_vxq_2pb.]

Network Management and Monitoring

- **Operational command RPCs support returning JSON and XML output in minified format in NETCONF sessions (ACX1000, ACX1100, ACX2100, ACX4000, ACX5048, ACX5096, ACX5448, EX2300, EX2500, EX3400, EX4300, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48P, EX4400-48T, EX4600, EX4650, EX9200, MX104, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10001, PTX10002, PTX10008, PTX10016, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX10002, QFX10002-60C, QFX10008, QFX10016, SRX550, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, operational command RPCs, including the **<get-configuration>** RPC, support the **format="json-minified"** and **format="xml-minified"** attributes in NETCONF sessions to return JSON or XML output in minified format. Minified format removes any characters that are not required for computer processing—for example, unnecessary spaces, tabs, and newlines. Minified format decreases the size of the data, and as a result, can reduce transport costs as well as data delivery and processing times.

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

- **sFlow support for IP-IP traffic (PTX1000, PTX10008, and QFX10002)**—Starting in Junos OS Release 21.1R1, you can use sFlow technology to sample IP over IP (IP-IP) traffic on a physical port. sFlow sampling is supported for IP-IP tunnels that have an IPv4 outer header that carry IPv4 or IPv6 traffic. You can use sFlow monitoring technology to randomly sample network packets from IP-IP tunnels and to send the samples to a destination collector for monitoring. Devices that act as an IP-IP tunnel entry point, transit device, or tunnel endpoint support sFlow sampling.

  [See Overview of sFlow Technology and Configuring IP Tunnel Interfaces.]

Routing Protocols

- **Support for configuring multiple independent IGP instances of IS-IS (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.1R1, you can configure and run multiple independent IGP instances of IS-IS simultaneously on a router.

  > **NOTE**: Junos OS does not support configuring the same logical interface in multiple IGP instances of IS-IS.

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

- **Support for IP forward backup path for BGP-LS peer SIDs (PTX Series)**—Starting in Junos OS Release 21.1R1, you can configure an IP forward backup path that provides protection at the local node or the point of local repair for egress peer engineering. When the primary segment goes down, the packet is forwarded to the configured IP backup path. This IP forward backup path has local node significance only. BGP does not send the IP forward backup path information to the controller in its periodic BGP Link State (BGP-LS) updates. If you have configured both segment protection and IP forward backup path, then backup segment protection takes precedence over the IP forward backup path protection.

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

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

- **Support for BGP Auto-discovered Neighbor (MX Series, PTX1000, PTX10008, QFX5120-32C, QFX5200, QFX5210, and QFX10008)**—Starting in Junos OS Release 21.1R1, we support BGP auto-discovered neighbors using IPv6 Neighbor Discovery Protocol (ND). With this feature, you can enable BGP to create peer neighbor sessions using link-local IPv6 addresses of directly connected neighbor devices. You need not specify remote or local neighbor IP addresses.

  To enable peering for a given interface or set of interfaces without specifying the local or remote neighbor addresses, configure the **peer-auto-discovery** statement at the [**edit fabric protocols bgp group <*name*> dynamic-neighbor <*name*>**] hierarchy level.

  [See BGP Auto-Discovered Neighbors, and peer-auto-discovery.]

Segment Routing

- **Support for flexible algorithm in OSPFv2 for segment routing traffic engineering (ACX Series, MX Series, and PTX Series)**—Starting in Junos OS Release 21.1R1, you can thin-slice a network by defining flexible algorithms that compute paths using different parameters and link constraints based on your requirements. For example, you can define a flexible algorithm that computes a path to minimize IGP metric and define another flexible algorithm to compute a path based on traffic engineering metric to divide the network into separate planes. This feature allows networks without a controller to configure traffic engineering and utilize segment routing capability of a device.

  To define a flexible algorithm, include the **flex-algorithm** statement at the **[edit routing-options]** hierarchy level.

  To configure a device to participate in a flexible algorithm, include the **flex-algorithm** statement at the **[edit protocols ospf source-packet-routing]** hierarchy level.

  [See How to Configure Flexible Algorithms in OSPF for Segment Routing Traffic Engineering.]

- **Support for strict SPF and IGP shortcut (ACX710, MX960, MX10008, MX2020, PTX5000, and PTX1000)**—Starting in Junos OS Release 21.1R1, you can configure segment routing algorithm 1 (strict SPF) and advertise its SIDs in IS-IS link-state PDU (LSPDU) and use these SIDs to create SR-TE tunnels to forward the traffic by using the shortest IGP path to reach the tunnel endpoint while avoiding loops. You can also specify a set of prefixes in the import policy, based on which the tunnel can redirect the traffic to a certain destination. You can use algorithm 1 (strict SPF) along with algorithm 0 (default SPF) by default when Source Packet Routing in Networking (SPRING) is enabled.

[See How to Enable Strict SPF SIDs and IGP Shortcut, prefix-segment, and source-packet-routing.]

Services Applications

- **Support for inline active flow monitoring (PTX10008 and PTX10016)**—Starting in Junos OS Release 21.1R1, we support inline active flow monitoring for the PTX10K-LC1105 line card. Inline active flow monitoring supports version 9 and IPFIX flow collection templates. Both the IPFIX and the version 9 templates are supported for IPv4, IPv6, and MPLS, and use UDP as the transport protocol.

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

What's Changed

IN THIS SECTION

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

What's Changed in Release 21.1R1

IN THIS SECTION

General Routing

- **Change in severity of fabric output CRC errors (PTX5000)**—We've reduced the severity of fabric output CRC errors from fatal to minor. With this change, the fabric output CRC errors (CMERROR_TQ_FO_CRC) no longer cause the Packet Forwarding Engines to be disabled.

Junos XML API and Scripting

- **The jcs:invoke() function supports suppression of root login and logout events in system log files for SLAX commit scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The **jcs:invoke()** extension function supports the **no-login-logout** parameter in SLAX commit scripts. If you include the parameter, the function does not generate and log UI_LOGIN_EVENT and UI_LOGOUT_EVENT messages when the script logs in as root to execute the specified remote procedure call (RPC). If you omit the parameter, the function behaves as in earlier releases in which the root UI_LOGIN_EVENT and UI_LOGOUT_EVENT messages are included in system log files.

  [See invoke() Function (SLAX and XSLT).]

- **The jcs:invoke() function supports suppression of root login and logout events in system log files for SLAX event scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The **jcs:invoke()** extension function supports the **no-login-logout** parameter in SLAX event scripts. If you include the parameter, the function does not generate and log UI_LOGIN_EVENT and UI_LOGOUT_EVENT messages when the script logs in as root to execute the specified remote procedure call (RPC). If you omit the parameter, the function behaves as in earlier releases in which the root UI_LOGIN_EVENT and UI_LOGOUT_EVENT messages are included in system log files.

  [See invoke() Function (SLAX and XSLT).]

- **Python 2.7 deprecation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, devices running Junos OS no longer support Python 2.7. We've deprecated the corresponding **language python** statement at the **[edit system scripts]** hierarchy level. To execute Python scripts, configure the **language python3** statement at the **[edit system scripts]** hierarchy level to execute the scripts using Python 3.

  [See Understanding Python Automation Scripts for Devices Running Junos OS.]

Network Management and Monitoring

- **Support for disconnecting unresponsive NETCONF-over-SSH clients (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—You can enable devices to automatically disconnect unresponsive NETCONF-over-SSH clients by configuring the **client-alive-interval** and **client-alive-count-max** statements at the **[edit system services netconf ssh]** hierarchy level. The **client-alive-interval** statement specifies the timeout interval in seconds, after which, if no data has been received from the client, the device requests a response. The **client-alive-count-max** statement specifies the threshold of missed client-alive responses that triggers the device to disconnect the client, thereby terminating the NETCONF session.

[See ssh (NETCONF).]

- **Support for specifying the YANG modules to advertise in the NETCONF capabilities and supported schema list (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—You can configure devices to emit third-party, standard, and Junos OS native YANG modules in the capabilities exchange of a NETCONF session by configuring the appropriate statements at the **[edit system services netconf hello-message yang-module-capabilities]** hierarchy level. In addition, you can specify the YANG schemas that the NETCONF server should include in its list of supported schemas by configuring the appropriate statements at the **[edit system services netconf netconf-monitoring netconf-state-schemas]** hierarchy level.

  [See hello-message and netconf-monitoring.]

User Interface and Configuration

- **Verbose format option to export JSON configuration data (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The Junos OS CLI exposes the **verbose** statement at the **[edit system export-format json]** hierarchy level. We changed the default format to export configuration data in JavaScript Object Notation (JSON) from **verbose** to **ietf** starting in Junos OS Release 16.1R1. You can explicitly specify the default export format for JSON configuration data by configuring the appropriate statement at the **[edit system export-format json]** hierarchy level. Although the **verbose** statement is exposed in the Junos OS CLI as of the current release, you can configure this statement starting in Junos OS Release 16.1R1.

  [See export-format.]

Known Limitations

IN THIS SECTION

Learn about known limitations in this release for the PTX Series.

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

General Routing

- Multiple explicit null labels will be present on packet if BGPoLDPoRSVP next hop hierarchy has multiple explicit-null labels . No attempt will be done to combine them. PR1556328

Open Issues

IN THIS SECTION

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

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

General Routing

- PTX Series platforms with the FPC-PTX-P1-A or FPC2-PTX-P1A line card might encounter a single event upset (SEU) event that can cause a linked-list corruption of the TQCHIP. The following syslog message is reported: **Jan 9 08:16:47.295 router fpc0 TQCHIP1: Fatal error pqt_min_free_cnt is zero Jan 9 08:16:47.295 router fpc0 CMSNG: Fatal ASIC error, chip TQ Jan 9 08:16:47.295 router fpc0 TQ Chip::FATAL ERROR!! from PQT free count is zero jan 9 08:16:47.380 router alarmd[2427]: Alarm set: FPC color=RED, class=CHASSIS, reason=FPC 0 Fatal Errors - TQ Chip Error code: 0x50002 Jan 9 08:16:47.380 router craftd[2051]: Fatal alarm set, FPC 0 Fatal Errors - TQ Chip Error code: 0x50002** The Junos OS chassis management error handling does detect such a condition, and raises an alarm and performs the disable-pfe action for the affected Packet Forwarding Engine entity. To recover this Packet Forwarding Engine entity, a restart of the FPC is needed. Soft errors are transient or non-recurring. FPCs experiencing such SEU events do not have any permanent damage.

Contact your Juniper Networks support representative if the issue is seen after an FPC restart. PR1254415

- The following log message might be seen on an FPC with WINTEC mSATA SSD: SMART ATA Error Log Structure error: invalid SMART checksum. PR1354070
- The firewall counter for the lo0 interface might not increase. PR1420560
- An rpd core file is generated when FIPS mode is set. PR1530951
- sFlow reports incorrect **Extended Router Data** for traffic going over a nondefault VRF. PR1537190
- The output VLAN is not reported correctly in the extended switch data for IP-IP transit traffic when you configure both dynamic tunnel and FTI as backups. PR1537648
- The following error comes up when the ukern socket to sflowd daemon (server) is closed: **Socket to sflowd closed**. The error is rectified by itself as the client successfully reestablishes the connection in the subsequent attempts. When these errors are consistent, it indicates a communication issue between sFlow running on the FPC with the sflowd. PR1538863
- A crash is triggered when the IPv6 transit statistics feature is bounced, that is, enable - disable - enable in presence of aggregated Ethernet configuration. With scalar interfaces, this is not known to occur. This only affects the uKern (Packet Forwarding Engine) and has no effect on the Routing Engine. PR1571279

Interfaces and Chassis

- The **resiliencyd.re.re0** core file is seen when executing cminfra scripts. There is no functional impact on resiliencyd. Once cored resiliencyd recovered, then it behaves normally as expected. PR1578822

Layer 2 Ethernet Services

- Issuing the **request system zeroize** command sometimes does not trigger ZTP. Workaround is to reinitiate ZTP. PR1529246

MPLS

- The RSVP interface update threshold configuration syntax has changed between Junos OS Releases 18.2X75-D435 and 20.3X75-D10 to include curly braces are the threshold value. As such upgrading and downgrading between these two releases is not entirely automatic and now requires the user to delete this stanza if configured before the downgrade and then manually reconfigure. PR1554744

Routing Protocols

- After a remote transit router reboot, due to a race between route reconvergence and BGP PIC version up message to the Packet Forwarding Engine, certain BGP routes might reuse stale LDP next hops and cause packet discard at the transit router during the route reconvergence window. PR1495435
- Device allows more SSH connection than configured under connection-limit. PR1559305

Resolved Issues

IN THIS SECTION

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

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

Resolved Issues: 21.1R1

IN THIS SECTION

Forwarding and Sampling

- The l2ald process might crash due to a next-hop issue in the EVPN-MPLS. PR1548124

General Routing

- On PTX10016 routers, flow control is disabled by default on both aggregated Ethernet interfaces. PR1478715
- In IP-in-IP, end-to-end (CE device to CE device) traceroute is not working as expected. PR1488379
- The following error message might be seen after links flap: **t6e_dfe_tuning_state:et-6/0/0 - Failed to dfe tuning count 10**. PR1512919
- The FPC-E might get stuck. PR1519673
- The chassisd memory leak might cause traffic loss. PR1537194
- Aggregated Ethernet interface framing errors might display increasing values before restoring correct value. PR1539537
- The error message **expr_dfw_action_topo_connect_anh:1434 expr_dfw_action_topo_connect_anh:eda_anh_discard is FALSE for nh-id 568 - return** is observed in PTX1000 routers. PR1540064
- The Packet Forwarding Engine might crash in an MPLS IPv6-tunneling scenario when the next hop changes. PR1540793
- The rpd crash might be seen when BGP service route is resolved over color-only SR-TE policy. PR1550736
- The interface filter with source-port 0 matches everything instead of port 0. PR1551305
- The **show system health-monitor** command is disabled on PTX10008 routers. PR1560268
- On PTX10008 router, BGP next-hop index (indirect and unilist) change after GRES and NSR trigger causes a momentary (unexpected) traffic loss. PR1560323

- The **set chassis display** command is disabled on PTX1008 routers. PR1560453
- An enhancement to enable watchdog petting log on the PTX10000 line cards. PR1561980
- On PTX1000, DCPFE crashes in steady state and generates the following error: **PFE_ERROR_NO_RESOURCE: NH: Failed to alloc for element list**. PR1564147

Infrastructure

- Interface drop counters might display 0 during a race condition when VOQ statistics are also polled simultaneously. PR1537960
- The kernel crashes and generates a core file if churn happens for a flood composite next hop. PR1548545

Interfaces and Chassis

- EOAM IEEE802.3ah link discovery state is Down instead of Active Send Local after deactivating interfaces on routers. PR1532979
- Logs are not being written in /var/log/messages on certain PTX Series platforms. PR1551374

Layer 2 Ethernet Services

- The copying of files to the RCB over WAN ports is slow. PR1496895

MPLS

- Traffic loss might be observed due to rpd crash in an MPLS scenario. PR1528460

Network Management and Monitoring

- A memory leak in the mib2d and snmpd processes might result in SNMP being unresponsive to SNMP queries. PR1543508
- The syslog messages might not be sent with the correct port. PR1545829

Platform and Infrastructure

- The BGP session replication might fail to start after the session crashes on the backup Routing Engine. PR1552603

Routing Policy and Firewall Filters

- Generate route goes to hidden state when the protect core statement is enabled. PR1562867

Routing Protocols

- Traffic might be silently discarded when the clear bgp neighbor all command is executed on a router and also on the corresponding route reflector in succession. PR1514966
- The rpd process generates a core file at gp_rtarget_tsi_update,bgp_rtarget_flash_rt,bgp_rtarget_flash. PR1541768
- BGP-LU session might flap with AIGP scenario. PR1558102

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Basic Procedure for Upgrading to Release 21.1

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

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

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

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

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

To download and install Junos OS Release 21.1R1:

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

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

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

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

4. Select the **Software** tab.

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

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

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

10. Install the new jinstall package on the router.

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

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

```
user@host> request system software add validate reboot source/junos-install-ptx-x86-64-21.1R1.9.tgz
```

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

```
user@host> request system software add validate reboot source/junos-install-ptx-x86-64-21.1R1.9-limited.tgz
```

Replace the source with one of the following values:

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

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

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

Rebooting occurs only if the upgrade is successful.

> **NOTE**: You need to install the Junos OS software package and host software package on the routers with the RE-PTX-X8 Routing Engine. For upgrading the host OS on this router with VM

Host support, use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the **request vmhost software add** command. For more information, see the VM Host Installation topic in the Installation and Upgrade Guide.

NOTE: After you install a Junos OS Release 21.1 jinstall package, you cannot return to the previously installed software by issuing the **request system software rollback** command. Instead, you must issue the **request system software add validate** command and specify the jinstall package that corresponds to the previously installed software.

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

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind.

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

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

Upgrading a Router with Redundant Routing Engines

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

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

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

Junos OS Release Notes for QFX Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

Hardware

- **Support for JNP-100G-DAC-1M, JNP-100G-DAC-3M, and JNP-100G-DAC-5M DACs (QFX10002-60C)**—Starting in Junos OS Release 21.1R1, the QFX10002-60C switches support the JNP-100G-DAC-1M, JNP-100G-DAC-3M, and JNP-100G-DAC-5M direct attach copper (DAC) cables.

  [See Hardware Compatibility Tool.]

- **Support for the JNP-QSFP-100G-BXSR and the JNP-QSFP-40G-BXSR bidirectional transceivers**—Starting in Junos OS Release 21.1R1, the QFX5210-64C switches support the JNP-QSFP-100G-BXSR and JNP-QSFP-40G-BXSR bidirectional transceivers.

  [See Hardware Compatibility Tool.]

Authentication and Access Control

- **802.1X authentication on trunk ports (QFX5100 switches)**—Starting in Junos OS Release 21.1R1, you can enable 802.1X authentication on trunk ports on QFX5100 switches. Authentication on the trunk port is supported only in single supplicant and single-secure supplicant modes.

  [See 802.1X Authentication.]

EVPN

- **Tunnel endpoint in the PMSI tunnel attribute field for EVPN Type 3 routes (ACX5448, EX4600, EX4650, EX9200, and QFX10002)**—Starting in Junos OS Release 21.1R1, you can set the tunnel endpoint in the provider multicast service interface (PMSI) tunnel attribute field to use the ingress router's secondary loopback address. When you configure multiple loopback IP addresses on the local provider edge (PE) router and the primary router ID is not part of the MPLS network, the remote PE router cannot set up a PMSI tunnel route back to the ingress router.

  To configure the router to use a secondary IP address that is part of the MPLS network, include the **pmsi-tunnel-endpoint*****pmsi-tunnel-endpoint*** statement at the **[edit routing-instances *routing-instance-name* protocols evpn]** hierarchy level for both EVPN and virtual-switch instance types.

  [See EVPN.]

- **Support for remote port mirroring based on VNI match conditions (QFX10002, QFX10008, QFX10016)**—Starting in Junos OS Release 21.1R1, You can use VXLAN network identifier (VNI) values as a match condition when filtering traffic for remote port mirroring. VNI packets that match the configured VNI will be mirrored, with the VNI packet contents, on the designated interface. This addition extends functionality introduced in previous releases.

  [See Filter-based forwarding in EVPN-VXLAN networks and Remote port mirroring to an IP address.]

- **Explicit congestion notification (ECN) over VXLAN tunnels (EX4650 and QFX5120)**—Starting in Junos OS Release 21.1R1, by default, standalone EX4650 and QFX5120 switches support explicit congestion notification (ECN) for packets that are encapsulated across VXLAN tunnels, as follows:

  - During VXLAN encapsulation at the source virtual tunnel endpoint (VTEP), the switch copies the ECN bits of the Type-of-Service (ToS) field from the original packet IP header to the outer VXLAN encapsulation IP header.

  - During VXLAN de-encapsulation at the remote VTEP, the switch copies the ECN bits of the ToS field from the outer VXLAN encapsulation IP header to the original packet IP header.

  You can configure the **vxlan-disable-copy-tos-encap** statement or the **vxlan-disable-copy-tos-decap** statement at the **[set forwarding-options]** hierarchy on the encapsulation or de-encapsulation ends of the tunnel, respectively, to disable the ECN copy operation.

> **NOTE**: These switches also copy the differentiated services code point (DSCP) bits in the ToS field of the IP header upon VXLAN encapsulation and de-encapsulation by default, and the same statements disable copying both the DSCP and ECN bits.

[See vxlan-disable-copy-tos-encap and vxlan-disable-copy-tos-decap.]

Interfaces

- **Dual-speed support on 100Gbps DAC breakout cable (QFX5120-48Y, QFX5200-32C, and QFX5210-64C)**—Starting in Junos OS Release 21.1R1, we support 4x10Gbps speed along with 4x25Gbps speed on the QSFP28 100Gbps DAC breakout cable with the other end SFP28 transceivers. Supported cable lengths are 1, 2, 3, and 5 meters. You can set the 4x10Gbps speed by using the **set chassis fpc *fpc* pic *pic* port *port number* channel-speed 10g** command.

  [See Hardware Compatibility Tool.]

IP Tunneling

- **Support for IPv4 and IPv6 unicast IP-over-IP tunneling (QFX5000)**—Starting in Junos OS Release 21.1R1, we support IP-over-IP tunneling for IPv4 and IPv6 traffic on QFX5000. QFX5000 switches also support recursive route resolution for IP-over-IP tunnels.

  [See Overview of Next-Hop-Based Dynamic Tunneling Using IP-Over-IP Encapsulation.]

- **Support for BGPoverBGPoverBGP recursive route resolution (QFX5100, QFX5110, QFX5120, QFX5200, and QFX5210)**—Starting in Junos OS Release 21.1R1, you can enable BGPoverBGPoverBGP route resolution by creating an expanded route hierarchy, using the **preserve-nexthop-hierarchy** statement at the **[edit routing-options resolution]** hierarchy level.

  [See resolution.]

Junos Telemetry Interface

- **Packet Forwarding Engine and Routing Engine sensor support with JTI (QFX5210)**—Starting in Junos OS Release 21.1R1, you can use Junos telemetry interface (JTI) with remote procedure call (gRPC) services to export Packet Forwarding Engine statistics and Routing Engine statistics from QFX5210 switches to an outside collector. These statistics can also be exported through UDP (native) sensors.

  The supported Packet Forwarding Engine sensors are:

  - Sensor for CPU (microkernel) memory (resource path **/junos/system/linecard/cpu/memory/**)

  - Sensor for firewall filter statistics (resource path **/junos/system/linecard/firewall/**)

  - Sensor for physical interface traffic (resource path **/junos/system/linecard/interface/**)

- Sensor for logical interface traffic (resource path **/junos/system/linecard/interface/logical/usage/**)
- Sensor for software-polled queue-monitoring statistics (resource path **/junos/system/linecard/qmon-sw/**)

The supported Routing Engine sensors are:

- Sensor for LACP state export (resource path **/lacp/**)
- Sensor for chassis environmentals export (resource path **/junos/system/components/component/**)
- Sensor for chassis components export (resource path **/components/**)
- Sensor for LLDP statistics export (resource path **/lldp/interfaces/interface[name='*name*']/**)
- Sensor for BGP peer information export (resource path **/network-instances/networkinstance/protocols/protocol/bgp/**)
- Sensor for RPD task memory utilization export (resource path **/junos/task-memoryinformation/**)
- Sensor network discovery ARP table state (resource path **/arp-information/**)
- Sensor for network discovery NDP table state (resource path **/nd6-information/**)

[See Understanding OpenConfig and gRPC on Junos Telemetry Interface.]

Layer 2 Features

- **Configurable EtherType values (QFX10002-36Q, QFX10002-72Q, and QFX10008)**—Starting in Junos OS Release 21.1R1, you can customize the EtherType field values stored in the ternary content addressable memory (TCAM) tables. Ethernet frame headers contain an EtherType field to identify the protocol in the frame's payload so the receiving device knows how to process the traffic. The device keeps a default list of the EtherType values it can process in TCAM for fast access. With this feature, you can define custom EtherType values in place of some of the default values in the TCAM table either for a specified FPC slot or for all currently active FPCs on the switch. Some EtherType values are reserved; you can’t change or reconfigure those values.

  [See ether-type.]

MPLS

- **Nonstop active routing (NSR) support for controller-initiated RSVP label-switched paths (LSPs) (MX Series, PTX Series, and QFX Series)**—Starting in Junos OS Release 21.1R1, we support NSR for controller-initiated RSVP-based point-to-point (P2P) and point-to-multipoint (P2MP) LSPs. The primary Routing Engine synchronizes all RSVP LSPs initiated by Path Computation Elements (PCEs), including multicast flow specifications for any PCE-initiated P2MP LSPs, with the backup Routing

Engine. This ensures zero traffic loss for the traffic carried over PCE-initiated RSVP LSPs during Routing Engine switchovers. This feature is enabled when NSR is configured.

[See PCEP Configuration.]

Multicast

- **Support for next-generation multicast VPN (QFX10002, QFX10008, and QFX10016)**—Starting in Junos OS Release 21.1R1, we support Multiprotocol BGP (MBGP) next-generation multicast VPNs with the following types of provider tunnels:

  - Ingress replication
  - RSVP-Traffic Engineering (RSVP-TE) point-to-multipoint (P2MP)
  - Multipoint LDP P2MP

  A P2MP is a Multiprotocol Label Switching (MPLS) label-switched path (LSP) with a single source and multiple destinations. By taking advantage of MPLS packet replication capability of the network, P2MP LSPs avoid unnecessary packet replication at the ingress router. Packet replication takes place only when packets are forwarded to two or more different destinations requiring different network paths.

  [See Multiprotocol BGP MVPNs Overview and provider-tunnel.]

Network Management and Monitoring

- **Operational command RPCs support returning JSON and XML output in minified format in NETCONF sessions (ACX1000, ACX1100, ACX2100, ACX4000, ACX5048, ACX5096, ACX5448, EX2300, EX2500, EX3400, EX4300, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48P, EX4400-48T, EX4600, EX4650, EX9200, MX104, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10001, PTX10002, PTX10008, PTX10016, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX10002, QFX10002-60C, QFX10008, QFX10016, SRX550, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, operational command RPCs, including the **<get-configuration>** RPC, support the **format="json-minified"** and **format="xml-minified"** attributes in NETCONF sessions to return JSON or XML output in minified format. Minified format removes any characters that are not required for computer processing—for example, unnecessary spaces, tabs, and newlines. Minified format decreases the size of the data, and as a result, can reduce transport costs as well as data delivery and processing times.

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

- **sFlow support for IP-IP traffic (PTX1000, PTX10008, and QFX10002)**—Starting in Junos OS Release 21.1R1, you can use sFlow technology to sample IP over IP (IP-IP) traffic on a physical port. sFlow sampling is supported for IP-IP tunnels that have an IPv4 outer header that carry IPv4 or IPv6 traffic. You can use sFlow monitoring technology to randomly sample network packets from IP-IP tunnels and to send the samples to a destination collector for monitoring. Devices that act as an IP-IP tunnel entry point, transit device, or tunnel endpoint support sFlow sampling.

[See Overview of sFlow Technology and Configuring IP Tunnel Interfaces.]

- **Remote port mirroring to IPv6 address (GRE encapsulation)(EX4650, EX4650-48Y-VC, QFX5120, QFX5120-32C, QFX511120-48T, QFX5120-48T-VC, QFX5120-48Y, and QFX5120-48YM)**—Starting in Junos OS Release 21.1R1, you can use remote port mirroring to copy packets entering a port or VLAN and sends the copies to the IPv6 address of a device running an analyzer application on a remote network (sometimes referred to as “extended port mirroring”). When you use remote port mirroring the mirrored packets are GRE-encapsulated.

  Add the address you would like to have the copied packets sent to in the CLI hierarchy. For example, **set forwarding-options analyzer ff output ipv6-address 2000::1**.

  [See Understanding Port Mirroring and Analyzers.]

Platform and Infrastructure

Routing Policy and Firewall Filters

- **Support for microsegmentation on VLANs and VXLANs (QFX5110 and QFX5120)**—Starting in Junos OS Release 21.1R1, you can configure egress filters with Layer 2 and Layer 3 match conditions in both VLAN and VXLAN deployments. Junos OS already supports filtering in Layer 2 match conditions in the ingress direction.

  To use egress filters for microsegmentation in a VXLAN, enable the **epacl-firewall-optimization** statement at the **[edit chassis]** level of the hierarchy and create the firewall rules with the match conditions that you want to filter on. For egress filtering on VLANs, you don't need to enable **epacl-firewall-optimization**. Both the QFX5110 and QFX5120 support egress filtering, for VLANs and VXLANs, with the following match conditions:

  - **ip-source-address**
  - **ip-destination-address**
  - **destination-port**
  - **destination-mac-address**
  - **user-vlan-id**
  - **ip-protocol**
  - **source-mac-address**

  Valid actions for these rules are **accept**, **count**, and **discard**.

[See Overview of Firewall Filters (QFX Series) and Understanding Firewall Filter Match Conditions.]

Software Installation and Upgrade

- **Zero-touch provisioning (ZTP) with IPv6 support (QFX5120-32C)**—Starting in Junos OS Release 21.1R1, you can use a DHCPv6 client and ZTP to provision a QFX5120-32C switch.. During the bootstrap process, the device first uses the DHCPv4 client to request for information regarding the image and configuration file from the DHCP server. The device checks the DHCPv4 bindings sequentially. If there is a failure with one of the DHCPv4 bindings, the device continues to check for bindings until provisioning is successful. However, if there are no DHCPv4 bindings, the device checks for DHCPv6 bindings and follows the same process as for DHCPv4 until the device is provisioned successfully. Both DHCPv4 and DHCPv6 clients are included as part of the default configuration on the device.

  The DHCP server uses DHCPv6 options 59 and 17 and applicable suboptions to exchange ZTP-related information between itself and the DHCP client.

  [See Zero Touch Provisioning.]

- **Support for signed third-party application installation (MX10003, MX10008, QFX5210, QFX10002, and QFX10008 routers with VM host architecture)**—Starting in Junos OS Release 21.1R1, you can install signed third-party application installation and carry over the application between upgrades.

  The backup of third-party package occurs during upgrade. Hence, the package is restored even if the installed package is deleted or uninstalled before a reboot. However, as the third party package restoration depends on the contents saved on the disk during upgrade and the configuration to allow the package to be installed, restoration is not possible when

  - Configuration is removed after upgrade
  - Content is removed due to deletion by configuring **request vmost zeroize** command

  On platforms where jinstall-host.tgz images are installed, the minimum space required for the backup is 250MB. After backup, if the free space available is less than 200MB, the backup would be deleted to make space for upgrade. On platforms where junos-vmhost images are installed, the minimum space required for backup of third party unbundled packages is 1200MB. After the backup, if the free space is less than 512MB, the backup would be deleted to free up space for upgrade.

  [See Installing, Upgrading, Backing Up, and Recovery of VM Host.]

What's Changed

IN THIS SECTION

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

What's Changed in Release 21.1R1

General Routing

- **Support for unicast ARP request on table entry expiration**—You can configure the device to send a unicast ARP request instead of the default broadcast request when an ARP table entry is about to expire. The retry requests are unicast at intervals of 5 seconds. Without this option, the retry requests are broadcast at intervals of 800 milliseconds. This behavior reduces ARP overall broadcast traffic. It also supports the use case where access nodes are configured not to forward broadcast ARP requests toward customer CPEs for security reasons and instead translate ARP broadcasts to unicast requests. To confirm whether this is configured, you can issue the **show configuration system arp | grep unicast-mode-on-expire** command.

  [See arp.]

- **Change in license bandwidth command on vMX virtual routers**—Starting in Junos OS 21.1R1, to use the available license bandwidth, explicitly set the license bandwidth use the **set chassis license bandwidth <in Mbps>** command.

  [See Configuring Licenses on vMX Virtual Routers..]

- **Support only for manual channelization on QSFP-100G-SR4-T2 optics (QFX5120-48T and QFX5120-32C)**—We recommend that you use the active optical cable (AOC) for auto-channelization. The QSFP-100G-SR4-T2 cables do not support auto-channelization. To use the QSFP-100G-SR4-T2 optics with an external breakout cable, you must configure the channelization manually by including the **channel-speed** statement at the **edit chassis fpc slot-number pic pic-number (port port-number | port-range port-range-low port-range-high)** hierarchy level.

  [See channel-speed.]

Junos XML API and Scripting

- **The jcs:invoke() function supports suppression of root login and logout events in system log files for SLAX commit scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The **jcs:invoke()** extension function supports the **no-login-logout** parameter in SLAX commit scripts. If you include the parameter, the function does not generate and log UI_LOGIN_EVENT and UI_LOGOUT_EVENT messages when the script logs in as root to execute the specified remote procedure call (RPC). If you omit the parameter, the function behaves as in earlier releases in which the root UI_LOGIN_EVENT and UI_LOGOUT_EVENT messages are included in system log files.

  [See invoke() Function (SLAX and XSLT).]

- **The jcs:invoke() function supports suppression of root login and logout events in system log files for SLAX event scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The **jcs:invoke()** extension function supports the **no-login-logout** parameter in SLAX event scripts. If you include the parameter, the function does not generate and log UI_LOGIN_EVENT and UI_LOGOUT_EVENT messages when the script logs in as root to execute the specified remote procedure call (RPC). If you omit the parameter, the function behaves as in earlier releases in which the root UI_LOGIN_EVENT and UI_LOGOUT_EVENT messages are included in system log files.

  [See invoke() Function (SLAX and XSLT).]

- **Python 2.7 deprecation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, devices running Junos OS no longer support Python 2.7. We've deprecated the corresponding **language python** statement at the **[edit system scripts]** hierarchy level. To execute Python scripts, configure the **language python3** statement at the **[edit system scripts]** hierarchy level to execute the scripts using Python 3.

  [See Understanding Python Automation Scripts for Devices Running Junos OS.]

Layer 2 Ethernet Services

- **Modification to sync-reset command (All JUNOS and EVO platforms)**—Starting from this release, the sync-reset command is disabled by default on all Junos and EVO platforms. Sync-reset command enables the device to send the sync bit in the LACP packets on minimum-link failure. Previously the sync-reset command was enabled by default on QFX and EX series, while it was by default disabled on MX, PTX and ACX series.

  [See sync-reset.]

Network Management and Monitoring

- **Support for disconnecting unresponsive NETCONF-over-SSH clients (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—You can enable devices to automatically disconnect unresponsive NETCONF-over-SSH clients by configuring the **client-alive-**

interval and **client-alive-count-max** statements at the **[edit system services netconf ssh]** hierarchy level. The **client-alive-interval** statement specifies the timeout interval in seconds, after which, if no data has been received from the client, the device requests a response. The **client-alive-count-max** statement specifies the threshold of missed client-alive responses that triggers the device to disconnect the client, thereby terminating the NETCONF session.

[See ssh (NETCONF).]

- **Support for specifying the YANG modules to advertise in the NETCONF capabilities and supported schema list (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—You can configure devices to emit third-party, standard, and Junos OS native YANG modules in the capabilities exchange of a NETCONF session by configuring the appropriate statements at the **[edit system services netconf hello-message yang-module-capabilities]** hierarchy level. In addition, you can specify the YANG schemas that the NETCONF server should include in its list of supported schemas by configuring the appropriate statements at the **[edit system services netconf netconf-monitoring netconf-state-schemas]** hierarchy level.

  [See hello-message and netconf-monitoring.]

User Interface and Configuration

- **Verbose format option to export JSON configuration data (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The Junos OS CLI exposes the **verbose** statement at the **[edit system export-format json]** hierarchy level. We changed the default format to export configuration data in JavaScript Object Notation (JSON) from **verbose** to **ietf** starting in Junos OS Release 16.1R1. You can explicitly specify the default export format for JSON configuration data by configuring the appropriate statement at the **[edit system export-format json]** hierarchy level. Although the **verbose** statement is exposed in the Junos OS CLI as of the current release, you can configure this statement starting in Junos OS Release 16.1R1.

  [See export-format.]

Known Limitations

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

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

General Routing

- This issue occurs due to PECHIP limitation when underlay is tagged. After de-encapsulation when the inner packet is recirculated, it still retains the VLAN tag property from the outer header as the outer header was tagged. Thus 4 bytes of the inner tag got overwritten in the inner packet and the packet got corrupted, which results in EGP checksum trap seen in PECHIP. Fixing PECHIP limitation in software has high risk. Workaround is provided to enable the "encapsulate-inner-vlan" configuration statement. PR1435864

- This warning will pop up at reboot/power-off time. This notification is part of unmount routine, which is harmless and has not function impact. This might get fixed in coming RPCL/WRL release. PR1527581

- In case of fan failure, "show chassis environment" and "show chassis fan" show "failed" and "check" status, respectively. This is expected and there is no discrepancy in terms of real status. PR1527628

- On QFX10002 platform, for sFlow egress sampling on AE interface under Dynamic IP-IP tunnel transit scenario, the nextHop field is not present in sFlow export data. PR1533307

- ECMP over GRE does not work for BGP routes. Traffic is polarized to just one egress interface but not distributed to multiple egress interfaces. PR1537924

- In QFX5100 and EX4300 non-TVP platforms, the sample rate is limited by the IPC between the Packet Forwarding Engine and the sFlow process, so the supported limit is around 700 samples per second in these platforms. This is applicable to any sampled packets in these platforms and not specific to IPnIP. PR1539815

- ISSU is not supported from releases before Junos OS Release 20.4 to releases after Junos OS Release 20.4. There is a major SDK upgrade from 6.3.2 to 6.5.16, due to which the warm boot feature needed for ISSU is not supported by Broadcom. PR1554915

Routing Protocols

- On QFX5210 platforms, when two flex hash rules are configured, on deactivating the first one, the second one is not programmed in hardware. Commit works though. 1. Two flex hash profiles with same traffic type and different hash parameters cannot be configured. For example: * Profile 1: Below profile applies flex hash rule for traffic with mpls 2 -label and pick the offsets configured set forwarding-options enhanced-hash-key flex-hashing FH-MPLS-2-V4-TCP-UDP ethtype mpls num-labels 2 set forwarding-options enhanced-hash-key flex-hashing FH-MPLS-2-V4-TCP-UDP ethtype mpls conditional-match CM-MPLS-2-V4-TCP set forwarding-options enhanced-hash-key flex-hashing FH-MPLS-2-V4-TCP-UDP ethtype mpls hash-offset offset1 base-offset1 start-of-L3-OuterHeader set forwarding-options enhanced-hash-key flex-hashing FH-MPLS-2-V4-TCP-UDP ethtype mpls hash-offset offset1 offset1-value 28 set forwarding-options enhanced-hash-key flex-hashing FH-MPLS-2-V4-TCP-UDP ethtype mpls hash-offset offset1 offset1-mask ffff * Profile 2: Below profile applies flex hash rule for traffic with mpls 2-label which is same as profile 1. Since already there is a profile1 configured to match mpls label-2 traffic, this profile will not be installed and doesn't have any impact . set forwarding-options enhanced-hash-key flex-hashing FH1-MPLS-2-V4 ethtype mpls num-labels 2 set forwarding-options enhanced-hash-key flex-hashing FH1-MPLS-2-V4 ethtype mpls hash-offset offset1 base-offset1 start-of-L3-OuterHeader set forwarding-options enhanced-hash-key flex-hashing FH1-MPLS-2-V4 ethtype mpls hash-offset offset1 offset1-value 0 set forwarding-options enhanced-hash-key flex-hashing FH1-MPLS-2-V4 ethtype mpls hash-offset offset1 offset1-mask ffff 2. Two flex hash profiles with same traffic types can be configured only when below conditions are met : 1. All the flex-hash parameters like base-offset, offset-value, offset-mask are same for both profiles. 2. Both profiles should have different conditional profiles attached. 3. The conditional parameters like base-offset and offset-value have to be same for both profiles. 4. Combination of "match-data match-mask" has to be different for both profiles . PR1521306

- On QFX5100 devices not running qfx-5e codes (non TVP architecture), when image with Broadcom SDK upgrade (6.5.x) is installed, the CPU utilization may go up by around 5 percent. PR1534234

Open Issues

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

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

General Routing

- VXLAN VNI (multicast learning) scaling on QFX5110 traffic issue is seen from VXLAN tunnel to Layer 2 interface. PR1462548

- After repeated deletion and addition of a logical switch on an NSX-V setup, with OVSDB configured, ping between the VM to the baremetal server fails intermittently (only on a few iterations out of the total number of iterations). PR1506097

- Changing the scaled firewall profiles on the fly does not release the TCAM resources as expected. PR1512242

- On the QFX10000 line of switches, when an explicit Layer 2 classifier is applied on a Layer 3 interface, the default Layer 3 classifiers are not removed. By design, the Layer 3 classifier takes precedence over the Layer 2 classifier. PR1520570

- After performing NSSU and GRES from Junos OS Release 20.1 or Release 20.2 to Junos OS Release 20.3 on the QFX5000 line of switches, the land backup member of Virtual Chassis might be in unstable state with db> prompt. PR1533874

- On QFX10002 devices acting as PHP, egress sFlow samples do not report MPLS explicit-null label in the raw packet header. The MPLS payload can be of IPv4 or IPv6 protocol. PR1537946

- "Socket to sflowd closed" error is seen when the ukern socket to sflowd daemon (server) is closed. The error is rectified by itself when the connection is re-established in the subsequent attempts. When these errors are consistent, it indicates the communication issue between sFlow running on the FPC with the sflowd. PR1538863

- EVPN-VXLAN: vmcore seen on primary and backup Routing Engines of QFX10008 with Layer 2 or Layer 3 multicast configuration. PR1539259

- Moving WRL7 SDK to RCPL31 for QFX10000 platforms. RCPL31 provides tweaking of build infra and fixes related to performance enhancements and vulnerabilities in WRL7 Linux. PR1547565

- 100G AOC from InnoLight does not come up after multiple reboots. It recovers after the interface is disabled and then enabled. PR1548525

- Traffic does not get load-balanced by QFX10000 platforms over ESI links with EVPN-VXLAN configured, PR1550305

- 5M DAC connected between QFX10002-60C and MX2010 doesn't link up. But with 1M and 3M DAC this interoperation works as expected. Also it is to be noted on QFX10002-60C and ACX Series devices or traffic generator, the same 5M DAC works seamlessly. There seems to be certain SI or link-level configuration on both QFX10002-60C and MX2010 that needs to be debugged with the help from HW and SI teams and resolved. PR1555955

- In Junos OS Release 20.2, some features show up as licensed features. Customer might see alarms, commit warnings, and the following **show system license** output. However, there would be no functional impact. user@router> show system license License usage: Licenses Licenses Licenses Expiry Feature name used installed needed esi-lag 1 0 1 invalid. PR1558017

- In VXLAN Layer3 Gateway scenario, untagged traffic routed over native-vlan-id interface might drop. The issue is seen on the QFX5110 line of switches because of the BRCM hardware errata, where routing of an untagged packet does not delete the internal VLAN tag assigned to the packet. PR1560038

- To avoid the additional interface flap, interface hold time needs to be configured . PR1562857

- RPD core file is generated when the device reboots and daemon restarts. Daemon recovers and there is no service impact on routing protocol usage.PR1567043

- With reference to the topology used in the PR, out of all IS-IS sessions only below IS-IS sessions are not getting established:- that is between the r0(mx240) and r3/r4(Qfx10k) devices. The above devices are connected by intermediate nodes r1 and r2. The issue seems to be specific to these intermediate nodes and its config No issue is seen between the routers that is, between r3 and r4, here IS-IS sessions are all up between these nodes. PR1580971

- The renew-ack's might not be seen in the dhcp client while checking DHCP smart relay over IRB interfaces in QFX5100 device running Junos OS Release 21.1R1. PR1581025

Layer 2 Ethernet Services

- It was observed rarely that issuing a "request system zeroize" did not trigger ZTP. A simple workaround is to reinitiate ZTP. PR1529246

Platform and Infrastructure

- Upgrading satellite devices may lead to some SDs in SyncWait state. Cascade port flap does not cause this issue. PR1556850

Routing Policy and Firewall Filters

- On all Junos OS platforms with "set policy-options rtf-prefix-list" configured, if upgraded to a specific version, the device might fail to validate its configuration, which eventually causes rpd to crash unexpectedly due to a software fault. PR1538172

Routing Protocols

- On QFX5000 platforms, when the host forwarding table is full and the host entries are installed in the LPM forwarding table, or when lpm-profile with unicast-in-lpm option is used, the Layer 3 IP route might not be installed in the LPM forwarding table if there are SER errors, hence there might be traffic impact. PR1429504

- Currently IPIP, IPv6 and gre decapsulations are supported. It is not recommended to configure gre and IPIP/IPv6 in a single filter. If gre and IPIP/IPv6 are configured in a single filter, then the last decapsulate filter term is used to program the entire filter terms. PR1580468

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for QFX Series switches.

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

Resolved Issues: 21.1R1

EVPN

- All the ARP reply packets toward some address are flooded across the entire fabric. PR1535515
- EVPN-VXLAN registers MAC-move counters under system statistics bridge even though there is no actual MAC move for the multihomed clients. PR1538117
- The l2ald process might generate a core file when changing the EVPN-VXLAN configuration. PR1541904
- The l2ald deamon might crash when **forwarding-options evpn-vxlan shared-tunnels** is configured. PR1548502
- The l2ald process generates a core file at l2ald_iff_rtm_delete_subintf_ifbds during dci fusion run. PR1550109
- QFX10002 :: mac-vrf: QFX10k l2ald core: l2ald_vxlan_ifl_create_event_handler at /src/junos/usr.sbin/l2ald/platform/junos/l2ald_rtsock_vxlan.c:477 PR1560068
- [evpn_vxlan]: evpn vxlan mac-ip aging testcase failed. PR1562925
- l2ald process generates a core file at vlogging_event, l2ald_vxlan_ifl_create_event_handler, l2ald_vxlan_ifl_event_handler, l2ald_process_event. PR1576558

Forwarding and Sampling

- The l2ald process might crash due to a next-hop issue in the EVPN-MPLS. PR1548124

General Routing

- Port qualifier is not supported for QFX5000 platforms. PR1440980
- On the QFX5000 line of switches, the egress ACL filter entries is only 512 in Junos OS Release 19.4R1. PR1472206
- On the QFX10000 device, the chassisd process might generate core files on the backup Routing Engine after commit for 200 seconds due to the following error message: CHASSISD_MAIN_THREAD_STALLED. PR1481143

- On the QFX5000 line of switches, multicast traffic loss is observed due to a few missing multicast routes in the spine node. PR1510794
- The DHCP traffic might not be forwarded correctly when DHCP sends unicast packets. PR1512175
- Channelized interfaces might fail to come up. PR1512203
- The output of the show chassis forwarding-options command displays incorrect display issue, Virtual Chassis environment, and configured num-65-127-prefix values. PR1512712
- On the QFX5100 device, the cprod process timeout triggers high CPU utilization. PR1520956
- Output interface index in the sFlow packet is zero when transit traffic is observed on the IRB interface with VRRP enabled. PR1521732
- Some inter-VLAN traffic flows do not converge after rebooting a spine (QFX10002) device in an EVPN-VXLAN non-collapsed scaled scenario. PR1522585
- Traffic loss might be observed on interfaces in a VXLAN environment. PR1524955
- Channelizing the 40GbE port to a 10GbE port might bring down another interface on the QFX10000 platforms. PR1527814
- When a multicast feed is received with TTL 1 on QFX10002 line of switches. There will be 2 copies of the packet sent to the host - one from the normal flow and another from the multicast module. These packets are logged in the firewall log incorrectly. PR1533814
- High rate of ARP or NS packets might be observed between a device that runs Junos OS and the host when the device that runs Junos OS receives an ARP or NS packet on an interface in transition. PR1534796
- The following Packet Forwarding Engine error message is observed in the BRCM-VIRTUAL: brcm_virtual_tunnel_port_create() ,489: Failed NW vxlan port token(45) hw-id(7026) status(Entry not found). PR1535555
- The interfaces on QFX5100-48T switch might stay up when the peer device is rebooting PR1538071
- On the QFX5100-48T, interfaces are not created after a channel speed of 10 Gbps is applied on ports 48 through 53. PR1538340
- The BFD sessions might not come up in an VXLAN scenario. PR1538600
- Management Ethernet link down alarm is seen while verifying system alarms in a Virtual Chassis setup. PR1538674
- ARP request may be dropped in leaf node in an EVPN-VXLAN scenario. PR1539278

- The rpd memory leak might be observed on the backup Routing Engine due to link flaps PR1539601
- Unable to take RSI properly due to the authentication error. PR1539654
- FPC might not be recognized after power cycle (hard reboot) PR1540107
- Traffic loss might be seen in the OVSDB VXLAN scenario. PR1540208
- On the QFX5100 Virtual Chassis, the End Segment Not Present message is not reported for the ping overlay function with the local host MAC. PR1542226
- On the QFX5000 device running EVPN-VXLAN, the following Packet Forwarding Engine error message might be seen: bd_platform_irb_ifl_attach_detach: platform specific irb ifl attach/detach failed (-1). PR1543812
- On the QFX10002-60C device, the show pfe filter command is unavailable. PR1545019
- The chip on FPC linecard might crash during the system booting. PR1545455
- OSPFv3 session may keep flapping and OSPFv3 hellos might be dropped in the host path. PR1547032
- On a QFX10000 device, traffic might get dropped when the set routing-options forwarding-table no-ecmp-fast-reroute configuration is changed to 128 ECMP entries. PR1547457
- On the QFX5100 Virtual Chassis, the backup Routing Engines clear the reporting alarm for a PEM failure intermittently for a missing power source. PR1548079
- The VXLAN encapsulated packet might be sent on the network port with an incorrect inner VLAN ID 4095. PR1548218
- The 40GbE interface might be channelized after restarting the Virtual Chassis member. PR1548267
- The Neighbor Solicitation might be dropped from the peer device. PR1550632
- The interface filter with source-port 0 matches everything instead of port 0. PR1551305
- On the QFX5110 and QFX5120 devices, the DHCPv6 traffic received over the VTEP might not be forwarded. PR1551710
- On the QFX5000 devices, ARP resolution might fail. PR1552671
- The **action-shutdown** configuration of storm control does not work for ARP broadcast packets. PR1552815
- Traffic might not passed due to the addition of the VLAN tag 2 while passing through the Virtual Chassis port. PR1555835
- Traffic might be dropped when a firewall filter rule uses the then VLAN action. PR1556198

- The dcpfe process crashes and a core file is generated on QFX10002-60C while running Type 5 EVPN_VXLAN configuration with 2000 VLANs. PR1556561
- DHCP Discover packets are not getting flooded with VXLAN configuration. PR1557049
- Traffic storm might be caused by the analyzer due to link flapping. PR1557274
- Firewall filter might fail to work on QFX5000 platforms. PR1558320
- On the QFX5120 device, amber LEDs are displayed for the fan modules after upgrading to Junos OS Release 20.2R1. PR1558407
- Pseudo Random Binary Sequence (PRBS) test on QFX5200 platform fails for 100GbE interfaces with default settings. PR1560086
- There are a few instances of IPv6 ARP ND failure after loading the base configurations. PR1560161
- When configuring static MAC and static ARP on the EVPN core aggregate interface, the underlay next-hop programming might not be updated in the Packet Forwarding Engine. PR1561084
- PTP boundary clock with G.8275.2.enh profile_2 512 clients does not come up. PR1561348
- PTP lock status gets stuck at the Acquiring state instead of the Phase Aligned state. PR1561372
- Firewall filters might not be working after ISSU. PR1561690
- On QFX10000 platforms, the dcpfe process might crash during configuration changes. PR1561746
- Traffic loss might happen in a large-scaled EVPN scenario when the next-hop type changes between Discard and Unicast. PR1562425
- Port mirroring might not work as expected on QFX5000 platforms. PR1562607
- Output of the **show chassis fpc ether-types** command includes the FPC slot number. PR1564496
- QFX10K: Firewall log incorrectly populating from PFE for IPv6 traffic. PR1569120
- QFX10002:OpenConfig to Junos OS configuration translation has failed while translating interface-mode trunk and vlan members. PR1580292

Interfaces and Chassis

- The logical interface might flap after the addition or deletion of the native VLAN configuration. PR1539991
- MAC address entry issue might be seen after MC-LAG interface failover or failback. PR1562535

Layer 2 Ethernet Services

- DHCP packet drop may be seen when DHCP relay is configured on the leaf device. PR1554992

Layer 2 Features

- Check traffic with VXLAN encapsulation header fails.PR1541316
- Traffic may be forwarded incorrectly on an interface having VXLAN enabled and "hold-time up xxx" statement configured. PR1550918
- On EX4650-48Y and QFX5120 platforms, packets with VLAN ID 0 are dropped. PR1566850

Routing Policy and Firewall Filters

- The policy configuration might be mismatched between the rpd and mgd process when deactivate policy-options prefix-list is involved in the configuration sequence. PR1523891

Routing Protocols

- On the QFX5100-48T-6Q Virtual Chassis or Virtual Chassis fabric, the following error message is observed while copying the image to the Virtual Chassis fabric member and trying to downgrade the image: rcp for member 14, failed. PR1486632
- The IPv6 traffic might be silently dropped due to null-route filtering when falling back from IP-in-IP tunnel to inet.0/inet6.0. PR1508631
- Traffic might be silently discarded when the clear bgp neighbor all command is executed on a router and also on the corresponding route reflector in succession. PR1514966
- The OSPF neighborship gets stuck in the Start state after configuring the EVPN-VXLAN. PR1519244
- DCPFE crash might be observed while updating VRF for multicast routes during IRB uninit. PR1546745
- [pfe] [generic] : qfx5100-24q-2p :: fxpc core in brcm_nh_unilist.c:2162 during stress test PR1556224
- BGP-LU session flap might be seen with AIGP used scenario. PR1558102
- On the QFX5110-32Q device, the following syslog error message is observed after loading the NC T5 EVPN-VXLAN configuration: BCM-L2,pfe_bcm_l2_sp_bridge_port_tpid_set() Config TPID New/Old (8100:8100) Other-Tpid's ba49, 4aa0, 80f. PR1558189
- Layer 3 inter pod IPv4 traffic issue observed after loading non-collapsed Type 5 EVPN-VXLN configuration. PR1560173

- On the QFX5110 platform, ARP resolution may fail if "native-vlan-id" is configured on the VXLAN interface. PR1563569
- The dcpfe process might crash when the size of the Local Bias Filter Bitmap string exceeds 256 characters. PR1568159
- On the QFX5210-64C device, ping does not work while verifying the native VLAN behavior on the Q-in-Q interface. PR1568533

User Interface and Configuration

- set chassis fpc 0 ether-type applicable only for ether index 6 to 27. PR1565695

Virtual Chassis

- On the QFX5000 Virtual Chassis, the DDoS violations that occur on the backup are not reported to the Routing Engine. PR1490552

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

Upgrading Software on QFX Series Switches

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

If you are not familiar with the download and installation process, follow these steps:

1. In a browser, go to https://www.juniper.net/support/downloads/junos.html.

   The Junos Platforms Download Software page appears.

2. In the QFX Series section of the Junos Platforms Download Software page, select the QFX Series platform for which you want to download the software.

3. Select **20.3** in the Release pull-down list to the right of the Software tab on the Download Software page.

4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 20.3 release.

   An Alert box appears.

5. In the Alert box, click the link to the PSN document for details about the software, and click the link to download it.

   A login screen appears.

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

7. Download the software to a local host.

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

9. Install the new jinstall package on the device.

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

Customers in the United States and Canada use the following command:

```
user@host> request system software add source/jinstall-host-qfx-5-x86-64-20.3-R1.n-secure-signed.tgz reboot
```

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 20.3 **jinstall** package, you can issue the **request system software rollback** command to return to the previously installed software.

Installing the Software on QFX10002-60C Switches

This section explains how to upgrade the software, which includes both the host OS and the Junos OS. This upgrade requires that you use a VM host package—for example, a **junos-vmhost-install-*x*.tgz** .

During a software upgrade, the alternate partition of the SSD is upgraded, which will become primary partition after a reboot .If there is a boot failure on the primary SSD, the switch can boot using the snapshot available on the alternate SSD.

NOTE: The QFX10002-60C switch supports only the 64-bit version of Junos OS.

NOTE: If you have important files in directories other than /config and /var, copy the files to a secure location before upgrading. The files under /config and /var (except /var/etc) are preserved after the upgrade.

To upgrade the software, you can use the following methods:

If the installation package resides locally on the switch, execute the **request vmhost software add** ***<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add /var/tmp/junos-vmhost-install-qfx-x86-64-20.4R1.9.tgz
```

If the Install Package resides remotely from the switch, execute the **request vmhost software add** ***<pathname><source>*** command.

For example:

```
user@switch> request vmhost software add ftp://ftpserver/directory/junos-vmhost-install-qfx-
x86-64-20.4R1.9.tgz
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Installing the Software on QFX10002 Switches

NOTE: If you are upgrading from a version of software that does not have the FreeBSD 10 kernel (15.1X53-D30, for example), you will need to upgrade from Junos OS Release 15.1X53-D30 to Junos OS Release 15.1X53-D32. After you have installed Junos OS Release 15.1X53-D32, you can upgrade to Junos OS Release 15.1X53-D60 or Junos OS Release 18.3R1.

NOTE: On the switch, use the **force-host** option to force-install the latest version of the Host OS. However, by default, if the Host OS version is different from the one that is already installed on the switch, the latest version is installed without using the **force-host** option.

If the installation package resides locally on the switch, execute the **request system software add** ***<pathname><source>*** **reboot** command.

For example:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-f-x86-64-20.4R1.n-secure-signed.tgz reboot
```

If the Install Package resides remotely from the switch, execute the **request system software add** ***<pathname><source>*** **reboot** command.

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-f-x86-64-20.4R1.n-secure-signed.tgz reboot
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Upgrading Software from Junos OS Release 15.1X53-D3X to Junos OS Release 15.1X53-D60, 15.1X53-D61.7, 15.1X53-D62, and 15.1X53-D63 on QFX10008 and QFX10016 Switches

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

The switch contains two Routing Engines, so you will need to install the software on each Routing Engine (re0 and re1).

If the installation package resides locally on the switch, execute the **request system software add *<pathname><source>*** command.

To install the software on re0:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* re0** command.

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re0
```

To install the software on re1:

```
user@switch> request system software add /var/tmp/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* re1** command.

For example:

```
user@switch> request system software add ftp://ftpserver/directory/jinstall-host-qfx-10-m-15.1X53-D60.n-secure-domestic-signed.tgz re1
```

Reboot both Routing Engines.

For example:

```
user@switch> request system reboot both-routing-engines
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

```
user@switch> show version
```

Installing the Software on QFX10008 and QFX10016 Switches

Because the switch has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation.

NOTE: Before you install the software, back up any critical files in **/var/home**. For more information regarding how to back up critical files, contact Customer Support at https://www.juniper.net/support.

WARNING: If graceful Routing Engine switchover (GRES), nonstop bridging (NSB), or nonstop active routing (NSR) is enabled when you initiate a software installation, the software does not install properly. Make sure you issue the CLI **delete chassis redundancy** command when prompted. If GRES is enabled, it will be removed with the **redundancy** command. By default, NSR is disabled. If NSR is enabled, remove the nonstop-routing statement from the **[edit routing-options]** hierarchy level to disable it.

1. Log in to the master Routing Engine's console.

   For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

2. From the command line, enter configuration mode:

   ```
   user@switch> configure
   ```

3. Disable Routing Engine redundancy:

   ```
   user@switch# delete chassis redundancy
   ```

4. Disable nonstop-bridging:

```
user@switch# delete protocols layer2-control nonstop-bridging
```

5. Save the configuration change on both Routing Engines:

```
user@switch# commit synchronize
```

6. Exit the CLI configuration mode:

```
user@switch# exit
```

After the switch has been prepared, you first install the new Junos OS release on the backup Routing Engine, while keeping the currently running software version on the master Routing Engine. This enables the master Routing Engine to continue operations, minimizing disruption to your network.

After making sure that the new software version is running correctly on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the software version on the other Routing Engine.

7. Log in to the console port on the other Routing Engine (currently the backup).

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

8. Install the new software package using the **request system software add** command:

```
user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-
x86-64-20.4R1.n-secure-signed.tgz
```

For more information about the **request system software add** command, see the CLI Explorer.

9. Reboot the switch to start the new software using the **request system reboot** command:

```
user@switch> request system reboot
```

NOTE: You must reboot the switch to load the new installation of Junos OS on the switch.

To abort the installation, do not reboot your switch. Instead, finish the installation and then issue the **request system software delete** ***<package-name>*** command. This is your last chance to stop the installation.

All the software is loaded when you reboot the switch. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

While the software is being upgraded, the Routing Engine on which you are performing the installation is not sending traffic.

10. Log in and issue the **show version** command to verify the version of the software installed.

```
user@switch> show version
```

Once the software is installed on the backup Routing Engine, you are ready to switch routing control to the backup Routing Engine, and then upgrade or downgrade the master Routing Engine software.

11. Log in to the master Routing Engine console port.

For more information about logging in to the Routing Engine through the console port, see the specific hardware guide for your switch.

12. Transfer routing control to the backup Routing Engine:

```
user@switch> request chassis routing-engine master switch
```

For more information about the **request chassis routing-engine master** command, see the CLI Explorer.

13. Verify that the backup Routing Engine (slot 1) is the master Routing Engine:

```
user@switch> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Backup
    Election priority              Master (default)

Routing Engine status:
```

```
  Slot 1:
    Current state                  Master
    Election priority              Backup (default)
```

14. Install the new software package using the **request system software add** command:

    ```
    user@switch> request system software add validate /var/tmp/jinstall-host-qfx-10-f-x86-64-20.4R1.n-secure-signed.tgz
    ```

    For more information about the **request system software add** command, see the CLI Explorer.

15. Reboot the Routing Engine using the **request system reboot** command:

    ```
    user@switch> request system reboot
    ```

    NOTE: You must reboot to load the new installation of Junos OS on the switch.

    To abort the installation, do not reboot your system. Instead, finish the installation and then issue the **request system software delete jinstall *<package-name>*** command. This is your last chance to stop the installation.

    The software is loaded when you reboot the system. Installation can take between 5 and 10 minutes. The switch then reboots from the boot device on which the software was just installed. When the reboot is complete, the switch displays the login prompt.

    While the software is being upgraded, the Routing Engine on which you are performing the installation does not send traffic.

16. Log in and issue the **show version** command to verify the version of the software installed.

17. Transfer routing control back to the master Routing Engine:

    ```
    user@switch> request chassis routing-engine master switch
    ```

    For more information about the **request chassis routing-engine master** command, see the CLI Explorer.

18. Verify that the master Routing Engine (slot 0) is indeed the master Routing Engine:

```
user@switch> show chassis routing-engine
Routing Engine status:
  Slot 0:
    Current state                  Master
    Election priority              Master (default)

outing Engine status:
  Slot 1:
    Current state                  Backup
    Election priority              Backup (default)
```

Performing a Unified ISSU

You can use unified ISSU to upgrade the software running on the switch with minimal traffic disruption during the upgrade.

NOTE: Unified ISSU is supported in Junos OS Release 13.2X51-D15 and later.

Perform the following tasks:

- "Preparing the Switch for Software Installation" on page 213
- "Upgrading the Software Using Unified ISSU" on page 214

Preparing the Switch for Software Installation

Before you begin software installation using unified ISSU:

- Ensure that nonstop active routing (NSR), nonstop bridging (NSB), and graceful Routing Engine switchover (GRES) are enabled. NSB and GRES enable NSB-supported Layer 2 protocols to synchronize protocol information between the master and backup Routing Engines.

  To verify that nonstop active routing is enabled:

NOTE: If nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

```
user@switch> show task replication
        Stateful Replication: Enabled
        RE mode: Master
```

If nonstop active routing is not enabled (**Stateful Replication** is **Disabled**), see *Configuring Nonstop Active Routing on Switches* for information about how to enable it.

- Enable nonstop bridging (NSB). See *Configuring Nonstop Bridging on Switches (CLI Procedure)* for information on how to enable it.
- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the **request system snapshot** command.

Upgrading the Software Using Unified ISSU

This procedure describes how to upgrade the software running on a standalone switch.

To upgrade the switch using unified ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in *Installing Software Packages on QFX Series Devices*.
2. Copy the software package or packages to the switch. We recommend that you copy the file to the **/var/tmp** directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Start the ISSU:
   - On the switch, enter:

   ```
   user@switch> request system software in-service-upgrade /var/tmp/package-name.tgz
   ```

   where ***package-name*.tgz** is, for example, **jinstall-host-qfx-10-f-x86-64-20.4R1.n-secure-signed.tgz**.

NOTE: During the upgrade, you cannot access the Junos OS CLI.

The switch displays status messages similar to the following messages as the upgrade executes:

```
warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get
lost!
ISSU: Validating Image
ISSU: Preparing Backup RE
Prepare for ISSU
ISSU: Backup RE Prepare Done
Extracting jinstall-host-qfx-5-f-x86-64-18.3R1.n-secure-signed.tgz ...
Install jinstall-host-qfx-5-f-x86-64-19.2R1.n-secure-signed.tgz completed
Spawning the backup RE
Spawn backup RE, index 0 successful
GRES in progress
GRES done in 0 seconds
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item           Status                  Reason
  FPC 0          Online (ISSU)
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff
```

NOTE: A unified ISSU might stop, instead of abort, if the FPC is at the warm boot stage. Also, any links that go down and up will not be detected during a warm boot of the Packet Forwarding Engine (PFE).

NOTE: If the unified ISSU process stops, you can look at the log files to diagnose the problem. The log files are located at **/var/log/vjunos-log.tgz**.

5. Log in after the reboot of the switch completes. To verify that the software has been upgraded, enter the following command:

```
user@switch> show version
```

6. Ensure that the resilient dual-root partitions feature operates correctly, by copying the new Junos OS image into the alternate root partitions of all of the switches:

```
user@switch> request system snapshot slice alternate
```

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19.3, 19.4, and 20.1 are EEOL releases. You can upgrade from Junos OS Release 19.3 to Release 19.4 or from Junos OS Release 19.3 to Release 20.1.

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

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

Junos OS Release Notes for SRX Series

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for the SRX Series Services Gateways. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

Application Identification (AppID)

- **Application signature package enhancements (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 21.1R1, we've enhanced the application signature package by grouping all newly added signatures under the junos:all-new-apps group. When you download the application signature package on your device, the predefined application group is downloaded. You can use this application group in the security policy configuration.

  We've also introduced a list of application tags, based on attributes, in the application signature package. You can group similar applications based on these predefined tags. By doing so, you can consistently reuse the application groups when you define security policies.

  [See Predefined Application Signatures for Application Identification.]

- **Enhancements to packet capture of unknown applications (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 21.1R1, your security device stores the packet capture of unknown applications' details per session. As a result of this change, the packet capture (.pcap) file now includes the session ID in the filename. We now store the file in **destination-IP-address.destination-**

port.protocol.session-id.pcap format in the **/var/log/pcap** location. (Previously, the packet capture file was saved in **destination-IP-address. destination-port.protocol.pcap** format.)

In addition, we've enhanced packet capture of unknown application functionality to capture unknown Server Name Indication (SNI) details.

[See Packet Capture of Unknown Application Traffic Overview.]

- **Application signature enhancements (NFX Series, SRX Series, and vSRX)**—Starting in Junos OS Release 21.1R1, we've introduced the following enhancements to application signatures:
  - Support for FTP data context propagation
  - Skipping of deep packet inspection (DPI) for the sessions offloaded by advanced policy-based routing (APBR) on application system cache (ASC) hit (when only APBR service is enabled).
  - Forceful installation of the application signature pack over the same version of signature pack.
  - Display (in the CLI command output) of the application signature pack release date.
  - Display (in the CLI command output) of the list of deprecated application signatures available in the installed signature pack.

  [See Predefined Application Signatures for Application Identification.]

Authentication and Access Control

- **Configure client information to connect to the JIMS server (cSRX, SRX300, SRX340, SRX345, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting with Junos OS Release 21.1R1, you can configure which specifc interface, source IP address or routing instance SRX should use for connecting to a JIMS server.
  [See Configuring the Connection to an SRX Series Device.]

Chassis

- **Layer 2 channel error alarm (SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 21.1R1, you can configure a threshold limit for the L2 channel error count and set an alarm when the error count crosses the threshold using two new configuration statements. Use l2-channel-errorthreshold to set a threshold limit for the L2 channel error count, and use l2-channel-errors to set an alarm when the error count crosses the threshold at the [set chassis alarm] hierarchy level. This configuration generates a SNMP trap of the L2 channel error whenever the alarm is raised.

  [See l2-channel-error-threshold (chassis), l2-channel-errors (chassis), and show system alarms.]

Chassis Cluster

- **Support for NAT functionalities on multinode high availability (SRX5400, SRX5600, and SRX5800 with SPC3 card)**—Starting in Junos OS Release 21.1R1, we support the following NAT functionalities on HA nodes in multinode high availability:

  - IPv6 NAT (source NAT, destination NAT, and static NAT)

  - NAT64 persistent NAT

  - Logical and tenant systems NAT (source NAT, destination NAT, and static NAT)

  - Port block allocation (PBA) and NAT logs.

  [See Multinode High Availability, and NAT for User Logical Systems.]

- **Enabling and disabling control link (SRX4100, SRX4200, and SRX4600)**—Starting in Junos OS Release 21.1R1, you can enable or disable control links, using the following commands, to control the status of the cluster nodes and minimize failovers.

  - **delete chassis cluster control-interface node 0 disable**

  - **delete chassis cluster control-interface node 1 disable**

  - **set chassis cluster control-interface node0 disable**

  - **set chassis cluster control-interface node1 disable**

  [See chassis and fabric-options].

Ethernet Switching and Bridging

- **LLDP on routed and reth interfaces (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800)**—Starting in Junos OS Release 21.1R1, you can enable LLDP on all physical interfaces, including routed and redundant Ethernet (reth) interfaces. LLDP is a link-layer protocol used by network devices to advertise capabilities, identity, and other information to a LAN.

  [See LLDP Overview.]

EVPN

- **EVPN-VXLAN tunnel inspection (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 21.1R1, we've introduced the following enhancements to the VXLAN support for SRX Series devices:

  - Support for SRX5000 line of devices in addition to the SRX4000 line and vSRX

  - Enhancements to tunnel inspection for VXLAN-encapsulated traffic by applying Layer 4 or Layer 7 security services to the tunnel traffic. The supported services are:

- Application identification
- IDP
- Juniper Advanced Threat Prevention (ATP Cloud)
- Unified threat management (UTM)

Layer 7 security services provide application-level security and protect users from security threats through VXLAN tunnel.

[See Configuring Tunnel Traffic Inspection.]

- **Security policy enhancement for EVPN-VXLAN tunnel inspection (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting in Junos OS Release 21.1R1, we've enhanced EVPN-VXLAN tunnel inspection by adding zone-level policy control for the inner traffic. When you create a policy that applies to the inner session created by VXLAN inner header, you can define the following parameters as match conditions for the inner traffic:

  - Source zone
  - Destination zone
  - URL category
  - Dynamic applications

  Additional matching criteria in the security policy provide granular control and extensibility to manage traffic.

  [See Configuring Tunnel Traffic Inspection.]

Flow-Based and Packet-Based Processing

- **Support for PowerMode IPsec (PMI) solution (SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800 with SPC3 cards, vSRX, and vSRX3.0) and GRE acceleration solution (SRX Series and NFX Series)**—Starting in Junos OS Release 21.1R1, we support the PMI and GRE acceleration solutions to improve the software-defined WAN (SD-WAN) performance.

Table 9: Solutions and Details

Solution	How to Enable?
PMI	Include the **power-mode-ipsec** and **gre-performance-acceleration** statements at the **[edit security flow]** hierarchy level. **NOTE**: PMI supports both IPsec and GRE. In this case, traffic flows through the PMI data path.
GRE acceleration	Include the **gre-performance-acceleration** statement at the **[edit security flow]** hierarchy level. **NOTE**: By default, **gre-performance-acceleration** is turned off. In this case, traffic flows through the GRE acceleration data path.

[See gre-performance-acceleration (Security Flow), flow (Security Flow), and show security flow status.]

- **Enhanced monitoring and troubleshooting of the flow session (SRX Series)**—Starting in Junos OS Release 21.1R1, we've introduced additional filters to the show security flow session operational command. The additional filters allow you to generate specified outputs in a list so that you can easily monitor the flow session. We've also introduced the show security flow session pretty and show security flow session plugins operational commands to view detailed information about the flow session.

  You can also trace the packet-drop information without committing the configuration using the monitor security packet-drop operational command. This command output is displayed on the screen until you press Ctrl+c or until the security device collects the requested number of packet drops. The command includes various filters to generate the output fields per your requirement.

  [See show security flow session, show security flow session pretty, show security flow session plugins, and monitor security packet-drop.]

- **Packet-based ECMP support for Express Path (SRX5400, SRX5600, and SRX5800)**—In earlier releases, Express Path supported only session-based ECMP traffic. Starting in Junos OS Release 21.1R1, Express Path also supports packet-based ECMP traffic from different network processors of the SRX Series device. In the packet-based ECMP mode, the SPU creates multiple network processor sessions on multiple network processors at a time. This feature is enabled by default.

  [See Express Path.]

High Availability

- **Distributed mode support for fast BFD failure detection (SRX1500, SRX4100, SRX4200, and SRX4600)**—Starting in Junos OS Release 21.1R1, we support distributed mode for BFD. This mode provides a faster BFD failure detection time of 3 x 300 ms. You enable distributed mode by configuring the BFD failure detection time to a value less than 500 ms. We support this feature for a standalone SRX Series device. It is not supported for chassis clusters.

  > **NOTE**: SRX1500 devices run in dedicated mode if you've configured **set chassis dedicated-ukern-cpu**, regardless of the BFD failure detection time. You can enable distributed mode on SRX1500 devices only when dedicated mode is not enabled.

  [See detection-time (BFD Liveness Detection) and Understanding Distributed BFD.]

Interfaces

- **Native VLAN ID configuration on the reth interface (SRX300, SRX320, SRX340, SRX345, SRX380, SRX550HM, SRX1500, SRX4100, SRX4200, and SRX4600)** —Configuring the native VLAN ID on the redundant Ethernet (reth) interface enables the logical interface whose VLAN ID matches the native VLAN ID that is configured for that interface to accept untagged packets as well as tagged packets. Using the same logical interface with the native VLAN ID enabled ensures that any packet going out of that interface does not have a tag attached. Packets can be outbound control packets or transit data packets.

  [See native-vlan-id.]

Intrusion Detection and Prevention

- **Support for Perl-compatible regular expression (PCRE) version 8.40 (SRX Series and NFX Series)**—Starting in Junos OS Release 21.1R1, we've upgraded the codebase of intrusion detection and prevention (IDP) from PCRE version 5.40 to PCRE version 8.40. As PCRE version 8.40 supports new regex constructs, this upgrade enhances the capability of Junos OS IDP attack signatures to match regular expressions. With this upgrade, we've also addressed security vulnerabilities in the Junos OS PCRE codebase.

  [See pattern-pcre (Security IDP).]

- **Support for Snort IPS signatures (SRX Series and NFX Series)**—Starting in Junos OS Release 21.1R1, Juniper Networks IDP supports Snort IPS signatures. IDP secures your network by using signatures that help to detect attacks. Snort is an open-source intrusion prevention system (IPS). You can convert the Snort IPS rules into Juniper IDP custom attack signatures using the Juniper Integration of Snort Tool (JIST). These rules help detect malicious attacks.

  - JIST is included in Junos OS by default. The tool supports Snort version 2 and version 3 rules.

- JIST converts the Snort rules with snort-ids into equivalent custom attack signatures on Junos OS with respective snort-ids as the custom attack names.

- When you run the **request** command with Snort IPS rules, JIST generates **set** commands equivalent to the Snort IPS rules. Use the **request security idp jist-conversion** command to generate the **set** commands as CLI output. To load the **set** commands, use the **load set terminal** statement or copy and paste the commands in the configuration mode, and then commit. You can then configure the existing IDP policy with the converted custom attack signatures.

- All the Snort IPS rule files that didn't get converted are written to **/tmp/jist-failed.rules**. The error log files generated during the conversion are written to **/tmp/jist-error.log**.

- To view the jist-package version, use the **show security idp jist-package-version** command.

[See Understanding Snort IPS Signatures, request security idp jist-conversion , and show security idp jist-package-version .]

Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud)

- **Server Message Block (SMB) protocol support for Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud) file inspection (SRX Series)**—Starting in Junos OS Release 21.1R1, SRX Series devices support the SMB protocol in advanced anti-malware (AAMW) file inspection. Use the **set services advanced-anti-malware policy *policy-name* smb** command to configure file inspection for the SMB protocol.

  [See advanced-anti-malware policy and show services advanced-anti-malware statistics.]

- **Support for configuring DNS sinkhole (SRX5000 line of devices)**—Starting in Junos OS Release 21.1R1, we support DNS sinkhole feature on the SRX5000 line of devices in addition to its existing support on SRX4000 line of devices and vSRX. You can configure DNS filtering to identify DNS requests for disallowed domains. You can either:

  - Block access to the domain by sending a DNS response that contains the IP address or fully qualified domain name (FQDN) of a sinkhole server. This ensures that when the client attempts to send traffic to the disallowed domain, the traffic instead goes to the sinkhole server.

  - Log the DNS request and reject access.

  [See dns-filtering.]

- **Support for username feed type in adaptive threat profiling (SRX Series devices and vSRX)**—Starting in Junos OS Release 21.1R1, you can add the user source identity (username) as a feed type in adaptive threat profiling. Use the **add-source-identity-to-feed *user-identity*** and **add-destination-identity-to-feed *user-identity*** commands at the **[edit security policies from-zone *zone-name* to-zone *zone-name* policy *policy-name* then [permit|deny|reject] application-services]** hierarchy level to configure the username feed type.

[See security-intelligence (security policies), show services security-intelligence sec-profiling-feed status and show services security-intelligence category.]

- **Enhancements to alerts, alarms, and fallback options (SRX Series)**—Starting in Junos OS Release 21.1R1, we've enhanced the following alerts, alarms, and fallback options for failure conditions when you enroll SRX Series devices with Juniper ATP Cloud.

  - Add new SNMP traps for the following:

    - Advanced-anti-malware (AAMW)—**jnxJsAAMWChannelUp** and **jnxJsAAMWChannelDown**.

    - Encrypted traffic insights—**jnxJsSMSChannelUp** and **jnxJsSMSChannelDown**

    - Security intelligence (SecIntel)—**jnxJsSecIntelChannelUp** and **jnxJsSecIntelChannelDown**

  - Raise new alarms for AAMW, encrypted traffic insights, and SecIntel.

  - Add new fallback options for action control in case of failure conditions. Configure the fallback options at the **[edit services advanced-anti-malware policy *policy-name*]** hierarchy level.

  [See advanced-anti-malware policy.]

- **Support for Juniper ATP Cloud services in VXLAN tunnel inspection (SRX4000 line of devices, SRX5000 line of devices, and vSRX)**—Starting in Junos OS Release 21.1R1, the listed SRX Series devices and vSRX support Juniper ATP Cloud services such as AAMW and SecIntel in VXLAN tunnel traffic inspection. These services inspect the VXLAN traffic only if there is a security policy configured to perform the inspection. When you configure VXLAN tunnel inspection policies on an SRX Series device, the device scans the VXLAN tunnel traffic through AAMW and SecIntel services.

  [See tunnel-inspection and show security flow session.]

- **Policy-based threat profiling (SRX Series devices and vSRX)**—Starting in Junos OS Release 21.1R1, you can add the user source identity (username) to a security policy to generate security feeds.

  Juniper ATP Cloud service consolidates the generated feeds from SRX Series device and shares the duplicated results back with that security device. The security device uses the feeds to perform actions against the designated traffic. You can enable the security device to use the feeds by configuring security policies with the feeds as matching criteria. When traffic matches policy conditions, the device applies policy actions.

  [See Threat Profiling Support in Security Policy.]

Network Management and Monitoring

- **Operational command RPCs support returning JSON and XML output in minified format in NETCONF sessions (ACX1000, ACX1100, ACX2100, ACX4000, ACX5048, ACX5096, ACX5448, EX2300, EX2500, EX3400, EX4300, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48P, EX4400-48T, EX4600, EX4650, EX9200, MX104, MX204, MX240, MX480, MX960, MX2008,**

MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10001, PTX10002, PTX10008, PTX10016, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX10002, QFX10002-60C, QFX10008, QFX10016, SRX550, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)—Starting in Junos OS Release 21.1R1, operational command RPCs, including the **<get-configuration>** RPC, support the **format="json-minified"** and **format="xml-minified"** attributes in NETCONF sessions to return JSON or XML output in minified format. Minified format removes any characters that are not required for computer processing—for example, unnecessary spaces, tabs, and newlines. Minified format decreases the size of the data, and as a result, can reduce transport costs as well as data delivery and processing times.

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

- **HMAC-SHA-2 authentication protocol support for users of SNMPv3 USM (MX Series and SRX Series)**—Starting in Junos OS Release 21.1R1, you can configure HMAC-SHA-2 authentication protocols for users of the SNMPv3 user-based security model (USM) with the following new CLI configuration statements:

  - authentication-sha224
  - authentication-sha256
  - authentication-sha384
  - authentication-sha512

  We've introduced these statements for local-engine users at **[edit snmp v3 usm local-engine user username]** and for remote-engine users at **[set snmp v3 usm remote-engine engine-id user user-name]**.

  [See authentication-sha224, authentication-sha256, authentication-sha348, and authentication-sha512.]

- **Log profiles and templates for customized logging (cSRX, SRX300, SRX320, SRX340, SRX345, SRX380, SRX550, SRX1500, SRX4100, SRX4200, SRX4600, SRX5800, and vSRX)**—Starting in Junos OS Release 21.1R1, you can configure log profiles and log templates for a policy. Use the configuration statement **profile** to select a log profile for a policy at the **[edit security log profile]** hierarchy level, and use the configuration statement **template** to select a predefined log template for a policy at the **[edit security log profile profile-name template]** hierarchy level. From this release, you can track the application tracking logs using the **set security application-tracking log-session-create**, **set security application tracking log-session-close**, **set security application-tracking session-update-interval**, **set security application-tracking no-volume-updates**, and **set services application-identification no-application statistics** commands. Unified threat management (UTM) features also support the log profiles and templates for customized logging.

  [See profile (security), application-tracking, application-identification, and show security log profile.]

Securing GTP and SCTP Traffic

- **Support for messages and message lists for aggregate rate limiting (SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, and SRX5800 with SPC2 and SPC3 cards, and vSRX)**—Starting in Junos OS Release 21.1R1, we support messages and message lists for aggregate rate limiting. To configure a message list, include the **message-list *msg-list-name* message *msg-number*** statement at the **[edit security gtp]** hierarchy level. To configure the default messages, use the **rate-limit default message {v0 | v1 | v2} *msg-list-name*** statement at the **[edit security gtp]** hierarchy level. Use the **show security gtp message-list** to display message-list profiles. Use the **show security gtp rate-limit default** to display default rate-limit messages.

  [See message-list, rate-limit (Aggregated rate limit), show security gtp message-list, and show security gtp rate-limit default.]

Services Applications

- **Support for RFC 2544-based benchmarking tests (SRX300, SRX320, SRX340, SRX345, SRX380, and SRX550HM)**—Starting in Junos OS Release 21.1R1, we support only the Layer 3 reflector function for these tests, with the following limitations:

  - **family inet** option; no other families are supported

  - IPv4 source and destination addresses for the tests

  RFC 2544 tests measure and demonstrate the service-level agreement (SLA) parameters before service activation. You can use the tests to measure throughput, latency, frame loss rate, and the number of back-to-back frames. [See Understanding Using Probes for Real-Time Performance Monitoring on M, T, PTX, MX, and SRX Series Routers .]

Software Installation and Upgrade

- **request system software status command (MX480, MX960, MX2010, MX2020, SRX1500, SRX4100, SRX4400, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, you can use the CLI command **request system software status** to view the status of the software package installation or uninstallation on the local Routing Engine.

Unified Threat Management (UTM)

- **Source address configuration for UTM services (SRX Series)**—Starting in Junos OS Release 21.1R1, you can configure the **source-address** option at the following hierarchy levels for the Enhanced Web Filtering (EWF) cloud service, websense redirect policy service, and antivirus and antispam scan services. Configuring **source-address** for these Unified Threat Management (UTM) services enhances the network disaster recovery.

  - **[edit security utm default-configuration web-filtering juniper-enhanced server]**

  - **[edit security utm default-configuration web-filtering websense-redirect server]**

- **[edit security utm feature-profile web-filtering websense-redirect profile profile name server]**
- **[edit security utm default-configuration anti-virus sophos-engine server]**

  Antivirus and antispam services share the same **source-address** configuration under the Sophos engine server.

  [See source-address.]

VPNs

- **Enhancements to increase traffic selector flexibility (SRX Series)**—Starting in Junos OS Release 21.1R1, you can do the following to add flexibility to your traffic selectors in different deployment scenarios:

  - Configure the routing metric for a traffic selector.
  - Define the source port range, destination port range, and protocol for a traffic selector.
  - Define multiple terms within a traffic selector, instead of creating multiple traffic selectors (or child security associations or SAs) for a VPN. Each term comprises the local and remote IP prefixes, the source and destination port ranges, and the protocol identifier. You can use these parameters in a single IPsec SA negotiation. In earlier Junos OS releases, you configure each traffic selector with one set of local and remote IP prefixes to be used in an IPsec SA negotiation with a peer.

  [See traffic-selector and show security ipsec security-associations detail.]

What's Changed

IN THIS SECTION

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

What's Changed in Release 21.1R1

IN THIS SECTION

Flow-Based and Packet-Based Processing

- **Self-generated IKE packets choose outgoing interface matching source IP address (SRX Series)**—A self-generated IKE packet always selects the ECMP outgoing interface that matches the source IP address. Note that we don't support filter-based forwarding for self-generated traffic with rerouting.

General Routing

- **Support for unicast ARP request on table entry expiration**—You can configure the device to send a unicast ARP request instead of the default broadcast request when an ARP table entry is about to expire. The retry requests are unicast at intervals of 5 seconds. Without this option, the retry requests are broadcast at intervals of 800 milliseconds. This behavior reduces ARP overall broadcast traffic. It also supports the use case where access nodes are configured not to forward broadcast ARP requests toward customer CPEs for security reasons and instead translate ARP broadcasts to unicast requests. To confirm whether this is configured, you can issue the following command: **show configuration system arp | grep unicast-mode-on-expire**.

  [See arp.]

- **Change in show security firewall-authentication jims operational command (SRX4600)**—Starting in Junos OS Release 21.1R1, the **show security firewall-authentication jims (statistics | display)** operational command includes the **display** option.

  [See show security firewall-authentication jims statistics.]

- **New output field added in show pfe statistics traffic command (SRX380)**—Starting in Junos OS Release 21.1R1, you'll see **Unicast EAPOL** in the output of the **show pfe statistics traffic** command.

[See show pfe statistics traffic.]

- **Default MKA transmit interval (SRX380)**—On SRX380 devices, the default MACsec Key Agreement (MKA) transmit interval is 2000 milliseconds. If you deploy an SRX380 device with another security peer device with a MACsec secure link, you must change the MKA transmit interval on the peer device to 2000 milliseconds to match the new default MKA transmit interval of the SRX380 device.

  [See transmit-interval (MACsec).]

Intrusion Detection and Prevention

- **Intelligent offload state (SRX Series)**—We've introduced a new field in the **show security idp status** command to see the status of the IDP Intelligent offload.

  [See show security idp status.]

Junos XML API and Scripting

- **The jcs:invoke() function supports suppression of root login and logout events in system log files for SLAX commit scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The **jcs:invoke()** extension function supports the **no-login-logout** parameter in SLAX commit scripts. If you include the parameter, the function does not generate and log **UI_LOGIN_EVENT** and **UI_LOGOUT_EVENT** messages when the script logs in as root to execute the specified remote procedure call (RPC). If you omit the parameter, the function behaves as in earlier releases in which the root **UI_LOGIN_EVENT** and **UI_LOGOUT_EVENT** messages are included in system log files.

  [See invoke() Function (SLAX and XSLT).]

- **The jcs:invoke() function supports suppression of root login and logout events in system log files for SLAX event scripts (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The **jcs:invoke()** extension function supports the **no-login-logout** parameter in SLAX event scripts. If you include the parameter, the function does not generate and log **UI_LOGIN_EVENT** and **UI_LOGOUT_EVENT** messages when the script logs in as root to execute the specified remote procedure call (RPC). If you omit the parameter, the function behaves as in earlier releases in which the root **UI_LOGIN_EVENT** and **UI_LOGOUT_EVENT** messages are included in system log files.

  [See invoke() Function (SLAX and XSLT).]

- **Python 2.7 deprecation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, devices running Junos OS no longer support Python 2.7. We've deprecated the corresponding **language python** statement at the **[edit system scripts]** hierarchy level. To execute Python scripts, configure the **language python3** statement at the **[edit system scripts]** hierarchy level to execute the scripts using Python 3.

  [See Understanding Python Automation Scripts for Devices Running Junos OS.]

Network Management and Monitoring

- **Support for specifying the YANG modules to advertise in the NETCONF capabilities and supported schema list (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—You can configure devices to emit third-party, standard, and Junos OS native YANG modules in the capabilities exchange of a NETCONF session by configuring the appropriate statements at the **[edit system services netconf hello-message yang-module-capabilities]** hierarchy level. In addition, you can specify the YANG schemas that the NETCONF server should include in its list of supported schemas by configuring the appropriate statements at the **[edit system services netconf netconf-monitoring netconf-state-schemas]** hierarchy level.

  [See hello-message and netconf-monitoring.]

- **Support for disconnecting unresponsive NETCONF-over-SSH clients (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—You can enable devices to automatically disconnect unresponsive NETCONF-over-SSH clients by configuring the **client-alive-interval** and **client-alive-count-max** statements at the **[edit system services netconf ssh]** hierarchy level. The **client-alive-interval** statement specifies the timeout interval in seconds, after which, if no data has been received from the client, the device requests a response. The **client-alive-count-max** statement specifies the threshold of missed client-alive responses that triggers the device to disconnect the client, thereby terminating the NETCONF session.

  [See ssh (NETCONF).]

User Interface and Configuration

- **Verbose format option to export JSON configuration data (ACX Series, EX Series, MX Series, PTX Series, QFX Series, and SRX Series)**—The Junos OS CLI exposes the **verbose** statement at the **[edit system export-format json]** hierarchy level. We changed the default format to export configuration data in JavaScript Object Notation (JSON) from **verbose** to **ietf** starting in Junos OS Release 16.1R1. You can explicitly specify the default export format for JSON configuration data by configuring the appropriate statement at the **[edit system export-format json]** hierarchy level. Although the **verbose** statement is exposed in the Junos OS CLI as of the current release, you can configure this statement starting in Junos OS Release 16.1R1.

  [See export-format.]

VPNs

- **Support for trace options log levels (SRX5400, SRX5600, and SRX5800)**—You can configure the log levels using the **level (all | error | info | notice | verbose | warning)** statement at the **edit security ike traceoptions** hierarchy level for troubleshooting the IKE issues.

  [See traceoptions].

- **View the traffic selector type for an IPsec tunnel (SRX Series and MX Series)**—You can run the **show security ipsec security-associations detail** command to display the traffic selector type for a VPN. The **show security ipsec security-associations detail** command displays **proxy-id** or **traffic-selector** as a value for the **TS Type** output field based on your configuration.

  [See show security ipsec security-associations.]

Known Limitations

Learn about known limitations in this release for SRX Series devices.

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

Authentication and Access Control

- Unified access control drops packet at uac-plugin receives interest check event when jbuf is null. When flow get uac return value (some value indicated drop), flow would drop packet and log again. Normally when flow did the log, it will check the flag on jbuf. The flag would tell flow this drop had been logged and then flow won't log again. But for this UAC test case, the jbuf was not there hence no flag can be set so two logs were seen. PR1555850

Flow-Based and Packet-Based Processing

- For accelerated flows, the packet or byte counters in the session_close log and show session output take into account only those values that accumulated while traversing the NP. PR1546430

General Routing

- In SRX380 MACsec show security macsec statistics command, when encryption-offset is enabled, encrypted bytes and encrypted packets will include both encrypted and protected bytes. PR1534840

- Due to enhancements in AppID starting in Junos OS Release 21.1R1, database files are not compatible with earlier releases. Hence, this issue is expected to be seen during downgrade from 21.1R1 to previous Junos OS releases. PR1554490

VPNs

- In SPC2 and SPC3 mixed-mode HA deployments, tunnel per second (TPS) is getting affected while dead peer detection (DPD) is being served on existing tunnels. This limitation is due to a large chunk of CPU being occupied by infrastructure (gencfg) used by IKED to synchronize its DPD state to the backup nodes. PR1473482

Open Issues

Learn about open issues in this release for SRX Series devices.

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

General Routing

- PKI CMPv2 (RFC 4210) client certificate enrollment does not properly work on SRX Series devices when using root-CA. PR1549954
- Kernel might stop, with VM core files generated, and the system might reboot continuously after five child interfaces are added to the reth interface on one node. This might cause service impact. PR1551297
- When the device is downgraded to earlier than Junos OS Release 21.1 and then upgraded again to Junos OS Release 21.1, the appiddb tables might not get populated properly and have 0 entries. For such cases, after upgrading, uninstall and reinstall signature package. PR1567199

Routing Policy and Firewall Filters

- If a huge number of policies are configured on SRX Series devices and some policies are changed, the traffic that matches the changed policies might be dropped. PR1454907

VPNs

- When multiple traffic selectors are configured on a particular VPN, the iked process checks for a maximum of one DPD probe that is sent to the peer for the configured DPD interval. The DPD probe is sent to the peer if traffic flows over even one of the tunnels for the given VPN object. PR1366585
- In the output of the show security ipsec inactive-tunnels command, Tunnel Down Reason is not displayed as this functionality is not supported in Junos OS Release 18.2R2 and later. PR1383329
- On SRX5400, SRX5600, and SRX5800 devices with an SPC3 card, a new behavior has been introduced that differs from the behavior on the older SPC2 card. The SRX Series device with AutoVPN configuration can now accept multiple IPsec tunnels from a peer device (with the same source IP address and port number) using different IKE IDs. PR1407356

- On SRX5400, SRX5600, and SRX5800 devices, during in-service software upgrade (ISSU), the IPsec tunnels flap, causing a disruption of traffic. The IPsec tunnels recover automatically after the ISSU process is completed. PR1416334

- Tunnel debugging configuration is not synchronized to the backup node. It needs to be configured again after RG0 failover. PR1450393

- An IPsec policy must not have both ESP and AH proposals. The configuration will commit, but the IPsec traffic will not work. Do not configure an IPsec policy with proposals using both ESP and AH protocols. PR1552701

- Do not configure two traffic selectors for the same peer under the same IPsec VPN with the same values. PR1554533

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for SRX Series devices.

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

Resolved Issues: 21.1R1

Chassis Clustering

- Disabled node on SRX cluster sent out ARP request packets. PR1548173

- SPU process stop might be seen under a GPRS tunneling protocol scenario. PR1559802

Flow-Based and Packet-Based Processing

- When no logical system or tenant system flow trace is configured and no root-override is configured, the latest behavior is to not log any flow trace for that logical system or tenant system, instead of dumping all to root flow trace as before. PR1530904

- THR capacity update on SRX Series devices. PR1538058
- The rst-invalidate-session command does not work if configured together with the no-sequence-check command. PR1541954
- Application fragmented traffic might get dropped on SRX Series devices. PR1543044
- Instability with RGs on cluster. PR1550637
- Adjust the default route change timeout value. PR1553621
- The usp_max_tcplib_connection is not expected on SRX1500, SRX4100, and SRX4200 devices. PR1563881

General Routing

- On the SRX1500 device, the traffic rate shown in the CLI command is not accurate. PR1527511
- The MAC table is null in Layer 2 mode after one pass-through session is created successfully. PR1528286
- The firewall filter SA and DA tags are not in the log messages as expected in port details. PR1539338
- Packet drop might be seen when a packet with destination port 0 is received on the SRX380 device. PR1540414
- Tail drops might occur on SRX Series devices if shaping-rate is configured on lt- interface. PR1542931
- The nsd process might stop when DNS-based allowlisting is configured under SSL proxy. PR1542942
- The Wi-Fi Mini-Physical Interface Module (Mini-PIM) does not support pure g mode with 2.4-GHz radio. PR1543824
- The output of the show services application-identification group detail command incorrectly included Micro-Applications (Micro-Apps) in the output of every group. PR1544727
- On SRX4100 and SRX4200 devices, if PEM0 is removed, the output of jnxOperatingDescr.2 might be incomplete. PR1547053
- Advanced anti-malware file or e-mail statistics does not get incremented with the latest PB version. PR1547094
- Continuous "LCC: ch_cluster_lcc_set_context:564: failed to lock chassis_vmx mutex 11" chassisd logs generated. PR1547953
- Lcmd log "gw_cb_presence:136: PEM(slot = 0): error detecting presence (fruid = 15, drv_id = 30, status = -11)" generated every second on the SRX4100 and SRX4200. PR1550249

- On SRX1500, SRX-SFP-1GE-T (Part#740-013111) for a copper cable might be corrupted after reboot. PR1552820
- The volume displayed in traffic map are redefined. PR1553066
- The speed mismatch error is seen while trying to commit reth0 with gigether-options. PR1553888
- An IPFD core file might be generated when using Adaptive Threat Profiling. PR1554556
- On an SRX550M device, the dumpdisklabel command fails with message "ERROR: Unknown platform srx550m." PR1557311
- AppID's Unknown Packet Capture utility does not function on SRX Series devices when enhanced-services mode is enabled. PR1558812
- The show security log report top session-close group-by application order-by risk top-number 8 where-application-risk high xml encapsulation structure changed and caused script fail. PR1559013
- The show security log report top idp group-by threat-severity order-by count top-number 5 where-attack command display will change the idp reporting to match the threat-severity in idp log.. PR1560027
- High CPU usage on pkid process might be seen when the device is unable to connect to a particular CRL URL. PR1560374
- The DNS commands may not be executed and also any new configuration may not take effect on connecting the SRX Series device to Juniper ATP Cloud. PR1561169
- There is an idpd core file at ../../../../../../../src/junos/secure/usr.sbin/idp-confd/idpd_lsys.c:771. PR1561298
- When multiple IRB interfaces belong to the same VRRP group ID, if one of IRB intefaces goes down, it causes disruption in traffic going through another IRB interface. PR1572920

Interfaces and Chassis

- When SRX Series devices receive proxy ARP requests on VRRP interfaces, the devices send ARP replies with the underlying interface MAC address. PR1526851
- Backup Routing Engine or backup node may be stuck in bad status with an improper backup-router configuration. PR1530935

Intrusion Detection and Prevention (IDP)

- The greater than or less than symbols are allowed for age-of-attack filter of dynamic attack group configuration. The age-of-attack field in signatures will be changed to CVE dates from activation dates.

  PR1397599

- The flowd or srxpfe process might generate core files during the idpd process commit on SRX Series devices. PR1521682

- IDP now supports the ability to create dynamic-attack-groups based on attack-prefix wildcards. For example, you can include all of the Metasploit-based scans by applying this filter to a dynamic-attack-group: set attack-prefix values SCAN:METASPLOIT:*. PR1537195

- SOF support for partial packet plugins on traditional or unified policy. PR1542497

- Need syslog to indicate signature download completion. PR1543571

- IDP policy load might fail post image upgrade for Junos OS Release 15.1X49 releases. PR1546542

- The idpd process crashes and generates a core file. PR1547610

J-Web

- Sometimes, when you edit the local gateway in the remote access VPN workflow under VPN>IPsec VPN, J-web might not display one or more drop-down values. PR1521788

- J-Web browser tab title to include product model name and hostname. PR1523760

- J-Web GUI does not allow you to save the rules with more than 2500 cumulative shared objects. PR1540047

- After commit pending changes message is shown, the contents of other messages, landing page, or pop-ups will not be visible completely. PR1554024

Layer 2 Ethernet Services

- The RG1 interface failover occurs when RG0 failover is triggered. PR1366825

Platform and Infrastructure

- Syslog reporting PFE_FLOWD_SELFPING_PACKET_LOSS: Traffic impact: Selfping packets loss/err: 300 within 600 second error messages in node 0 and node 1 control panel. PR1522130

- The commit might not fail as expected when reth interface is deleted. PR1538273

Routing Policy and Firewall Filters

- Traffic might be dropped unexpectedly when the url-category match condition is used on a security policy. PR1546120
- Global policies working with multi-zones cause high Packet Forwarding Engine CPU utilization. PR1549366
- Policy configured with the route-active-on condition may work incorrectly for local routes. PR1549592
- NSD process stops when the secprofiling feed name is 64 bytes. PR1549676
- The junos-defaults construct within a unified-policies application match criteria now restricts the ports and protocols of a flow on a per-dynamic-application basis. PR1551984
- Unified policies in global zone contexts do not work when from-zone or to-zone is defined. PR1558009
- On the SRX5000 line of devices, the secondary node might get stuck in performing ColdSync after a reboot or upgrade, or if ISSU is performed. PR1558382
- The traffic may be dropped if you insert one global policy above others on SRX Series devices. PR1558827

Subscriber Access Management

- Incorrect counter type (counter instead of gauge) specified for some values in MIB jnxUserAAAMib. PR1533900

Unified Threat Management (UTM)

- Stream buffer memory leak might happen when UTM is configured under unified policies. PR1557278
- UTM license expiry event lost may cause the device can't quit advance service mode and maximum-sessions decreased by half. PR1563874

User Interface and Configuration

- The outbound-ssh routing-instance is shown as unsupported. PR1558808

VPNs

- The output of show security ipsec security-associations command might display empty space instead of keyword null for encryption algorithm. PR1507270
- On all SRX Series devices using IPsec with NAT traversal, MTU size for the external interface might be changed after IPsec SA is reestablished. PR1530684
- After IPsec tunnel using policy-based VPN is overwritten by another VPN client, traffic using this IPsec tunnel will be dropped. PR1546537
- Traffic going through a policy-based IPsec tunnel might be dropped after RG0 failover. PR1550232
- The iked process may crash with L3HA setup. PR1559121
- The iked process might crash by operational commands on the SRX5000 line of devices with SRX5000-SPC3 card installed. PR1566649

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

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

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

For information about ISSU, see the Chassis Cluster User Guide for Security Devices.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19,4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.1.

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

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

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

Junos OS Release Notes for vMX

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for vMX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

Network Management and Monitoring

- **Operational command RPCs support returning JSON and XML output in minified format in NETCONF sessions (ACX1000, ACX1100, ACX2100, ACX4000, ACX5048, ACX5096, ACX5448, EX2300, EX2500, EX3400, EX4300, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48P, EX4400-48T, EX4600, EX4650, EX9200, MX104, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10001, PTX10002, PTX10008, PTX10016, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX10002, QFX10002-60C, QFX10008, QFX10016, SRX550, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, operational command RPCs, including the **<get-configuration>** RPC, support the **format="json-minified"** and **format="xml-minified"** attributes in NETCONF sessions to return JSON or XML output in minified format. Minified format removes any characters that are not required for computer processing—for example, unnecessary spaces, tabs, and newlines. Minified format decreases the size of the data, and as a result, can reduce transport costs as well as data delivery and processing times.

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

Software Installation and Upgrade

- **request system software status command (MX480, MX960, MX2010, MX2020, SRX1500, SRX4100, SRX4400, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, you can use the CLI command **request system software status** to view the status of the software package installation or uninstallation on the local Routing Engine.

What's Changed

IN THIS SECTION

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

What's Changed in Release 21.1R1

IN THIS SECTION

Junos XML API and Scripting

- **Python 2.7 deprecation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, devices running Junos OS no longer support Python 2.7. We've deprecated the corresponding **language python** statement at the **[edit system scripts]** hierarchy level. To execute Python scripts, configure the **language python3** statement at the **[edit system scripts]** hierarchy level to execute the scripts using Python 3.

  [See Understanding Python Automation Scripts for Devices Running Junos OS.]

Network Management and Monitoring

- **Change in license bandwidth command on vMX virtual routers**

  —Starting in Junos OS, to use the available license bandwidth, explicitly set the license bandwidth use the set chassis license bandwidth <In Mbps> command.

  [See Configuring Licenses on vMX Virtual Routers.]

- **Support for disconnecting unresponsive NETCONF-over-SSH clients (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—You can enable devices to automatically disconnect unresponsive NETCONF-over-SSH clients by configuring the **client-alive-**

interval and **client-alive-count-max** statements at the **[edit system services netconf ssh]** hierarchy level. The **client-alive-interval** statement specifies the timeout interval in seconds, after which, if no data has been received from the client, the device requests a response. The **client-alive-count-max** statement specifies the threshold of missed client-alive responses that triggers the device to disconnect the client, thereby terminating the NETCONF session.

[See ssh (NETCONF).]

Known Limitations

There are no known limitations for vMX in Junos OS Release 21.1R1.

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

Open Issues

Learn about open issues in this release for vMX.

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

Platform and Infrastructure

- On vMX, the blockpointer in the ktree is getting corrupted leading to core-file generation. There is no function impact such as fpc restart or system down and the issue is not seen in hardware setups. PR1525594

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for vMX.

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

Resolved Issues: 21.1R1

General Routing

- Multiple vmxt core files might be generated on vMX platforms. PR1534641
- The riot forwarding process pause might be seen on vMX platforms configured with an IRB interface. PR1544856
- Observed ping failure on vMX while verifying SCU accounting. PR1569047

Upgrade Instructions

You cannot upgrade Junos OS for the vMX router from earlier releases using the **request system software add** command.

You must deploy a new vMX instance using the downloaded software package.

Remember to prepare for upgrades with new license keys and/or deploying Agile License Manager.

Junos OS Release Notes for vRR

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for vRR. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

There are no new features for vRR in Junos OS Release 21.1R1.

What's Changed

IN THIS SECTION

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

What's Changed in Release 21.1R1

There are no changes in behavior or syntax for vRR in Junos OS Release 21.1R1.

Known Limitations

There are no known limitations for vRR in Junos OS Release 21.1R1.

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

To learn more about common BGP or routing known limitations in Junos OS 21.1R1, see "Known Limitations" on page 121 for MX Series routers.

Open Issues

There are no known issues for vRR in Junos OS Release 21.1R1

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

To learn more about common BGP or routing knowns issues in Junos OS 21.1R1, see "Open Issues" on page 124 for MX Series routers.

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for vRR.

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

Resolved Issues: 21.1R1

To learn more about common BGP or routing resolved issues in Junos OS 21.1R1, see "Resolved Issues: 21.1R1" on page 133 for MX Series routers.

Routing Protocols

- BGP flap and rpd crash might be observed. PR1545837
- 6PE prefixes may not be removed from the RIB upon reception of withdrawal from a BGP neighbor when RIB sharding is enabled. PR1556271

Junos OS Release Notes for vSRX

IN THIS SECTION

These release notes accompany Junos OS Release 21.1R1 for vSRX. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

What's New

IN THIS SECTION

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

Authentication and Access Control

- **Configure client information to connect to the JIMS server (cSRX, SRX300, SRX340, SRX345, SRX1500, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, and vSRX)**—Starting with Junos OS Release 21.1R1, you can configure which specifc interface, source IP address or routing instance SRX should use for connecting to a JIMS server.

  [See Configuring the Connection to an SRX Series Device.]

- **LLDP support in Layer 3 mode (vSRX 3.0)**—Starting in Junos OS Release 21.1R1, vSRX 3.0 in Layer 3 mode supports Link Layer Discovery Protocol (LLDP) to learn and distribute device information on network links. The device information enables the vSRX 3.0 to identify a variety of devices quickly. This quick identification results in a LAN that interoperates smoothly and efficiently.

  [See Device Discovery Using LLDP and LLDP-MED on Switches and lldp.]

Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud)

- **Support for username feed type in adaptive threat profiling (SRX Series devices and vSRX)**—Starting in Junos OS Release 21.1R1, you can add the user source identity (username) as a feed type in adaptive threat profiling. Use the **add-source-identity-to-feed** ***user-identity*** and **add-destination-identity-to-feed** ***user-identity*** commands at the **[edit security policies from-zone** ***zone-name*** **to-zone** ***zone-name*** **policy** ***policy-name*** **then [permit|deny|reject] application-services]** hierarchy level to configure the username feed type.

  [See security-intelligence (security policies), show services security-intelligence sec-profiling-feed status and show services security-intelligence category.]

- **Support for Juniper ATP Cloud services in VXLAN tunnel inspection (SRX4000 line of devices, SRX5000 line of devices, and vSRX)**—Starting in Junos OS Release 21.1R1, the listed SRX Series devices and vSRX support Juniper ATP Cloud services such as AAMW and SecIntel in VXLAN tunnel traffic inspection. These services inspect the VXLAN traffic only if there is a security policy configured to perform the inspection. When you configure VXLAN tunnel inspection policies on an SRX Series device, the device scans the VXLAN tunnel traffic through AAMW and SecIntel services.

  [See tunnel-inspection and show security flow session.]

- **Policy-based threat profiling (SRX Series devices and vSRX)**—Starting in Junos OS Release 21.1R1, you can add the user source identity (username) to a security policy to generate security feeds.

  Juniper ATP Cloud service consolidates the generated feeds from SRX Series device and shares the duplicated results back with that security device. The security device uses the feeds to perform actions against the designated traffic. You can enable the security device to use the feeds by configuring security policies with the feeds as matching criteria. When traffic matches policy conditions, the device applies policy actions.

  [See Threat Profiling Support in Security Policy.]

Licensing

- **Juniper Agile Licensing (vSRX)—**

  Starting in Junos OS Release 21.1R1, we're moving toward supporting license-based software features. We now use Juniper Agile Licensing to support soft enforcement for virtual CPU (vCPU) usage on vSRX. With soft enforcement, you can use more vCPUs than the number of vCPU licenses you are entitled to use. However, if you do that, the device generates an alarm. You can see the list of alarms at System Log Explorer.

  Juniper Agile Licensing provides simplified and centralized license administration and deployment. You can use Juniper Agile Licensing to install and manage licenses for hardware and software features.

  "Table 10" on page 249 describes the licensing support for vSRX.

  Table 10: Licensed Features on vSRX

vSRX License Model	Use Case Examples or Solutions	Number of vCPUs Required	Feature List
Standard	Use for standard firewall and secure branch routers	2, 5, 9, 17, or 32 virtual CPUs (vCPUs)	Application Layer Gateways (ALGs), BGP, class of service (CoS), DHCP, diagnostics, firewall, GRE, IP tunneling, IPv4 and IPv6, J-Flow, management (J-Web, CLI, and NETCONF), MPLS, multicast, NAT, on-box logging, OSPF, screens, site-to-site VPN, static routing, and user firewall
Advanced	Advanced 1 Use for data center security	2, 5, 9, 17, or 32 vCPUs	Includes Standard features plus IPS and application security (application identification, application firewall, application quality of service, and application tracking)

Table 10: Licensed Features on vSRX *(Continued)*

vSRX License Model	Use Case Examples or Solutions	Number of vCPUs Required	Feature List
	Advanced 2 Use for next-generation firewall with cloud-based antivirus	2, 5, 9, 17, or 32 vCPUs	Includes Standard and Advanced 1 features, Sophos antivirus, Web filtering, antispam, and content filtering
	Advanced 3 Use for next-generation firewall with on-box antivirus	2, 5, 9, 17, or 32 vCPUs	Includes Standard and Advanced 1 features, Avira antivirus, Web filtering, antispam, and content filtering
Premium	Premium 1 Use for data center security and Juniper Advanced Threat Prevention Cloud (Juniper ATP Cloud)	2, 5, 9, 17, or 32 vCPUs	Includes Standard and Advanced 1 features, and Juniper ATP Cloud
	Premium 2 Use for next-generation firewall and Juniper ATP Cloud	2, 5, 9, 17, or 32 vCPUs	Includes Standard and Advanced 2 features, and Juniper ATP Cloud
	Premium 3 Use for next-generation firewall and Juniper ATP Cloud	2,5,9, 17, or 32 vCPUs	Includes Standard and Advanced 3 features, and Juniper ATP Cloud

[See Flex Software License for vSRX, Juniper Agile Licensing Guide, and Configuring Licenses in Junos OS.]

Network Management and Monitoring

- **Operational command RPCs support returning JSON and XML output in minified format in NETCONF sessions (ACX1000, ACX1100, ACX2100, ACX4000, ACX5048, ACX5096, ACX5448, EX2300, EX2500, EX3400, EX4300, EX4400-24P, EX4400-24T, EX4400-48F, EX4400-48P, EX4400-48T, EX4600, EX4650, EX9200, MX104, MX204, MX240, MX480, MX960, MX2008, MX2010, MX2020, MX10003, MX10008, MX10016, PTX1000, PTX5000, PTX10001, PTX10002, PTX10008, PTX10016, QFX5100, QFX5110, QFX5120, QFX5200, QFX5210, QFX10002, QFX10002-60C, QFX10008, QFX10016, SRX550, SRX4100, SRX4200, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, operational command RPCs, including the **<get-configuration>** RPC, support the **format="json-minified"** and **format="xml-minified"** attributes in NETCONF sessions to return JSON or XML output in minified format. Minified format removes any characters that are not required for computer processing—for example, unnecessary spaces, tabs, and newlines. Minified format decreases the size of the data, and as a result, can reduce transport costs as well as data delivery and processing times.

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

Software Installation and Upgrade

- **Phone-home client (vSRX)**—Starting in Junos OS Release 21.1R1, the phone-home client (PHC) is responsible for the initial bootup and configuration of the vSRX VM instance when the virtual machine (VM) instance is turned on. When the vSRX VM instance boots up with the factory-default configuration, the phone-home client connects to a redirect server, which then redirects to the phone-home serverr. The phone-home client downloads the initial configuration and the latest Junos OS image from the phone-home server. .The new image is installed first, and then the initial configuration is applied and committed on the vSRX VM instance.

  If the redirect server does not provide any phone-home server information, the phone-home client restarts the provisioning process and keeps connecting to the redirect server until provisioning is successful.

  [See Obtaining Configurations and Software Image Without User Intervention Using Phone-Home Client.]

- **request system software status command (MX480, MX960, MX2010, MX2020, SRX1500, SRX4100, SRX4400, SRX4600, SRX5400, SRX5600, SRX5800, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, you can use the CLI command **request system software status** to view the status of the software package installation or uninstallation on the local Routing Engine.

VPNs

- **Increased tunnel scaling (vSRX 3.0)**—Starting in Junos OS Release 21.1R1, vSRX 3.0 is supported by a new architecture similar to SRX5000 line of devices with SPC3 which increases the tunnel scale.

vSRX 3.0 instances support the IPsec VPN features that are supported on the SRX5000 line of devices with SPC3 (SRX5K-SPC3).

By default, when the vSRX 3.0 boots up, the legacy architecture is executed. To enable the new architecture, you must load and install a new package, junos-ike. The Junos OS releases includes this package, but its installation is optional. As an administrator, you must execute the **request system software add optional://junos-ike.tgz** command to load the junos-ike package.

[See IPsec VPN Features and Configurations Not Supported on SRX5K-SPC3 and vSRX Instances.]

What's Changed

IN THIS SECTION

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

What's Changed in Release 21.1R1

IN THIS SECTION

Junos XML API and Scripting

- **Python 2.7 deprecation (ACX Series, EX Series, MX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—Starting in Junos OS Release 21.1R1, devices running Junos OS no longer support Python 2.7. We've deprecated the corresponding **language python** statement at the **[edit system scripts]** hierarchy level. To execute Python scripts, configure the **language python3** statement at the **[edit system scripts]** hierarchy level to execute the scripts using Python 3.

  [See Understanding Python Automation Scripts for Devices Running Junos OS.]

Network Management and Monitoring

- **Support for disconnecting unresponsive NETCONF-over-SSH clients (ACX Series, EX Series, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, and vSRX)**—You can enable devices to automatically disconnect unresponsive NETCONF-over-SSH clients by configuring the **client-alive-interval** and **client-alive-count-max** statements at the **[edit system services netconf ssh]** hierarchy level. The **client-alive-interval** statement specifies the timeout interval in seconds, after which, if no data has been received from the client, the device requests a response. The **client-alive-count-max** statement specifies the threshold of missed client-alive responses that triggers the device to disconnect the client, thereby terminating the NETCONF session.

  [See ssh (NETCONF).]

Known Limitations

Learn about known limitations in this release for vSRX.

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

Platform and Infrastructure

- For SaaS DBs among all available links a best path chosen. If the link has no violation, and is the preferred link and has the highest prioty among all live links, any further configuration change won't be recognized. The recommendation to the user is to configure all the preferences and priorities during configuration time so that all of it can be properly honored. PR1559662

Open Issues

Learn about open issues in this release for vSRX.

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

Platform and Infrastructure

- When the device is downgraded to a release earlier than Junos OS Release 21.1 and then upgraded again to Junos OS Release 21.1, the appiddb tables might not get populated properly and have 0 entries. For such cases, after upgrading, uninstall and reinstall signature package. PR1567199

Resolved Issues

IN THIS SECTION

Learn which issues were resolved in the Junos OS main and maintenance releases for vSRX.

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

Resolved Issues: 21.1R1

General Routing

- The control link might be broken when there is excessive traffic load on the control link in a vSRX cluster deployment. PR1524243

- The master-password configuration is rejected if master-encryption-password (MEK) is not set. PR1537251

- The srxpfe process might crash when the Application Identification Packet-Capture functionality is enabled. PR1538991

- Upgrading to Junos OS Release 20.4R1 or later releases with a large, preexisting security-log database might result in LLMD consuming large amounts of CPU. PR1548423

- Configuration integrity mismatch error in vSRX3.0 running on Azure with key-vault integrated. PR1551419

- The command set protocols l2-learning global-mode is removed on vSRX3.0. Use the show ethernet-switching global-information command. PR1554388

- High CPU usage on pkid process might be seen when the device is unable to connect to a particular CRL URL. PR1560374

Intrusion Detection and Prevention (IDP)

- The flowd or srxpfe process might generate core files during the idpd process commit on SRX Series devices. PR1521682

- On vSRX3.0 the attack-group-entries filters direction 0 limit 1 command is not showing expected values. PR1564761

J-Web

- The J-Web GUI does not allow you to save the rules with more than 2500 cumulative shared objects. PR1540047
- After commit pending changes message is shown, the contents of other messages, landing page, or pop-upsare not visible completely. PR1554024

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

This section contains information about how to upgrade Junos OS for vSRX using the CLI. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

You also can upgrade to Junos OS Release 21.1R1 for vSRX using J-Web (see J-Web) or the Junos Space Network Management Platform (see Junos Space).

Direct upgrade of vSRX from Junos OS 15.1X49 Releases to Junos OS Releases 17.4, 18.1, 18.2, 18.3,18.4, 19.1, 19.2 and 19.4 is supported.

The following limitations apply:

- Direct upgrade of vSRX from Junos OS 15.1X49 Releases to Junos OS Release 19.3 and higher is not supported. For upgrade between other combinations of Junos OS Releases in vSRX and vSRX 3.0, the general Junos OS upgrade policy applies.
- The file system mounted on /var usage must be below 14% of capacity.

Check this using the following command:

```
show system storage | match " /var$" /dev/vtbd1s1f
 2.7G         82M        2.4G         3%   /var
```

Using the **request system storage cleanup** command might help reach that percentage.

- The Junos OS upgrade image must be placed in the directory /var/host-mnt/var/tmp/. Use the **request system software add /var/host-mnt/var/tmp/<upgrade_image>**
- We recommend that you deploy a new vSRX virtual machine (VM) instead of performing a Junos OS upgrade. That also gives you the option to move from vSRX to the newer and more recommended vSRX 3.0.
- Ensure to back up valuable items such as configurations, license-keys, certificates, and other files that you would like to keep.

NOTE: For ESXi deployments, the firmware upgrade from Junos OS Release 15.1X49-Dxx to Junos OS releases 17.x, 18.x, or 19.x is not recommended if there are more than three network adapters on the 15.1X49-Dxx vSRX instance. If there are more than three network adapters and you want to upgrade, then we recommend that you either delete all the additional network adapters and add the network adapters after the upgrade or deploy a new vSRX instance on the targeted OS version.

Upgrading Software Packages

To upgrade the software using the CLI:

1. Download the **Junos OS Release 21.1R1 for vSRX .tgz** file from the Juniper Networks website. Note the size of the software image.
2. Verify that you have enough free disk space on the vSRX instance to upload the new software image.

```
root@vsrx> show system storage
       Filesystem              Size       Used       Avail  Capacity   Mounted
on
       /dev/vtbd0s1a           694M       433M       206M        68%  /
       devfs                   1.0K       1.0K         0B       100%  /dev
       /dev/md0                1.3G       1.3G         0B       100%  /junos
```

```
        /cf                         694M        433M        206M        68%   /junos/cf
        devfs                       1.0K        1.0K          0B       100%   /junos/
dev/
        procfs                      4.0K        4.0K          0B       100%   /proc
        /dev/vtbd1s1e               302M         22K        278M         0%   /config
        /dev/vtbd1s1f               2.7G         69M        2.4G         3%   /var
        /dev/vtbd3s2                 91M        782K         91M         1%   /var/host
        /dev/md1                    302M        1.9M        276M         1%   /mfs
        /var/jail                   2.7G         69M        2.4G         3%   /jail/var
        /var/jails/rest-api           2.7G         69M        2.4G         3%   /web-api/
var
        /var/log                    2.7G         69M        2.4G         3%   /
jail/var/log
        devfs                       1.0K        1.0K          0B       100%   /jail/dev
        192.168.1.1:/var/tmp/corefiles       4.5G        125M        4.1G
3%   /var/crash/corefiles
        192.168.1.1:/var/volatile       1.9G        4.0K        1.9G
0%   /var/log/host
        192.168.1.1:/var/log       4.5G        125M        4.1G      3%   /var/log/
hostlogs
        192.168.1.1:/var/traffic-log       4.5G        125M        4.1G
3%   /var/traffic-log
        192.168.1.1:/var/local       4.5G        125M        4.1G    3%   /var/db/
host
        192.168.1.1:/var/db/aamwd       4.5G        125M        4.1G
3%   /var/db/aamwd
        192.168.1.1:/var/db/secinteld       4.5G        125M        4.1G
3%   /var/db/secinteld
```

3. Optionally, free up more disk space, if needed, to upload the image.

```
root@vsrx> request system storage cleanup
        List of files to delete:
        Size Date       Name
        11B Sep 25 14:15 /var/jail/tmp/alarmd.ts
        259.7K Sep 25 14:11 /var/log/hostlogs/vjunos0.log.1.gz
        494B Sep 25 14:15 /var/log/interactive-commands.0.gz
        20.4K Sep 25 14:15 /var/log/messages.0.gz
        27B Sep 25 14:15 /var/log/wtmp.0.gz
        27B Sep 25 14:14 /var/log/wtmp.1.gz
        3027B Sep 25 14:13 /var/tmp/BSD.var.dist
        0B Sep 25 14:14 /var/tmp/LOCK_FILE
```

```
        666B Sep 25 14:14 /var/tmp/appidd_trace_debug
        0B Sep 25 14:14 /var/tmp/eedebug_bin_file
        34B Sep 25 14:14 /var/tmp/gksdchk.log
        46B Sep 25 14:14 /var/tmp/kmdchk.log
        57B Sep 25 14:14 /var/tmp/krt_rpf_filter.txt
        42B Sep 25 14:13 /var/tmp/pfe_debug_commands
        0B Sep 25 14:14 /var/tmp/pkg_cleanup.log.err
        30B Sep 25 14:14 /var/tmp/policy_status
        0B Sep 25 14:14 /var/tmp/rtsdb/if-rtsdb
        Delete these files ? [yes,no] (no) yes
<
output omitted>
```

NOTE: If this command does not free up enough disk space, see [SRX] Common and safe files to remove in order to increase available system storage for details on safe files you can manually remove from vSRX to free up disk space.

4. Use FTP, SCP, or a similar utility to upload the Junos OS Release 21.1R1 for vSRX .tgz file to **/var/crash/corefiles/** on the local file system of your vSRX VM. For example:

```
root@vsrx> file copy ftp://username:prompt@ftp.hostname.net/pathname/
junos-vsrx-x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz /var/crash/
corefiles/
```

5. From operational mode, install the software upgrade package.

```
root@vsrx> request system software add /var/crash/corefiles/junos-vsrx-
x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz no-copy no-validate reboot
Verified junos-vsrx-x86-64-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE signed by
PackageDevelopmentEc_2017 method ECDSA256+SHA256
THIS IS A SIGNED PACKAGE
WARNING:     This package will load JUNOS 20.4 software.
WARNING:     It will save JUNOS configuration files, and SSH keys
WARNING:     (if configured), but erase all other files and information
WARNING:     stored on this machine.  It will attempt to preserve dumps
WARNING:     and log files, but this can not be guaranteed.  This is the
WARNING:     pre-installation stage and all the software is loaded when
WARNING:     you reboot the system.
Saving the config files ...
```

```
Pushing Junos image package to the host...
Installing /var/tmp/install-media-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE.tgz
Extracting the package ...
total 975372
-rw-r--r-- 1 30426 950 710337073 Oct 19 17:31 junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-app.tgz
-rw-r--r-- 1 30426 950 288433266 Oct 19 17:31 junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz
Setting up Junos host applications for installation ...
============================================
Host OS upgrade is FORCED
Current Host OS version: 3.0.4
New Host OS version: 3.0.4
Min host OS version required for applications: 0.2.4
============================================
Installing Host OS ...
upgrade_platform: -------------------
upgrade_platform: Parameters passed:
upgrade_platform: silent=0
upgrade_platform: package=/var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz
upgrade_platform: clean install=0
upgrade_platform: clean upgrade=0
upgrade_platform: Need reboot after staging=0
upgrade_platform: -------------------
upgrade_platform:
upgrade_platform: Checking input /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz ...
upgrade_platform: Input package /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz is valid.
upgrade_platform: Backing up boot assets..
cp: omitting directory '.'
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
initrd.cpio.gz: OK
upgrade_platform: Checksum verified and OK...
/boot
upgrade_platform: Backup completed
upgrade_platform: Staging the upgrade package - /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz..
./
```

```
./bzImage-intel-x86-64.bin
./initramfs.cpio.gz
./upgrade_platform
./HOST_COMPAT_VERSION
./version.txt
./initrd.cpio.gz
./linux.checksum
./host-version
bzImage-intel-x86-64.bin: OK
initramfs.cpio.gz: OK
version.txt: OK
upgrade_platform: Checksum verified and OK...
upgrade_platform: Staging of /var/tmp/junos-srx-mr-
vsrx-20.4-2020-10-12.0_RELEASE_20.4_THROTTLE-linux.tgz completed
upgrade_platform: System need *REBOOT* to complete the upgrade
upgrade_platform: Run upgrade_platform with option -r | --rollback to
rollback the upgrade
Host OS upgrade staged. Reboot the system to complete installation!
WARNING:     A REBOOT IS REQUIRED TO LOAD THIS SOFTWARE CORRECTLY. Use the
WARNING:     'request system reboot' command when software installation is
WARNING:     complete. To abort the installation, do not reboot your system,
WARNING:     instead use the 'request system software rollback'
WARNING:     command as soon as this operation completes.
NOTICE: 'pending' set will be activated at next reboot...
Rebooting. Please wait ...
shutdown: [pid 13050]
Shutdown NOW!
*** FINAL System shutdown message from root@ ***
System going down IMMEDIATELY
Shutdown NOW!
System shutdown time has arrived\x07\x07
```

If no errors occur, Junos OS reboots automatically to complete the upgrade process. You have successfully upgraded to Junos OS Release 21.1R1 for vSRX.

NOTE: Starting in Junos OS Release 17.4R1, upon completion of the vSRX image upgrade, the original image is removed by default as part of the upgrade process.

6. Log in and use the **show version** command to verify the upgrade.

```
--- JUNOS 20.4-2020-10-12.0_RELEASE_20.4_THROTTLE Kernel 64-bit
JNPR-11.0-20171012.170745_fbsd-
At least one package installed on this device has limited support.
Run 'file show /etc/notices/unsupported.txt' for details.
root@:~ # cli
root> show version
Model: vsrx
Junos: 20.4-2020-10-12.0_RELEASE_20.4_THROTTLE
JUNOS OS Kernel 64-bit  [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs [20171012.170745_fbsd-builder_stable_11]
JUNOS OS runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS OS time zone information [20171012.170745_fbsd-builder_stable_11]
JUNOS OS libs compat32 [20171012.170745_fbsd-builder_stable_11]
JUNOS OS 32-bit compatibility [20171012.170745_fbsd-builder_stable_11]
JUNOS py extensions [20171017.110007_ssd-builder_release_174_throttle]
JUNOS py base [20171017.110007_ssd-builder_release_174_throttle]
JUNOS OS vmguest [20171012.170745_fbsd-builder_stable_11]
JUNOS OS crypto [20171012.170745_fbsd-builder_stable_11]
JUNOS network stack and utilities [20171017.110007_ssd-
builder_release_174_throttle]
JUNOS libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Web Management Platform Package [20171017.110007_ssd-
builder_release_174_throttle]
JUNOS srx libs compat32 [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx runtime [20171017.110007_ssd-builder_release_174_throttle]
JUNOS common platform support [20171017.110007_ssd-
builder_release_174_throttle]
JUNOS srx platform support [20171017.110007_ssd-builder_release_174_throttle]
JUNOS mtx network modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp modules [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srxtvp libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx libs [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx Data Plane Crypto Support [20171017.110007_ssd-
builder_release_174_throttle]
JUNOS daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS srx daemons [20171017.110007_ssd-builder_release_174_throttle]
JUNOS Online Documentation [20171017.110007_ssd-builder_release_174_throttle]
```

```
JUNOS jail runtime [20171012.170745_fbsd-builder_stable_11]
JUNOS FIPS mode utilities [20171017.110007_ssd-builder_release_174_throttle]
```

Validating the OVA Image

If you have downloaded a vSRX .ova image and need to validate it, see Validating the vSRX .ova File for VMware.

Note that only .ova (VMware platform) vSRX images can be validated. The .qcow2 vSRX images for use with KVM cannot be validated the same way. File checksums for all software images are, however, available on the download page.

Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases

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

You can upgrade or downgrade to the EEOL release that occurs directly before or after the currently installed EEOL release, or to two EEOL releases before or after. For example, Junos OS Releases 19,4, 20.2, and 20.4 are EEOL releases. You can upgrade from Junos OS Release 19.4 to Release 20.1, 20.2, 20.3 or to 20.4. Or from Junos OS Releases 20.2, 20.3 or 20.4 to Release 21.1.

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

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

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

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.

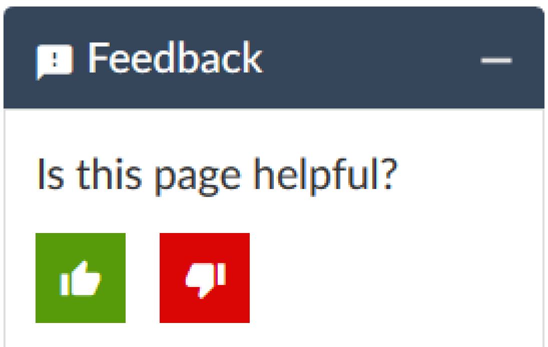
- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about Common Criteria, FIPS, Homologation, RoHS2, and USGv6.

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

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback system—Click TechLibrary Feedback, on the lower right of any page on the Juniper Networks TechLibrary site, and do one of the following:

  - Click the thumbs-up icon if the information on the page was helpful to you.
  - Click the thumbs-down icon if the information on the page was not helpful to you or if you have suggestions for improvement, and use the pop-up form to provide feedback.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable)

Requesting Technical Support

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/
- Create a service request online: https://myjuniper.juniper.net/

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

Creating a Service Request with JTAC

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

- Visit https://myjuniper.juniper.net/
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

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

Revision History

7 April 2021—Revision 4, Junos OS Release 21.1R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

31 March 2021—Revision 3, Junos OS Release 21.1R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

29 March 2021—Revision 2, Junos OS Release 21.1R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.

26 March 2021—Revision 1, Junos OS Release 21.1R1– ACX Series, cRPD, cSRX, EX Series, JRR Series, Juniper Secure Connect, Junos Fusion, MX Series, NFX Series, PTX Series, QFX Series, SRX Series, vMX, vRR, and vSRX.