Junos® OS 12.1 Release Notes

Release 12.1B2
23 February 2012
Revision 5

These release notes accompany Release 12.1B2 of the Junos OS. They describe device documentation and known problems with the software. Junos OS runs on all Juniper Networks M Series, MX Series, and T Series routing platforms, SRX Series Services Gateways, J Series Services Routers, and the EX Series Ethernet Switches.

For the latest, most complete information about outstanding and resolved issues with the Junos OS software, see the Juniper Networks online software defect search application at http://www.juniper.net/prsearch.

You can also find these release notes on the Juniper Networks Junos OS Documentation Web page, which is located at https://www.juniper.net/beta/junos/.

Contents

Junos OS Release Notes for EX Series Switches

New Features in Junos OS Release 12.1 for EX Series Switches

This section describes new features in Release 12.1 of the Junos operating system (Junos OS) for EX Series switches.

Not all EX Series software features are supported on all EX Series switches in the current release. For a list of all EX Series software features and their platform support, see "EX Series Switch Software Features Overview."

New features are described on the following pages:

Hardware

- **New optical transceiver support for EX2200, EX3200, EX4200, EX4500, EX6200, and EX8200 switches**—EX2200, EX3200, EX4200, EX4500, EX6200, and EX8200 switches now support the following optical transceivers:
  - SFP-1G-CWDM-LH (wavelengths: 1470 nm, 1490 nm, 1510 nm, 1530 nm, 1550 nm, 1570 nm, 1590 nm, and 1610 nm)
  - XFP-10G-T-DWDM-ZR (10GBASE-ZA, 80 km; EX3200 and EX4200 Series only)
- **New optical transceiver support for EX3300 switches**—EX3300 switches now support the following transceivers:
  - EX-SFP-1G-CWDM-LH
  - EX-SFP-1GE-LH
  - EX-SFP-1GE-LX40K
  - EX-SFP-1GE-T
  - EX-SFP-10GE-ER
  - EX-SFP-GE10KT13R15
  - EX-SFP-GE10KT15R13
  - EX-SFP-GE10KT13R14
  - EX-SFP-GE10KT14R13
  - EX-SFP-GE40KT13R15
  - EX-SFP-GE40KT15R13
- **Redundant Power System (RPS) support on EX2200 and EX3300 switches**—Unlike other EX Series switches, which support redundant power supplies, EX2200 switches and EX3300 switches have only one power supply. If you deploy one of these switches in a critical situation, we recommend that you connect an RPS to that switch to supply backup power in case a loss of power occurs. RPS is not a primary power supply—it provides backup power to switches only when the single dedicated power supply fails. An RPS operates in parallel with the single dedicated power supplies of the switches connected to it and provides all connected switches with either PoE or non-PoE backup power.
- **New AC power supply support on EX6200 switches**—EX6200 switches now support 5000 W AC power supplies.
- **Enhancements for EX6210 switch line cards and SRE modules**—The EX6210 switch has 10 horizontal slots on the front of the chassis. Slots 0 through 3 and 6 through 9 accept one line card each. You can now install either a line card or a Switch Fabric and Routing (SRE) module in slots 4 and 5. You can install a maximum of nine line cards in a switch in slots 0 though 9; however, at least one SRE module must be installed in the switch.

- **New optical transceiver support for EX8200 switches**—The 40-port SFP+ and 48-port SFP line cards in EX8200 switches now support the following transceivers:
  - EX-SFP-FE20KT13R15
  - EX-SFP-FE20KT15R13
  - EX-SFP-1G-CWDM-LH
  - EX-SFP-GE10KT13R15 (for 40-port SFP+ line cards only)
  - EX-SFP-GE10KT15R13 (for 40-port SFP+ line cards only)
  - EX-SFP-GE40KT13R15
  - EX-SFP-GE40KT15R13
- **New SFP+ active direct attach cable support**—EX Series switches now support the following SFP+ active direct attach cables:
  - EX-SFP-10GE-ACT-1M
  - EX-SFP-10GE-ACT-3M
  - EX-SFP-10GE-ACT-5M
- **LCD panel support for the XRE200 External Routing Engine**—The LCD panel on the XRE200 External Routing Engine can now be used to configure and better monitor the external Routing Engine. You can now navigate to the Maintenance or Status menus using the LCD panel. You can use the Maintenance menu to perform basic maintenance tasks, such as halting or rebooting the external Routing Engine or loading a rescue or factory-default configuration. You can use the Status menu to monitor external Routing Engine status, including monitoring of the Virtual Chassis ports (VCPs), power supplies, temperatures, and the installed Junos OS version.
- **XRE200 External Routing Engine hard disk drive monitoring test**—You can now run a hard disk drive monitoring test on an XRE200 External Routing Engine to check the health of RAID storage and the hard disk drive memory.

Access Control and Port Security

- **EX4500 access control feature enhancements**—EX4500 switches now support 802.1X authentication (port-based, multiple supplicant) and 802.1X authentication with VLAN assignment and voice over IP (VoIP) VLAN support.
- **EX4500 port security feature enhancements**—EX4500 switches now support DHCP snooping, persistent storage for DHCP snooping, and IP source guard.

Class of Service (CoS)

- **Enhancements to policing and rate-limiting**—You can now police and rate-limit traffic to prioritize and rate-limit packets destined for and coming from the CPU on both line cards and Routing Engines.

Converged Networks (LAN and SAN)

- **DCBX support for the application protocol TLV on EX4500 switches**—Support for the Data Center Bridging Capability Exchange protocol (DCBX) on EX4500 switches has been expanded to include support for the application protocol type, length, and value (TLV). This feature allows you to implement DCBX for other Layer 2 and Layer 4 applications in addition to implementing it for Fibre Channel over Ethernet (FCoE) applications. DCBX is required for FCoE applications. While it is not required for other applications, it adds reliability for enterprise data storage. By default, the FCoE application is enabled on DCBX interfaces. To use this feature for other Layer 2 and Layer 4 applications, you must configure an application map and then associate it with the DCBX interface that is carrying the application's traffic.

Ethernet Switching and Spanning Trees

- **Diagnostics and debugging enhancement**—A new command, **show pfe statistics bridge**, displays counts of the number of packets received, the number of ingress packets discarded and the reasons for the discard, and the number of packets transmitted through the egress pipeline of the Packet Forwarding Engine. You can use this information to inform troubleshooting investigations.
- **Edge virtual bridging (EVB)**—EVB is a software capability on a switch running Junos OS that allows multiple virtual machines to communicate with each other and with external hosts in the Ethernet network environment. Servers using virtual Ethernet port aggregator (VEPA) do not send packets directly from one virtual machine (VM) to another. Instead, the packets are sent to virtual bridges on an adjacent switch for processing. EX Series switches use EVB as a virtual bridge to return the packets on the same interface that delivered the packets.
- **Ethernet ring protection switching for EX Series switches**—Ethernet ring protection switching (ERPS), defined by ITU-T G8032, is a mechanism for preventing unwanted loops in Ethernet networks. It is supported on EX2200 and EX4200 switches.

Firewall Filters

- **Support for the vlan action now available on EX8200 standalone switches and Virtual Chassis**—In firewall filter configurations for EX8200 standalone switches, you can now apply the **vlan** action on ports and VLANs for IPv4 and IPv6 ingress traffic. However, the **vlan** action works properly only when the **interface** action modifier is also configured along with the **vlan** action. For EX8200 Virtual Chassis, you can apply the **vlan** action (provided that the **interface** action modifier is also configured) only on VLANs for IPv4 and IPv6 ingress traffic. You can specify the **interface** action modifier to forward matched packets to a specific interface, bypassing the switching lookup. You can specify the **vlan** action to forward matched packets to a specific VLAN.

High Availability

- **GRES for IGMP snooping on EX3300 Virtual Chassis, EX4500 Virtual Chassis, and EX6200 switches**—Graceful Routing Engine switchover (GRES) is now supported for IGMP snooping on these indicated platforms.
- **Nonstop active routing for BGP, IGMP, IS-IS, OSPF, and RIP with BFD on EX3300 Virtual Chassis**—Nonstop active routing (NSR) for OSPF with BFD, RIP with BFD, IS-IS with BFD, BGP with BFD, and IGMP with BFD is now supported on EX3300 Virtual Chassis. You can now configure NSR to enable the transparent switchover between the master and backup Routing Engines without having to restart any of these protocols.
- **Nonstop active routing for PIM on EX8200 switches and Virtual Chassis**—Nonstop active routing (NSR) for Protocol Independent Multicast (PIM) is now supported on EX8200 switches and Virtual Chassis.
- **Nonstop bridging for spanning-tree protocols on EX4500 Virtual Chassis and EX8200 Virtual Chassis**—Nonstop bridging (NSB) for spanning-tree protocols is now supported on EX4500 Virtual Chassis and EX8200 Virtual Chassis. You can now configure NSB to enable the transparent switchover between the master and backup Routing Engines without having to restart any spanning-tree protocol.
- **Nonstop bridging for spanning-tree protocols, LACP, LLDP, and LLDP-MED on EX6200 switches**—Nonstop bridging (NSB) for spanning-tree protocols, Link Aggregation Control Protocol (LACP), Link Layer Discovery Protocol (LLDP), and Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) is now supported on EX6200 switches. You can now configure NSB to enable the transparent switchover between the master and backup Routing Engines without having to restart any of these protocols.
- **Nonstop software upgrade on EX4200 and EX4500 Virtual Chassis**—Nonstop software upgrade (NSSU) is now supported on EX4200 and EX4500 Virtual Chassis.
- **Virtual Chassis fast failover for EX4500 Virtual Chassis and mixed EX4200 and EX4500 Virtual Chassis**—Virtual Chassis fast failover is now supported on Virtual Chassis ports (VCPs) in an EX4500 Virtual Chassis or in a mixed EX4200 and EX4500 Virtual Chassis. The Virtual Chassis fast failover feature is a hardware-assisted failover mechanism that automatically reroutes traffic and reduces traffic loss in the event of a link or switch failure.

Infrastructure

- **Extended DHCP server and extended DHCP relay support**—EX Series switches now support extended DHCP server and extended DHCP relay.
- **Generic routing encapsulation support**—EX3200 and EX4200 switches now support generic routing encapsulation (GRE), a tunneling protocol to transport packets over a network. You can use GRE tunneling services to encapsulate any network layer protocol over any other network layer protocol. Acting as a tunnel source router, the switch encapsulates a payload packet that is to be transported through a tunnel to a destination network. The switch first encapsulates the payload packet in a GRE packet and then encapsulates the resulting GRE packet in a delivery protocol. A switch performing the role of a tunnel remote router extracts the tunneled packet and forwards the packet to the destination network. GRE tunnels can be used to connect noncontiguous networks and to provide options for networks that contain protocols with limited hop counts.
- **New software feature support for EX6200 switches**—The following software features are now supported for EX6200 switches:
  - Bidirectional Forwarding Detection (BFD) protocol for BGP, IS-IS, OSPF, PIM, and RIP
  - BGP for IPv6
  - Captive portal authentication for Layer 3 interfaces
  - CoS—DSCP, IEEE 802.1p, and IP precedence packet rewrites on ingress routed VLAN interfaces (RVIs)
  - Distributed BFD
  - Filter-based S-VLAN tagging
  - Firewall filters on management Ethernet interfaces
  - IPv6 firewall filters
  - IPv6 ping
  - IPv6 static routing
  - IPv6 traceroute
  - IS-IS for IPv6
  - Junos OS image rollback
  - Layer 2 protocol tunneling (L2PT)
  - Multiple VLAN Registration Protocol (MVRP) (IEEE 802.1ak)
  - Multiprotocol Border Gateway Protocol (MBGP)
  - Neighbor Discovery Protocol (NDP)

  - OSPFv3
  - Path MTU discovery
  - Protocol Independent Multicast (PIM) for IPv6 multicast
  - Q-in-Q tunneling
  - Real-time performance monitoring (RPM)—hardware timestamps with routed VLAN interfaces (RVIs)
  - Routing Information Protocol next generation (RIPng)
  - RPM client and server on the same interface
  - Self-signed digital certificates for enabling SSL services
  - sFlow monitoring technology
  - Various class-of-service features for IPv6
  - Virtual Router Redundancy Protocol (VRRP) for IPv6

- **Support for the wildcard range configuration mode command**—EX Series switches now support the CLI **wildcard range** configuration mode command. The **wildcard range** command allows you to specify ranges in **activate**, **deactivate**, **delete**, **protect**, **set**, **show**, and **unprotect** commands. You can use ranges to specify a range of interfaces, logical units, VLANs, and other numbered elements. The **wildcard range** command expands the command you entered into multiple commands, each of which corresponds to one item in the range. For example, the command **wildcard range interfaces deactivate ge-0/0/[1-3]** expands to the commands **deactivate interfaces ge-0/0/1**, **deactivate interfaces ge-0/0/2**, and **deactivate interfaces ge-0/0/3**.

Interfaces

- **EX8200 switch and XRE200 External Routing Engine support for uplink failure detection**—Uplink failure detection allows an EX Series switch to detect link failure on uplink interfaces and to propagate the failure to the downlink interfaces so that servers connected to those downlinks can switch over to secondary interfaces. Switches can have up to 48 groups, each with up to 48 uplinks and 48 downlinks for uplink failure detection.

J-Web Interface

- **EX2200-C, EX3300, and EX6210 switches configuration in the J-Web interface**—You can now configure these switches in the J-Web interface.

MPLS

- **MPLS enhancements on EX8200 switches**—EX8200 Virtual Chassis now support all the MPLS features that are supported on an EX8200 standalone switch. In addition to this, EX8200 standalone switches and Virtual Chassis support the following enhancements:

- IPv6 tunneling and IPv6 Layer 3 VPNs—You can now configure EX8200 switches to tunnel IPv6 over an MPLS-based IPv4 network. This configuration allows you to interconnect a number of smaller IPv6 networks over an IPv4-based network core, enabling you to provide IPv6 service without having to upgrade the switches in your core network.
- MPLS over routed VLAN interfaces (RVIs) or Layer 3 subinterfaces—You can now use an RVI or a Layer 3 subinterface as the MPLS core-facing interface. The RVI functions as a logical router, eliminating the need for having both a switch and a router. Layer 3 subinterfaces allow you to route traffic among multiple VLANs along a single trunk line that connects an EX Series switch to a Layer 2 switch.
- Static LSPs—For static label-switched paths (LSPs), you must manually assign labels on all the switches that are part of the LSP (ingress, transit, and egress). No signaling protocol is needed. Configuring static LSPs is similar to configuring static routes on individual switches. As with static routes, there is no error reporting, liveliness detection, or statistics reporting.
- Ultimate-hop popping using explicit NULL labels—EX8200 switches now support ultimate-hop popping. With ultimate-hop popping enabled, EXP bits are carried through to the egress PE switch. The egress PE switch makes use of EXP bits to classify the packets and send them out from the MPLS network. By default, ultimate-hop popping is disabled.

- **MPLS CoS enhancements on EX8200 switches**—EX8200 switches, both standalone and Virtual Chassis, support MPLS enhancements that allow you to prioritize certain types of traffic during periods of congestion. The enhancements are provided through the following class-of-service (CoS) configurations:
  - EXP classification—EX8200 switches now support EXP classification and rewriting. If you enable the MPLS protocol family on a logical interface, the default MPLS EXP classifier is automatically applied to that logical interface. The default MPLS classifier maps EXP bits to forwarding classes and loss priorities.
  - EXP rewriting—You can now configure rewrite rules on the egress provider-edge (PE) switch to alter the CoS settings of the packets. Rewrite rules set the value of the CoS bits within the packet's header. Each rewrite rule reads the current forwarding class and loss priority information associated with the packet, locates the chosen CoS value from a table, and writes this CoS value into the packet header
  - Label-switched path (LSP) CoS for both Layer 3 VPNs and Layer 2 VPNs—You can now configure a fixed CoS value for each LSP or for all LSPs on the switch. A fixed CoS value ensures that all packets entering the LSP are assigned the same class of service.

- **EX8200 Virtual Chassis MPLS feature support**—EX8200 Virtual Chassis now support all MPLS features that are supported on EX8200 standalone switches. In addition, you can now use a routed VLAN interface (RVI) or a Layer 3 subinterface as the MPLS core-facing interface. The RVI functions as a logical router, eliminating the need for having both a switch and a router. Layer 3 subinterfaces allow you to route traffic among multiple VLANs along a single trunk line that connects an EX Series switch to a Layer 2 switch.

EX8200 standalone switches and EX8200 Virtual Chassis now support IPv6 tunneling and IPv6 Layer 3 VPNs. You can configure EX8200 switches to tunnel IPv6 over an MPLS-based IPv4 network. This configuration allows you to interconnect a number of smaller IPv6 networks over an IPv4-based network core, enabling you to provide IPv6 service without having to upgrade the switches in your core network.

Multicast Protocols

- **MLD snooping support on EX Series switches**—Multicast Listener Discovery (MLD) snooping enables the switch to monitor MLD messages between IPv6 multicast routers and hosts. MLD version 1 (MLDv1) and MLDv2 are supported. When MLD snooping is enabled, the switch can determine which interfaces in a VLAN have interested listeners and forward multicast traffic only to those interfaces instead of flooding all interfaces in the VLAN.

Power over Ethernet (PoE)

- **PoE firmware upgrade**—You can now upgrade the PoE controller firmware from the CLI using the new command **request system firmware upgrade poe**.

Software Installation and Upgrade

- **EX3300 switch support for advanced feature licenses**—EX3300 switches now require an advanced feature license (AFL) to run all the advanced software features on the switch.

Virtual Chassis

- **IPv6 support for firewall filters on EX4500 switches**—On EX4500 Virtual Chassis and EX4500 standalone switches, you can apply match conditions to IPv6 traffic on Layer 3 interfaces and aggregated Ethernet interfaces. The following match conditions are now applicable to IPv6 traffic: **destination-address**, **destination-port**, **icmp-code**, **icmp-type**, **next-header**, **source-address**, **source-port**, **tcp-established**, **tcp-flags**, **tcp-initial**, and **traffic-class**.

  The following actions and action modifiers are applicable to IPv6 traffic: **accept**, **analyzer**, **count**, **discard**, **forwarding-class**, **loss-priority**, and **policer**.

- **Interface-specific IPv6 classifiers and rewrite rules**—EX4500 Virtual Chassis and EX4500 standalone switches now allow you to configure and apply IPv6 classifiers and rewrite rules for each interface.

- **Ingress counters on EX8200 RVIs**—The ability to maintain an ingress count on EX8200 routed VLAN interface (RVI) use has been extended to EX8200 Virtual Chassis.

- **EX8200 Virtual Chassis member switch support enhancement**—You can now configure up to four EX8200 member switches in an EX8200 Virtual Chassis.

Related Documentation

- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for EX Series Switches on page 16
- Limitations in Junos OS Release 12.1 for EX Series Switches on page 16

Changes in Default Behavior and Syntax in Junos OS Release 12.1 for EX Series Switches

There are no changes in default behavior and syntax in Junos OS Release 12.1 for EX Series switches.

Related Documentation

Limitations in Junos OS Release 12.1 for EX Series Switches

This section lists the limitations in Junos OS Release 12.1 for EX Series switches. If the limitation is associated with an item in our bug database, the description is followed by the bug tracking number.

For the most complete and latest information about known Junos OS defects, use the Juniper online Junos Problem Report Search application at http://www.juniper.net/prsearch.

Ethernet Switching and Spanning Trees

- On EX Series switches, only dynamically learned routes can be imported from one routing table group to another. [This is a known software limitation.]

Firewall Filters

- On EX3200 and EX4200 switches, when a very large number of firewall filters are included in the configuration, it might take a long time, possibly as long as a few minutes, for the egress filter rules to be installed. [PR/468806: This is a known software limitation.]
- On EX3300 switches, if you add and delete filters with a large number of terms (on the order of 1000 or more) in the same commit operation, not all the filters are installed.

As a workaround, add filters in one commit operation, and delete filters in a separate commit operation. [PR/581982: This is a known software limitation.]

- On EX8200 switches, if you configure an implicit or explicit discard action as the last term in an IPv6 firewall filter on a loopback (**lo0**) interface, all the control traffic from the loopback interface is dropped. To prevent this, you must configure an explicit **accept** action. [This is a known software limitation.]

Hardware

- On 40-port SFP+ line cards for EX8200 switches, the LEDs on the left of the network ports do not blink to indicate that there is link activity if you set the speed of the network ports to 10/100/1000 Mbps. However, if you set the speed to 10 Gbps, the LEDs blink. [PR/502178: This is a known limitation.]
- The Uplink Modules in EX3200 Switches topic notes the following behavior for the SFP uplink module, which provides four ports for 1-gigabit small form-factor pluggable (SFP) transceivers: "On an EX3200 switch, if you install a transceiver in an SFP uplink module, a corresponding network port from the last four built-in ports is disabled. For example, if you install an SFP transceiver in port 2 on the uplink module (**ge-0/1/2**) on 24-port models, then **ge-0/0/22** is disabled. The disabled port is not listed in the output of **show interface** commands."

  Another note on the same page describes similar behavior of the SFP+ uplink module: "On an EX3200 switch, if you install a transceiver in an SFP+ uplink module when the uplink module is operating in the 1-gigabit mode, a corresponding network port from the last four built-in ports is disabled. For example, if you install an SFP transceiver in port 2 on the uplink module (**ge-0/1/2**), then **ge-0/0/22** is disabled. The disabled port is not listed in the output of **show interfaces** commands."

  However, in both cases what actually occurs is that when you install the SFP uplink module or explicitly configure the mode on an SFP+ uplink module to 1-gigabit operating mode and do not reboot the switch, the last four built-in ports on the switch are disabled. If transceivers are installed in the uplink module, the corresponding built-in network ports are not displayed in the output of **show interfaces** commands. The workaround is to move all four links to the uplink module, or to reboot the switch for correct initialization of the ports. [PR/686467: This is a known limitation.]

High Availability

- You cannot verify that nonstop bridging (NSB) is synchronizing Layer 2 protocol information to the backup Routing Engine even when NSB is properly configured. [PR/701495: This is a known software limitation.]

Infrastructure

- Do not use nonstop software upgrade (NSSU) to upgrade the software on an EX8200 switch from Junos OS Release 10.4 to Release 11.1 or later if you have configured the PIM, IGMP, or MLD protocols on the switch. If you attempt to use NSSU, your switch might be left in a nonfunctional state from which it is difficult to recover. If you have these multicast protocols configured, use the **request system software add** command to upgrade the software on an EX8200 switch from Release 10.4 to Release 11.1 or later. [This is a known software limitation.]
- On EX Series switches, the **show snmp mib walk etherMIB** command does not display any output, even though the **etherMIB** is supported. This occurs because the values are not populated at the module level—they are populated at the table level only. You can issue **show snmp mib walk dot3StatsTable**, **show snmp mib walk dot3PauseTable**, and **show snmp mib walk dot3ControlTable** commands to display the output at the table level. [This is a known software limitation.]
- Momentary loss of an inter-Routing Engine IPC message might trigger an alarm that displays the message “Loss of communication with Backup RE”. However, no functionality is affected. [PR/477943: This is a known software limitation.]
- Routing between virtual-router instances for local direct routes is not supported. [PR/490932: This is known software limitation.]
- On EX4500 switches, the maintenance menu is not disabled even if you include the **lcd maintenance-menu disable** statement in the configuration. [PR/551546: This is a known software limitation.]
- When you enable the **filter-id** attribute on the RADIUS server for a particular client, none of the required 802.1X authentication rules are installed in the IPv6 database. Therefore, IPv6 traffic on the authenticated interface is not filtered; only IPv4 traffic is filtered on that interface. [PR/560381: This is a known software limitation.]
- On EX8200 switches, if OAM link-fault management (LFM) is configured on a member of a VLAN on which Q-in-Q tunneling is also enabled, OAM PDUs cannot be transmitted to the Routing Engine. [PR/583053: This is a known software limitation.]
- If you have configured sFlow technology on an EX8200 switch that you are upgrading from Junos OS Release 10.4 or Release 11.1 using nonstop software upgrade (NSSU), disable sFlow technology before you perform the upgrade. Once the upgrade is complete, you can reenable sFlow technology. If you do not disable sFlow technology before you perform the upgrade with NSSU, sFlow technology will not work properly after the upgrade. Using NSSU to upgrade from Release 11.2 or later to a later release has no impact on sFlow technology functionality. [PR/587138: This is a known software limitation.]

- When you reconfigure the maximum transmission unit (MTU) value of a next hop more than eight times without restarting the switch, the interface uses the maximum value of the eight previously configured values as the next MTU value. [PR/590106: This is a known software limitation.]
- On EX8208 and EX8216 switches that have two Routing Engines, one Routing Engine cannot be running Junos OS Release 10.4 or later while the other one is running Release 10.3 or earlier. Ensure that both Routing Engines in a single switch run either Release 10.4 or later or Release 10.3 or earlier. [PR/604378: This is a known software limitation.]

Interfaces

- EX Series switches do not support IPv6 interface statistics. Therefore, all values in the output of the **show snmp mib walk ipv6IfStatsTable** command always display a count of 0. [PR/480651: This is a known software limitation.]
- On EX8216 switches, a link might go down momentarily when an interface is added to a LAG. [PR/510176: This is a known software limitation.]
- On EX Series switches, if you clear LAG interface statistics while the LAG is down, then bring up the LAG and pass traffic without checking for statistics, and finally bring the LAG interface down and check interface statistics again, the statistics might be inaccurate. As a workaround, use the **show interfaces *interface-name*** command to check LAG interface statistics before bringing down the interface. [PR/542018: This is a known software limitation.]
- Power over Ethernet (PoE) and Power over Ethernet Plus (PoE+) cannot be configured for EX8200 member switches in an EX8200 Virtual Chassis by using the XRE200 External Routing Engine.

  If you have not cabled the Virtual Chassis, configure PoE or PoE+ on each EX8200 member switch before cabling the Virtual Chassis. See Configuring PoE (CLI Procedure).

  To configure PoE and PoE+ on an EX8200 member switch in an operational EX8200 Virtual Chassis:

  1. Power off the EX8200 member switch. See Powering Off an EX8200 Switch.
  2. Uncable the switch from the Virtual Chassis.
  3. Power on the switch. See Powering On an EX8200 Switch
  4. Log in to the switch. See Connecting an EX Series Switch to a Management Console.
  5. Configure PoE. See Configuring PoE (CLI Procedure).
  6. Cable the EX8200 member switch back into the EX8200 Virtual Chassis. See Connecting an EX8200 Switch to an XRE200 External Routing Engine.

J-Web Interface

- The J-Web interface does not support role-based access control—it supports only users in the super-user authorization class. So a user who is not in the super-user class, such as a user with view-only permission, is able to launch the J-Web interface and is allowed

to configure everything, but the configuration fails on the switch, and the switch displays access permission errors. [PR/604595: This is a known software limitation.]

- In a mixed EX4200 and EX4500 Virtual Chassis, the J-Web interface does not list the features supported by member switches in the backup or linecard roles if those features are not also supported by the master. [PR/707671: This is a known software limitation.]

Layer 2 and Layer 3 Protocols

- On EX 3200 and EX4200 switches, MPLS on Layer 3 tagged subinterfaces and routed VLAN interfaces (RVIs) is not supported, even though the CLI allows you to commit a configuration that enables these features. [PR/612434: This is a known software limitation.]

Management and RMON

- On EX Series switches, an SNMP query fails when the SNMP index size of a table is greater than 128 bytes, because the Net SNMP tool does not support SNMP index sizes greater than 128 bytes. [PR/441789: This is a known software limitation.]
- When MVRP is configured on a trunk interface, you cannot configure connectivity fault management (CFM) on that interface. [PR/540218: This is a known software limitation.]
- The connectivity-fault management (CFM) process (cfmd) might create a core file. [PR/597302: This is a known software limitation.]

Virtual Chassis

- A standalone EX4500 switch with its PIC mode set to **virtual-chassis** has less bandwidth available for network ports than an EX4500 switch with its PIC mode set to **intraconnect**. The network ports on a standalone EX4500 switch with a **virtual-chassis** PIC mode setting often do not achieve line-rate performance.

  The PIC mode on an EX4500 switch can be set to **virtual-chassis** in one of the following ways:

  - The switch was ordered with a Virtual Chassis module installed and thus has its PIC mode set to **virtual-chassis** by default.
  - You entered the **request chassis pic-mode virtual-chassis** operational mode command to configure the switch as a member of a Virtual Chassis.

  You can check the PIC mode for your EX4500 switch that has a Virtual Chassis module installed by entering the **show chassis pic-mode** command.

  You should always set the PIC mode on a standalone EX4500 switch to **intraconnect**. Set the PIC mode to **intraconnect** by entering the **request chassis pic-mode intraconnect** operational mode command.

  [This is a known limitation.]

- The automatic software update feature is not supported on EX4500 switches that are members of a Virtual Chassis. [PR/541084: This is a known software limitation.]

- When an EX4500 switch becomes a member of a Virtual Chassis, it is assigned a member ID. If that member ID is a nonzero value, then if that member switch is downgraded to a software image that does not support Virtual Chassis, you cannot change the member ID to 0. A standalone EX4500 switch must have a member ID of 0. The workaround is to convert the EX4500 Virtual Chassis member switch to a standalone EX4500 switch before downgrading the software to an earlier release, as follows:

  1. Disconnect all Virtual Chassis cables from the member to be downgraded.
  2. Convert the member switch to a standalone EX4500 switch by issuing the **request virtual-chassis reactivate** command.
  3. Renumber the member ID of the standalone switch to 0 by issuing the **request virtual-chassis renumber** command.
  4. Downgrade the software to the earlier release.

  [PR/547590: This is a known software limitation.]

- When you add a new member switch to an existing EX4200 Virtual Chassis, EX4500 Virtual Chassis, or mixed EX4200 and EX4500 Virtual Chassis in a ring topology, a member switch that was already part of the Virtual Chassis might become nonoperational for several seconds. The member switch will return to the operational state with no user intervention. Network traffic to the member switch is dropped during the downtime. To avoid this issue, follow this procedure:

  1. Cable one dedicated or user-configured Virtual Chassis port (VCP) on the new member switch to the existing Virtual Chassis.
  2. Power on the new member switch.
  3. Wait for the new switch to become operational in the Virtual Chassis. Monitor the **show virtual-chassis** command output to confirm the new switch is recognized by the Virtual Chassis and is in the Prsnt state.
  4. Cable the other dedicated or user-configured VCP on the new member switch to the Virtual Chassis.

  [PR/591404: This is a known software limitation.]

Related Documentation

- New Features in Junos OS Release 12.1 for EX Series Switches on page 7
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for EX Series Switches on page 16
- Outstanding Issues in Junos OS Release 12.1 for EX Series Switches on page 22
- Resolved Issues in Junos OS Release 12.1 for EX Series Switches on page 23
- Changes to and Errata in Documentation for Junos OS Release 12.1 for EX Series Switches on page 31
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for EX Series Switches on page 32

Outstanding Issues in Junos OS Release 12.1 for EX Series Switches

The following are outstanding issues in Junos OS Release 12.1B2 for EX Series switches. The identifier following the description is the tracking number in our bug database.

For the most complete and latest information about known Junos OS defects, use the Juniper online Junos Problem Report Search application at http://www.juniper.net/prsearch.

Access Control and Port Security

- If incoming LLDP packets contain multiple Management Address TLVs, EX Series switches discard them. [PR/718781]
- When an EX Series switch is reauthenticating users using 802.1X (dot1x), if the switch loses reachability to RADIUS server, the dynamic filters that were installed when the same user was previously authenticated are not cleared, resulting in traffic issues. [PR/721124]

Ethernet Switching and Spanning Trees

- If the bridge priority of a VSTP root bridge is changed such that this bridge will become a nonroot bridge, the transition might take more than 2 minutes, and you might see a loop during the transition. [PR/661691]

Infrastructure

- On EX8208 switches, when a line card that has no interface configurations and is not connected to any device is taken offline using the **request chassis fpc-slot *slot-number* offline** command, the Bidirectional Forwarding Detection process (**bfd**) starts and stops repeatedly. The same **bfd** process behavior occurs on a line card that is connected to a Layer 3 domain when another line card that is on the same switch and is connected to a Layer 2 domain is taken offline. [PR/548225]

Related Documentation

- New Features in Junos OS Release 12.1 for EX Series Switches on page 7
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for EX Series Switches on page 16
- Limitations in Junos OS Release 12.1 for EX Series Switches on page 16
- Resolved Issues in Junos OS Release 12.1 for EX Series Switches on page 23
- Changes to and Errata in Documentation for Junos OS Release 12.1 for EX Series Switches on page 31
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for EX Series Switches on page 32

Resolved Issues in Junos OS Release 12.1 for EX Series Switches

The following are the issues that have been resolved in Junos OS Release 12.1 for EX Series switches. The identifier following the descriptions is the tracking number in our bug database.

For the most complete and latest information about known Junos OS defects, use the Juniper online Junos Problem Report Search application at http://www.juniper.net/prsearch.

- Issues Resolved in Release 12.1B2 on page 23

Issues Resolved in Release 12.1B2

The following issues have been resolved since Junos OS Release 11.4. The identifier following the description is the tracking number in our bug database.

Access Control and Port Security

- When you enable LLDP-MED autonegotiation on an EX Series switch, the **autonegotiation** bit in the LLDP-MED packet is set to **not-supported**, which might cause IP phones to discard LLDP-MED packets received from the switch. [PR/708752: This issue has been resolved.]
- When DHCP snooping information is not learned, ARP request packets might add the following message to the system log (syslog) file: "ESWD_DAI_FAILED: 3 (null) received, interface". [PR/719751: THis issue has been resolved.]
- When an EX Series switch is reauthenticating users using 802.1X (dot1x), if the switch loses reachability to the RADIUS server, the dynamic filters that were installed when the same user was previously authenticated are not cleared, resulting in traffic issues. [PR/72114: This issue has been resolved.]
- On EX Series switches running Junos OS Release 11.*x*, LLDP packets might not be generated out of interfaces that are part of a LAG, causing LLDP neighbors not to form. As a workaround, follow these steps:

  1. Delete the LLDP-MED configuration.
  2. Commit the configuration.
  3. Delete the LLDP configuration.
  4. Commit the configuration.
  5. Configure LLDP again.
  6. Commit the configuration.
  7. Optionally, configure LLDP-MED again.
  8. Commit the configuration.

[PR/727627: This issue has been resolved.]

- On EX2200, EX3300, and EX6200 switches, and on EX8200 Virtual Chassis, NetBIOS snooping does not work. [PR/706588: This issue has been resolved.]

Device Security

- If storm control is enabled, the Link Aggregation Control Protocol (LACP) might stop and then restart when Layer 2 packets are sent at a high rate of speed. As a workaround, disable storm control for all multicast traffic on aggregated Ethernet interfaces by issuing the **set ethernet-switching-options storm-control interface** *interface-name* **no-multicast** command. [PR/575560: This issue has been resolved.]
- You cannot configure the level for storm control. [PR/734307: This issue has been resolved.]

Ethernet Switching and Spanning Trees

- On EX Series switches, when you remove a VLAN that has a VLAN ID and then add the same VLAN ID but with a different VLAN name, the Ethernet switching process (eswd) might create a core file. [PR/668210: This issue has been resolved.]
- On an EX4200 switch, when you disable a Q-in-Q interface on which you have configured a large number (more than 500) of VLAN swap rules, control traffic might be affected for about 10 minutes. During this time, the forwarding process (pfem) can consume up to 98 percent of the CPU. The system resumes its normal state after the forwarding process completes its processing. [PR/678792: This issue has been resolved.]
- When you enable VLANs and Q-in-Q tunneling on a switch, the switch drops packets and no MAC address learning occurs. [PR/685481: This issue has been resolved.]
- On a link aggregation group (LAG) interface on which Q-in-Q tunneling is enabled on a VLAN, packets ingressing the LAG might be dropped. As a workaround, explicitly configure the VLAN to allow the desired traffic. [PR/699940: This issue has been resolved.]
- When ingress and egress ports are on different member switches and a packet is routed from the default routing instance to another forwarding instance type, the VLAN ID might be modified in such a way that the traffic is redirected to the default routing instance for subsequent routing. [PR/721436: This issue has been resolved.]
- When you configure the same VLAN ID on both interface VLAN tagging and global tagging, ARP entries cannot be resolved on the VLAN interface. [PR/722815: This issue has been resolved.]
- Routed VLAN interfaces (RVIs) might use the system MAC address instead of using the MAC address one greater than the system MAC address (that is, system MAC address + 1), and Layer 3 ports might use their hardware MAC address instead of using the system MAC address. [PR/723643: This issue has been resolved.]
- When you change the spanning-tree protocol from RSTP or VSTP to MSTP, the Ethernet switching process (eswd) might create a core file. [PR/725436: This issue has been resolved.]

Firewall Filters

- On EX8200 switches, if you configure a **discard** term on an egress firewall filter, the filter might not block ARP broadcast packets. [PR/672621: This issue has been resolved.]
- For two-rate, three-color policers, the egress traffic might not flow at the configured peak information rate (PIR). [PR/687564: This issue has been resolved.]
- When you configure VLAN ID translation when using Q-in-Q tunneling, if you apply a tricolor marking (TCM) policer to the Q-in-Q interface, a Packet Forwarding Engine (pfem) core file might be created. [PR/688438: This issue has been resolved.]
- In an EX8200 Virtual Chassis that is configured with an implicit **deny** statement and that has VCCP traffic flowing through 10-Gigabit Ethernet ports configured as Virtual Chassis ports (VCPs), if you apply a loopback filter, then the FPCs (line cards) of member 0 and member 1 can lose contact with the master Routing Engine. [PR/688983: This issue has been resolved.]
- Firewall rules might not be installed in the ternary content addressable memory (TCAM), and you might see the following error message: “dfw_grph_merge_dfw_bind: rules for filter ACL will not be installed.” [PR/689288: This issue has been resolved.]
- When you configure a **syslog** action in a firewall filter on the me0 interface, an EX2200 switch might crash when you commit the configuration. [PR/694602: This issue has been resolved.]
- If you configure a firewall filter on a loopback interface whose last term is **deny all**, static routes filtered with **reject** action reach the CPU, and multicast trap and RPF fail packets are implicitly allowed to reach the CPU. [PR/740641: This issue has been resolved.]
- If you configure both a regular and a firewall filter-based analyzer, the traffic from the regular analyzer might egress from the output port you configured for the firewall filter-based analyzer. [PR/724795: This issue has been resolved.]

Hardware

- On XRE200 External Routing Engines, the output of the **show chassis hardware** command might contain duplicate Routing Engine inventory information for members 8 and 9. [PR/663272: This issue has been resolved.]
- On EX6210 switches, traffic might not exit from the 10-Gigabit Ethernet interfaces on the Routing Engines. [PR/669330: This issue has been resolved.]
- For Opnext SFPs with Juniper part number 740-021308 and types SFP+ 10GE-SR, SFP+ 10GE-LR, or SFP+ 10GE-ER, when the low-power threshold is crossed, the power-low warning alarm is not set on extra-scale and Power over Ethernet (PoE) line cards. [PR/683732: This issue has been resolved.]
- On EX4500 switches, the LCD panel might not list the ADM (administrative status) or DPX (duplex) options in the Idle menu. Also, when you press Enter to cycle through the status LED modes, you might not be able to cycle through them. [PR/692341: This issue has been resolved.]

- On EX4200 switches, the EZsetup menu is not displayed on the LCD panel after you set the switch to the factory-default configuration. [PR/712322: This issue has been resolved.]
- On EX8200 switches, when the Switch Fabric and Routing Engine (SRE) module is in the spare state and you configure it to go offline and then come back online again, the module's ST LED does not turn back on. [PR/724455: This issue has been resolved.]

High Availability

- When you perform a nonstop software upgrade (NSSU) operation on an EX8200 Virtual Chassis, if you do not include the **reboot** option when you request the NSSU to have the switch perform an automatic reboot, the upgrade might hang indefinitely after the Junos OS images have been pushed to the master Routing Engine. [PR/692422: This issue has been resolved.]
- After a graceful Routing Engine switchover (GRES) operation, clone routes might move into the reject state. [PR/724729: This issue has been resolved.]

Infrastructure

- The system log (syslog) files might contain the message "Juniper syscall not available". These messages are harmless, and you can ignore them. [PR/519153: This issue has been resolved.]
- The system log (syslog) file might contain the following message: "/var: filesystem full". [PR/600145: This issue has been resolved.]
- On EX Series switches, the **request system snapshot** command mistakenly includes the **as-primary** option. [PR/603204: This issue has been resolved.]
- If you remove or change interfaces soon after completing a nonstop software upgrade (NSSU) operation, the multicast snooping process (mcsnoopd) might create a core file. [PR/662065: This issue has been resolved.]
- Layer 3 next-hop entries might remain queued in the kernel of the backup Routing Engine and might never be installed in the forwarding table. [PR/670799: This issue has been resolved.]
- On EX8200 switches, when you run a failover operation on the Routing Engines, a vmcore file might be created. [PR/678465: This issue has been resolved.]
- The management process (mgd) might create a core file when reading very long lines. For example, this can happen when you are displaying a Junos OS configuration file that contains very long lines. When mgd crashes, the command that you were executing does not complete and the following errors appear in the **messages** file: %KERN-3-BAD_PAGE_FAULT: pid 57182 (mgd), uid 0: pc 0x8870ab92 got a write fault at 0x8488000, x86 fault flags = 0x6 and %KERN-6: pid 57182 (mgd), uid 0: exited on signal 11 (core dumped). [PR/679992: This issue has been resolved.]
- On EX4500 switches, ICMPv6 packets might transit the Routing Engine even though IPv6 is not configured. [PR/682953: This issue has been resolved.]

- On an XRE200 External Routing Engine, the rescue configuration might not get synchronized with the backup external Routing Engine. [PR/687797: This issue has been resolved.]
- During a graceful Routing Engine switchover (GRES) operation between an EX4200 and an EX4500 switch, a Packet Forwarding Engine (pfem) core file might be created. [PR/688618: This issue has been resolved.]
- You might not be able to commit a configuration on an XRE200 External Routing Engine, and the switch might display the error "could not save to juniper.save+". [PR/689764: This issue has been resolved.]
- An EX4200 switch might stop forwarding traffic, and a Packet Forwarding Engine (pfem) core file might be created. [PR/691504: This issue has been resolved.]
- When the same MAC address is learned on both the primary and community VLANS, an Ethernet switching process (eswd) core file might be created. [PR/693942: This issue has been resolved.]
- On EX4200 switches, if you connect and then disconnect the cable to the port on which the Bidirectional Forwarding Detection (BFD) protocol is running, a software forwarding process (sfid) core file might be created. [PR/694150: This issue has been resolved.]
- EX Series switches might not learn the MAC addresses of directly connected devices. [PR/695280: This issue has been resolved.]
- On EX3200, EX4200, EX4500, EX6200, EX8208, and EX8216 switches, the **root** user is allowed to telnet into the me0 interface, which does not comply with the default Junos OS behavior, as documented in Telnet to JUNOS router fails with root login and Connecting and Configuring an EX Series Switch (CLI Procedure). [PR/695346: This issue has been resolved.]
- On EX Series switches, when you are configuring DHCP option 82, the **use-interface-description** statement, which uses the interface description rather than the interface name (the default) in the circuit ID or remote ID value in the DHCP option 82 information, does not work. [PR/695712: This issue has been resolved.]
- When you commit a configuration, the following message might be placed in the system log (syslog) file: "kernel: PFE not configured, Juniper syscall not available". This message is harmless and you can ignore it. [PR/696471: This issue has been resolved.]
- When the switch is performing 802.1X (dot1x) authentication using MAC RADIUS, you might see the following message in the system log (syslog) file: "kmem type temp using 57344K, exceeding limit 57344K". [PR/697815: This issue has been resolved.]
- When you add a new VLAN on a switch on which you have also configured loopback and other IPv4 firewall filters, a pfem core file might be created that contains the message "No space available in tcam". [PR/701779: This issue has been resolved.]
- On EX8200 switches that have IPv6 and IPv4 configured on routing instances, when many interfaces go down and come back up repeatedly, the next-hop programming for some routes might fail, which can cause disruptions in traffic. [PR/701985: This issue has been resolved.]
- When you run the **commit check** command, the word "operation" in the command output might be misspelled. [PR/704910: This issue has been resolved.]

- If the egress interface is a trunk interface, frames that exceed 9216 bytes might not be fragmented. [PR/705905: This issue has been resolved.]
- If you power off and then restart an EX Series switch, the chassis process (chassisd) might not restart. This problem might also occur in switches that have redundant power supplies. [PR/708872: This issue has been resolved.]
- If you perform a nonstop system software upgrade (NSSU) operation that includes the **reboot** option, some traffic loss might occur. [PR/717662: This issue has been resolved.]
- After a MAC address moves, the ARP index might not point to the correct MAC address. As a workaround, run the **clear ethernet-switching table** command. [PR/718698: This issue has been resolved.]
- A destination with two equal-cost next hops might not be installed in the Packet Forwarding Engine when a virtual management Ethernet (VME) interface is configured and a default route with a reachable next hop is present. As a workaround, remove and then re-add one of the two equal-cost next hops. [PR/719745: This issue has been resolved.]
- On EX4200 switches, after you issue the **request system zeroize media** command, you might not be able to establish a connection with the switch using SSH and you might not be able to issue the **commit** command on the switch. [PR/723918: This issue has been resolved.]
- New hosts and routes might not be installed in the Packet Forwarding Engine, and the system log (syslog) files might contain the following message: "Failed to jtm_alloc for mrvl_rt_nh_uc_install". [PR/726043: This issue has been resolved.]
- On EX8200 swithces, after you issue the **request system zeroize media** command, the FPCs might not come online. [PR/728082: This issue has been resolved.]
- On the Login page and in the Help mapping file in the J-Web interface, the copyright date is set to 2011. [PR/731790: This issue has been resolved.]
- The Ethernet switching process (eswd) might create a core file. [PR/732263: This issue has been resolved.]

Interfaces

- The displayed bandwidth on unit 0 of an interface might be incorrect. As a workaround, configure an interface speed on unit 0. [PR/471628: This issue has been resolved.]
- When you configure the member interfaces of an aggregated Ethernet interface before you configure the aggregated Ethernet (**ae***x*) device using **set** commands from the CLI, the aggregated Ethernet interface does not receive MAC updates. As a workaround, configure the aggregated Ethernet interface first, then configure the member interfaces. [PR/680913: This issue has been resolved.]
- When you configure an aggregated Ethernet interface with LACP in fast mode, the logical interface of the aggregated interface might flap after a graceful Routing Engine switchover (GRES) operation. [PR/686585: This issue has been resolved.]
- When 10-Gigabit Ethernet interfaces flap frequently, a routing protocol process (rpd) core file might be created. [PR/692126: This issue has been resolved.]

- EX Series switches do not show the control packet counters in both directions on the logical units of aggregated Ethernet (**aex**) interfaces. [PR/693202: This issue has been resolved.]
- Interfaces might not come up, and the system log (syslog) file might contain the message "DCD_CONFIG_WRITE_FAILED:configuration write failed for an RT ADD: Cannot allocate memory". [PR/697300: This issue has been resolved.]
- If you set an interface speed in the **[edit interfaces interface-range]** hierarchy, this speed might not be applied to the individual interface. If you set different interfaces speeds directly on the interface and in the **[edit interfaces interface-range]** hierarchy, both settings are applied on the interface. [PR/697478: This issue has been resolved.]
- On EX4500 switches with an interface in loopback mode, BPDUs might be processed instead of being dropped as expected, generating topology change notifications (TCNs). As a workaround, disable the interface that is in loopback mode. [PR/698077: This issue has been resolved.]
- When you configure the **no-preempt** and **interface-tracking** options on a switch that is a VRRP master router, if the VRRP mastership is taken over by a switch that is a VRRP backup router and the tracking interface on the original master router goes down, then if the tracking interface on the original master router comes back up and the master's original priority is restored, the new master's mastership might transition to the original master router. [PR/699243: This issue has been resolved.]

J-Web Interface

- In the J-Web interface, the dashboard does not display the uplink ports or uplink module ports unless transceivers are plugged into the ports. [PR/477549: This issue has been resolved.]
- In the J-Web interface, if you navigate to any of the top panel tabs (such as **Configure**, **Monitor**, **Maintain**, and **Troubleshoot**) and then click **Help > Help Contents**, you might be directed to an undefined page. To display the correct help for a feature, first click the menu item corresponding to the feature to load the page, and then click **Help > Help Contents**. [PR/684958: This issue has been resolved.]
- In the J-Web interface, if you discard any available MIB profile, file, or predefined object from **accounting-options** on the Point and Click CLI Configuration page (**Configure > CLI Tools > Point and Click CLI**), the J-Web session times out. As a workaround, perform the same operation from the CLI. [PR/689261: This issue has been resolved.]
- On EX4500 switches, you cannot configure BGP on the BGP Configuration page (**Configure > Routing > BGP**). [PR/699308: This issue has been resolved.]
- In the J-Web interface, the dashboard might not be displayed. [PR/700274: This issue has been resolved.]
- In the J-Web interface on an EX4500 Virtual Chassis, if you configure four or more Virtual Chassis members on the Support Information page (**Maintain > Customer Support > Support Information**), you might see the error "Configuration of switch is too large". [PR/704992: This issue has been resolved.]
- On SRX210 Services Gateways and EX Series switches, if you use the CLI to delete a DHCP pool, the J-Web interface Monitor page (**Monitor > Services > DHCP > Pools**)

might not display the correct value in the Excluded address field. Instead, it might display the text "[objec object]" in the table. [PR/723555: This issue has been resolved.]

Layer 2 and Layer 3 Protocols

- On EX Series switches and M Series routers, IPv6 neighbor unreachability detection does not work. As a workaround, use the **clear ipv6 neighbor** command to initiate neighbor detection. [PR/613230: This issue has been resolved.]
- When a BGP interface is flapping quickly, BGP might unnecessarily withdraw prefixes even when a good route to that prefix still exists. [PR/677191: This issue has been resolved.]
- On EX3200 and EX4200 switches, no counters are available for MPLS statistics for circuit cross-connects (CCCs) because of a hardware limitation. As a result, no counters are incremented in MPLS statistics files for LSPs that are used for CCCs. [PR/724371: This issue has been resolved.]

Management and RMON

- When you use the **snmpwalk** application to get information about switch interfaces, it returns information about incorrect interfaces. [PR/664940: This issue has been resolved.]
- EX Series switches might not send **jnxMIMst** traps. [PR/707141: This issue has been resolved.]

Multicast Protocols

- You might not be able to delete stale multicast routes even though no corresponding (S, G) traffic exists. [PR/674419: This issue has been resolved.]
- Approximately every 300 seconds, a multicast route entry is deleted and added back again, resulting in a traffic loss of about 1-3 seconds. [PR/698129: This issue has been resolved.]

Software Upgrade and Installation

- When you upgrade Junos OS from a release prior to Release 10.4R3, in which resilient dual-root partitioning was introduced, to a later release that supports resilient dual-root partitioning, the time required for the upgrade to complete is longer than upgrading either between two releases that are earlier than Release 10.4R3 or between two releases that are Release 10.4R3 or later. [PR/683337: This issue has been resolved.]
- On EX3300 switches, when you load the factory default settings, the last two ports of the uplink ports are configured as Virtual Chassis ports (VCPs). If you convert these ports to network ports, they might not pass traffic. As a workaround, reboot the switch after converting the ports. [PR/685300: This issue has been resolved.]
- After you upgrade Junos OS, a software forwarding process (sfid) core file might be created. [PR/691958: This issue has been resolved.]

Virtual Chassis

- On EX8200 Virtual Chassis, the link status of an aggregated Ethernet (**ae*x***) interface managed by LACP goes down and comes back up when a graceful Routing Engine switchover (GRES) operation is performed between the XRE200 External Routing Engines. This switchover might have been initiated from the Junos OS CLI or because of a failure of the master Routing Engine. [PR/599772: This issue has been resolved.]
- On EX8200 Virtual Chassis, if the topology is formed such that ingress multicast traffic is routed first to the rendezvous point (RP) and then returns to the Virtual Chassis for egress via Layer 2 multicast, the multicast traffic is forwarded only to receivers connected to the Virtual Chassis member in which the returned multicast traffic is received. Multicast traffic is not forwarded to other receivers in other Virtual Chassis members. [PR/666355: This issue has been resolved.]
- When EX4200 and EX4500 switches are interconnected into the same Virtual Chassis to form a mixed EX4200 and EX4500 Virtual Chassis, the switches might fail to form a Virtual Chassis. [PR/681072: This issue has been resolved.]
- On EX8200 Virtual Chassis, LACP and all Layer 3 protocols flap constantly when an LCC backup Routing Engine is rebooted. When the issue is happening, the connection between the master XRE200 External Routing Engine and the LCC FPC might be lost. [PR/700295: This issue has been resolved.]
- In mixed EX4200 and EX4500 Virtual Chassis, when you configure class of service, some traffic might be dropped because it is mapped to the incorrect queue. [PR/711071: This issue has been resolved.]

Related Documentation

- New Features in Junos OS Release 12.1 for EX Series Switches on page 7
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for EX Series Switches on page 16
- Limitations in Junos OS Release 12.1 for EX Series Switches on page 16
- Outstanding Issues in Junos OS Release 12.1 for EX Series Switches on page 22
- Changes to and Errata in Documentation for Junos OS Release 12.1 for EX Series Switches on page 31
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for EX Series Switches on page 32

Changes to and Errata in Documentation for Junos OS Release 12.1 for EX Series Switches

Changes to Junos OS for EX Series Switches Documentation

No changes have been made to the documentation for Junos OS Release 12.1 for EX Series switches since it was published.

Errata

There are no outstanding issues with the published documentation for Junos OS Release 12.1 for EX Series switches.

Related Documentation

- New Features in Junos OS Release 12.1 for EX Series Switches on page 7
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for EX Series Switches on page 16
- Limitations in Junos OS Release 12.1 for EX Series Switches on page 16
- Outstanding Issues in Junos OS Release 12.1 for EX Series Switches on page 22
- Resolved Issues in Junos OS Release 12.1 for EX Series Switches on page 23
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for EX Series Switches on page 32

Upgrade and Downgrade Instructions for Junos OS Release 12.1 for EX Series Switches

This section discusses the following topics:

- Upgrade and Downgrade Support Policy for Junos OS Releases on page 32
- Upgrading from Junos OS Release 10.4R3 or Later on page 33
- Upgrading from Junos OS Release 10.4R2 or Earlier on page 34
- Upgrading EX Series Switches Using NSSU on page 34

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 10.0, 10.4, and 11.4 are EEOL releases. You can upgrade from Junos OS Release 10.0 to Release 10.4 or even from Junos OS Release 10.0 to Release 11.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind. For example, you cannot directly upgrade from Junos OS Release 10.3 (a non-EEOL release) to Junos OS Release 11.4 or directly downgrade from Junos OS Release 11.4 to Junos OS Release 10.3.

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 http://www.juniper.net/support/eol/junos.html .

Upgrading from Junos OS Release 10.4R3 or Later

You can use this procedure to upgrade Junos OS on a standalone EX Series switch with a single Routing Engine. You can also use it to upgrade all members of a Virtual Chassis or a single member of a Virtual Chassis. To upgrade software on a standalone EX6200 switch or EX8200 switch with dual Routing Engines, see Installing Software on an EX Series Switch with Redundant Routing Engines (CLI Procedure).

On EX8200 switches and EX8200 Virtual Chassis, you can also use nonstop software upgrade (NSSU) to perform the upgrade. For more information, see "Upgrading EX Series Switches Using NSSU" on page 34.

To install software upgrades on a switch with a single Routing Engine or on a Virtual Chassis:

1. Download the software package as described in Downloading Software Packages from Juniper Networks.
2. (Optional) Back up the current software configuration to a second storage option. See the *Junos OS Installation and Upgrade Guide* for instructions.
3. (Optional) Copy the software package to the switch. We recommend that you use FTP to copy the file to the **/var/tmp** directory.

   This step is optional because Junos OS can also be upgraded when the software image is stored at a remote location.
4. Install the new package on the switch:

   ```
   user@switch> request system software add package
   ```

   Replace ***package*** with one of the following paths:

   - For a software package in a local directory on the switch—**/var/tmp/*package*.tgz**.
   - For a software package on a remote server:
     - **ftp://*hostname*/*pathname*/*package*.tgz**
     - **http://*hostname*/*pathname*/*package*.tgz**

   where ***package***.tgz is, for example, **jinstall-ex-4200-12.1R1.8-domestic-signed.tgz**.

   To install software packages on all the switches in a mixed EX4200 and EX4500 Virtual Chassis, use the **set** option to specify both the EX4200 package and the EX4500 package:

   ```
   user@switch> request system software add set [package package]
   ```

   Include the optional **member** option to install the software package on only one member of a Virtual Chassis:

   ```
   user@switch> request system software add package member member-id
   ```

   Other members of the Virtual Chassis are not affected. To install the software on all members of the Virtual Chassis, do not include the **member** option.

NOTE: To abort the installation, do not reboot your device; instead, finish the installation and then issue the **request system software delete** *package*.tgz command, where *package*.tgz is, for example, **jinstall-ex-8200-12.1R1.8-domestic-signed.tgz**. This is your last chance to stop the installation.

5. Reboot to start the new software (to reboot a single member, use the **member** option):

```
user@switch> request system reboot
```

6. After the reboot has completed, log in and verify that the new version of the software is properly installed:

```
user@switch> show version
```

Upgrading from Junos OS Release 10.4R2 or Earlier

To upgrade to Junos OS Release 12.1 from Release 10.4R2 or earlier, first upgrade to Release 11.4 by following the instructions in the 11.4 release notes. See *Upgrading from Junos OS Release 10.4R2 or Earlier* in the Junos OS 11.4 Release Notes (http://www.juniper.net/techpubs/en_US/junos11.4/information-products/topic-collections/release-notes/11.4/junos-release-notes-11.4.pdf).

Upgrading EX Series Switches Using NSSU

You can use nonstop software upgrade (NSSU) to upgrade Junos OS releases on EX8200 standalone switches and EX8200 Virtual Chassis. For instructions on how to perform an upgrade using NSSU, see Upgrading Software on an EX8200 Standalone Switch Using Nonstop Software Upgrade (CLI Procedure) or Upgrading Software on an EX8200 Virtual Chassis Using Nonstop Software Upgrade (CLI Procedure).

Table 1 on page 35 details NSSU support per Junos OS release and provides pointers to any known issues for particular upgrade scenarios.

Table 1: Using NSSU to Upgrade Junos OS on EX8200 Switches and EX8200 Virtual Chassis

Switch Platform	Upgrade from Release *x.x*	Upgrade to Release 10.4R4 or Later	Upgrade to Release 11.1R4	Upgrade to Release 11.2R1	Upgrade to Release 11.2R2	Upgrade to Release 11.3, 11.4, or 12.1
EX8200 standalone switch	10.4R1 or 10.4R2	Not supported	Not supported	Not supported	Not supported	Not supported
	10.4R3 or later	Supported	Supported	Supported	Supported	Supported
	11.1R1 or later	–	Supported	Supported	Supported	Supported
	11.2R1	–	–	Supported	Supported	Supported
	11.2R2	–	–	–	Supported	Supported
	11.3R1 or later	–	–	–	–	Supported
	11.4R1 or later	–	–	–	–	Supported
EX8200 Virtual Chassis	10.4R1 or later	Not supported	Not supported	Not supported	Not supported	Not supported
	11.1R1, 11.1R2, or 11.1R3	–	Not recommended	Not recommended	Not recommended	Not recommended
	11.1R4	–	Not recommended	Supported	Supported	Supported
	11.1R5	–	–	Supported	Supported	Supported
	11.2R1	–	–	Supported	Supported	Supported
	11.2R2	–	–	–	Supported	Supported
	11.3R1 or later	–	–	–	–	Supported
	11.4R1 or later	–	–	–	–	Supported

On an EX8200 Virtual Chassis, an NSSU operation can be performed only if you have configured the XRE200 External Routing Engine member ID to be 8 or 9.

NOTE: Do not use nonstop software upgrade (NSSU) to upgrade the software on an EX8200 switch from Junos OS Release 10.4 if you have configured the IGMP, MLD, or PIM protocols on the switch. If you attempt to use NSSU, your switch might be left in a nonfunctional state from which it is difficult to recover. If you have these multicast protocols configured, upgrade the software on the EX8200 switch from Release 10.4 by following the instructions in Installing Software on an EX8200 Switch with Redundant Routing Engines (CLI Procedure). This issue does not apply to upgrades from Release 11.1 or later.

NOTE: If you are using NSSU to upgrade the software on an EX8200 switch from Junos OS Release 10.4 or Release 11.1 and sFlow technology is enabled, disable sFlow technology before you perform the upgrade using NSSU. After the upgrade is complete, you can reenable sFlow technology. If you do not disable sFlow technology before you perform the upgrade with NSSU, sFlow technology will not work properly. This issue does not affect upgrades from Release 11.2 or later.

NOTE: If you are using NSSU to upgrade the software on an EX8200 switch from Junos OS Release 11.1 and NetBIOS snooping is enabled, disable NetBIOS snooping before you perform the upgrade using NSSU. After the upgrade is complete, you can reenable NetBIOS snooping. If you do not disable NetBIOS snooping before you perform the upgrade with NSSU, NetBIOS snooping will not work properly. This issue does not affect upgrades from Release 11.2 or later.

Related Documentation

- New Features in Junos OS Release 12.1 for EX Series Switches on page 7
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for EX Series Switches on page 16
- Limitations in Junos OS Release 12.1 for EX Series Switches on page 16
- Outstanding Issues in Junos OS Release 12.1 for EX Series Switches on page 22
- Resolved Issues in Junos OS Release 12.1 for EX Series Switches on page 23
- Changes to and Errata in Documentation for Junos OS Release 12.1 for EX Series Switches on page 31

Junos OS Release Notes for Branch SRX Series Services Gateways and J Series Services Routers

Powered by Junos OS, Juniper Networks SRX Series Services Gateways provide robust networking and security services. SRX Series Services Gateways range from lower-end branch devices designed to secure small distributed enterprise locations to high-end devices designed to secure enterprise infrastructure, data centers, and server farms. The branch SRX Series Services Gateways include the SRX100, SRX110, SRX210, SRX220, SRX240, SRX550, and SRX650 devices. The high-end SRX Series Services Gateways include the SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices.

Juniper Networks J Series Services Routers running Junos OS provide stable, reliable, and efficient IP routing, WAN and LAN connectivity, and management services for small to medium-sized enterprise networks. These routers also provide network security features, including a stateful firewall with access control policies and screens to protect against attacks and intrusions, and IPsec VPNs. The J Series Services Routers include the J2320, J2350, J4350, and J6350 devices.

New Features in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers

The following features have been added to Junos OS Release 12.1. Following the description is the title of the manual or manuals to consult for further information.

NOTE: For the latest updates about support and issues on Junos Pulse, see the Junos Pulse Release Notes.

Software Features

AppSecure

- **User role integration into AppTrack logs**—This feature is supported on all branch SRX Series devices.

  User identity details such as user name and user role have been added to the AppTrack session create, session close, and volume update logs. These fields will contain the user name and role associated with the policy match. The logging of username and roles are enabled only for security policies that provide UAC enforcement. For security policies without UAC enforcement, the username and roles is displayed as N/A. The user name is displayed as unauthenticated-user and user role is displayed as N/A, if the device cannot retrieve information for that session because there is no authentication table entry for that session or because logging of this information is disabled. The user-role field in the log will contain the list of all the roles performed by the user if match criteria is specific, authenticated-user, or any and the user name field in the log contains the correct username. The user-role field in the log will contain N/A if the match criteria and the username field in the log contains un-authenticated user or unknown user.

  [*Junos OS Security Configuration Guide*]

Chassis Cluster

- Chassis cluster is now supported on SRX550 devices in addition to existing support on SRX100, SRX210, SRX220, SRX240, and SRX650 devices.

  To form a chassis cluster, two of the same model of supported SRX550 devices combine to act as a single system that enforces the same overall security. The chassis cluster design requires two ports to manage the cluster. The cluster uses one port for chassis control and one port for data plane traffic. A maximum of 9 Flexible PIC Concentrator (FPC) slots is supported on SRX550 devices. SRX550 devices use separate high-availability (HA) control and fabric ports.

  NOTE: SRX550 devices also support fiber-optic ports.

  On SRX550 devices, ge-0/0/1 port on node 0 and ge-9/0/1 port on node 1 are used as HA control ports.

  SRX550 devices support the following features in chassis cluster mode:

  - All interfaces types supported in noncluster mode
  - Data plane
  - Firewall filters
  - IPsec
  - QoS
  - Redundancy groups

- Redundant Ethernet Interface
- SNMP
- WAN interfaces

Interfaces that require pseudointerface support are not supported in chassis cluster mode on SRX550 devices.

[*Junos OS Security Configuration Guide*]

Denial of Service (DoS)

- **Whitelists**—This feature is supported on all branch SRX Series devices.

  You can configure a whitelist of IP addresses that are to be exempt from the SYN cookie and SYN proxy mechanisms that occur during the SYN flood screen protection process. To do so, use the new **white-list** statement at the [**edit security screen ids-option screen-name tcp syn-flood**] hierarchy level.

  Both IP version 4 (IPv4) and IP version 6 (IPv6) whitelists are supported. Addresses in a whitelist must be all IPv4 or all IPv6. Each whitelist can have up to 32 IP address prefixes.

  [*Junos OS CLI Reference*, *Junos OS Security Configuration Guide*]

Intrusion Detection and Prevention (IDP) and AppSecure

- **Synchronizing application identification package in a chassis cluster**—This feature is supported on SRX100, SRX210, SRX220, SRX240, SRX550, SRX650, and J Series devices.

  The existing application identification package download feature is modified to download the security package on the primary node and synchronize it on the secondary node.

  When you download the application signature package on a device operating in chassis cluster mode, this feature enables you to download and install the package to the primary node, after which the primary and secondary nodes are automatically synchronized. This synchronization helps maintain the same version of the security package on both the primary node and the secondary node.

  You can use the command **request services application-identification download** to download the application identification package to the primary node and use the command **request services application-identification download status** to verify the download status of the application package and the status of the synchronization to the secondary node.

  [*Junos OS Security Configuration Guide*]

- **Synchronizing IDP security package in a chassis cluster**— This feature is supported on SRX100, SRX210, SRX220, SRX240, SRX550, SRX650, and J Series devices.

  The existing IDP security package download feature has been modified to download the security package on the primary node and synchronize it on secondary node.

When you download the IDP security package on a device operating in chassis cluster mode, this feature enables you to download and install the IDP signature database to the primary node, after which the primary and secondary nodes are automatically synchronized. This synchronization helps maintain the same version of the security package on both the primary node and the secondary node.

You can use the **request security idp security-package download** command to download the IDP signature database to the primary node.

When you check the security package download status using the **request security idp security-package download status** command, a message is displayed confirming that the downloaded security package is being synchronized on the primary and secondary nodes.

[*Junos OS Security Configuration Guide*]

J-Web

- **J-Web support for IPv6 stage 3 security features**—This feature is supported on all branch SRX Series and J Series devices.

  The following J-Web pages have been added to support the IPv6 feature:

  - Proxy ND Configuration page
  - DS-Lite Configuration page

  The following J-Web pages have been updated to include IPv6 support:

  - Source NAT Pool Configuration page
  - Static NAT Rule Configuration page
  - Source NAT Rule Configuration page

- Destination NAT Pool Configuration page
- Destination NAT Rule Configuration page

Routing

- **Equal-cost multipath (ECMP) flow-based forwarding**—This feature is supported on all branch SRX Series and J Series devices.

  An equal-cost multipath (ECMP) set is formed when the routing table contains multiple next-hop addresses for the same destination with equal cost. (Routes of equal cost have the same preference and metric values.) If there is an ECMP set for the active route, the Junos OS software uses a hash algorithm to choose *one* of the next-hop addresses in the ECMP set to install in the forwarding table.

  You can configure Junos OS so that multiple next-hop entries in an ECMP set are installed in the forwarding table. On Juniper Networks devices, per-packet or per-flow load balancing can be performed to spread traffic across multiple paths between routing devices. On Juniper Networks security devices, source and destination IP addresses and protocols are examined to determine individual traffic flows. Packets for the same flow are forwarded on the same interface; the interface does not change when there are additions or changes to the ECMP set. This is important for features such as source NAT, where the translation is performed only during the first path of session establishment; IDP; ALG; and route-based VPN tunnels. If a packet arrives on a given interface in an ECMP set, the security device ensures that reverse traffic is forwarded through the same interface.

  NOTE: ECMP flow-based forwarding on security devices applies only to IPv4 unicast traffic flows. Multicast and IPv6 flows are not supported.

  In a chassis cluster deployment, a *local* interface is an interface that is on the same node as the interface on which a packet arrives, and a *remote* interface is an interface that is on the other chassis cluster node. If an ECMP route has both local and remote interfaces in a chassis cluster, then the local interface is favored for the next hop.

  To configure ECMP flow-based forwarding on Juniper Networks security devices, first define a load-balancing routing policy by including one or more **policy-statement** configuration statements at the [**edit policy-options**] hierarchy level, with the action **load-balance per-packet**. Then apply the routing policy to routes exported from the routing table to the forwarding table. To do this, include the **forwarding-table** and **export** configuration statements at the [**edit routing-options**] hierarchy level.

  [*Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*]

Security Policy

- **Hit-count tracking**—This feature is supported on all branch SRX Series devices.

  The new **show security policies hit-count** command displays the utility rate of security policies according to the number of hits they receive. You can use this feature to determine which policies are being used on the device, and how frequently they are used. Depending on the command options that you choose, the number of hits can be listed without order or sorted in either ascending or descending order, and they can be restricted to the number of hits that fall above or below a specific count or within a range. Data is shown for all zones associated with the policies or named zones.

  [*Junos OS CLI Reference*, *Junos OS Security Configuration Guide*]

UAC Authentication

- **Security enhancement between an access control service and an Infranet Enforcer**—This feature is supported on all branch SRX Series devices.

  To improve security for a UAC configuration, a message appears if the Access Control Service's certificate cannot be verified on the SRX Series device. To ensure that the Access Control Service and the Enforcer are connected securely, configure the ca-profile on the SRX Series device to verify the Access Control Service's certificate.

  [*Junos OS Security Configuration Guide*]

User Role Firewalls

- **User role firewall providing flexibility and higher security**—This feature is supported on all branch SRX Series devices.

  Network security enforcement, monitoring, and reporting based solely on IP information soon will not be sufficient for today's dynamic and mobile workforce. By integrating user firewall policies, administrators can permit or restrict network access of employees, contractors, partners, and other users based on the roles they are assigned.

  A new match criteria, source-identity, defines applicable roles for each policy. In this way, traffic can be permitted or denied access based on the role of the user, as well as the zone pair, source and destination IP addresses, and application.

  To enhance a user role firewall implementation, the SRX Series device can be configured to interact with a Junos Pulse Access Control Service, providing a source of dynamic user role information. The Access Control Service can also be configured as a relay between a third-party authentication server and the SRX Series device. In this configuration, SPNEGO and Kerberos protocols provide a single sign-on environment for dynamic role provisioning.

  [*Junos OS Security Configuration Guide*, *Unified Access Control Solution Guide for SRX Series Services Gateways*]

Hardware Features—SRX550 Services Gateways

Introduction

Junos OS Release 12.1 supports the Juniper Networks SRX550 Services Gateway. The SRX550 Services Gateway is a mid-range dynamic services gateway that consolidates network infrastructure and security applications for regional offices, large branch offices,

and small to medium enterprises. The services gateway provides cost-effective, scalable integration of routing, security, and other mid-range applications for these sites.

Hardware Features

The SRX550 Services Gateway provides the following features:

- Symmetric Multiprocessing-based data forwarding.
- Hardware-based control and data plane separation.
- Six on-board 10/100/1000Base-T Gigabit Ethernet ports.
- Four on-board SFP Gigabit Ethernet ports.
- Support for dual AC or DC power supplies with a redundant configuration in the chassis. The 645 W AC and DC power supplies with or without Power over Ethernet (PoE) support. The AC and DC power supplies are hot-swappable.
- Junos OS support for advanced security and routing services on the Services and Routing Engine (SRE).
- The services gateway supports Gigabit-Backplane Physical Interface Modules (GPIMs) and also Mini Physical Interface Modules (Mini-PIMs). For details about the supported GPIMs and Mini-PIMs, see the *SRX Series Services Gateway for the Branch Physical Interface Modules Hardware Guide*.

Physical Specifications

Table 2 on page 43 provides information on the physical specifications of the SRX550 Services Gateway.

Table 2: SRX550 Services Gateway Specifications

Specification	Value
Chassis height	2 rack units (U)
Chassis width	17.5 in. (44.4 cm)
Chassis depth	18.2 in. (46.2 cm)
Chassis weight (includes one power supply without any GPIMs or Mini-PIMs)	21.96 lb (9.96 kg)

Table 2: SRX550 Services Gateway Specifications *(continued)*

Specification	Value
Power supply output/consumption	645 W AC and 645 W DC power supply can provide: • 390 W at 12 V • 255 W PoE on a single power supply, or with redundancy using the two power supplies • 510 W PoE using the two power supply option operating as nonredundant NOTE: Using the two power supply option operating as nonredundant for up to 510 W PoE power, the administrator has the ability to prioritize the PoE ports that will receive power if an outage should occur to either the power source or to one of the power supplies.
Altitude	No performance degradation to 13,000 ft (3962.4m)
Relative humidity	Normal operation ensured in relative humidity range of 5% to 90%, noncondensing
Temperature	Normal operation ensured in temperature range of 32°F (0°C) to 104°F (+40°C) Nonoperating storage temperature in shipping container: –40° F (–40°C) to 158° F (70°C)
Seismic	Designed to meet Telcordia Technologies Zone 4 earthquake requirements
Maximum thermal output	AC power: 4400 BTU/hour DC power with one 645 W power supply unit: 2200 BTU/hour DC power with two 645 W power supply units, nonredundant: 4400 BTU/hour NOTE: These specifications are estimates and subject to change.
AC input voltage	100 to 240 VAC
AC input line frequency	50 to 60 Hz
AC system current rating	7.6 to 3.8 A

NOTE: Install the services gateway only in restricted areas, such as dedicated equipment rooms and equipment closets, in accordance with Articles 110–16, 110–17, and 110–18 of the National Electrical Code, ANSI/NFPA 70.

Software Features—SRX550 Services Gateways

Software Features

- On SRX550 devices, the following software features are supported:
  - AppSecure
  - Chassis cluster
  - Cascading style sheet (CSS) integration test
  - Cellular broadband data bridge (CX111)
  - Data and voice Application Layer Gateways (ALGs)
  - Device Management Interface (DMI), Network and Security Manager (NSM), and Junos Space
  - Dynamic VPN configuration
  - Flow
  - Intrusion Detection and Prevention (IDP) Security
  - Interfaces
  - Internet Protocol Security Virtual Private Network (IPsec VPN)
  - Internet Protocol version 4 (IPv4), encapsulation, and quality of service (QoS)
  - Internet Protocol version 6 (IPv6)
  - IPv6 CSS
  - J-Web
  - Layer 2 Transparent Mode (L2TM), standalone and high availability
  - Layer 2 Switching Support
  - Network address translation
  - Policies
  - Screen
  - Simple Network Management Protocol (SNMP)
  - Syslog
  - Uboot
  - Unified Threat Management (UTM)

- VPN
- Zones

Related Documentation

- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 46
- Known Limitations in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 48
- Outstanding Issues in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 71
- Resolved Issues in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 76
- Errata and Changes in Documentation for Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 85
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 89

Changes in Default Behavior and Syntax in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers

The following current system behavior, configuration statement usage, and operational mode command usage might not yet be documented in the Junos OS documentation:

AppSecure

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, application tracking is enabled by default. You can disable application tracking with the set security application-tracking disable command. This command disables application tracking without deleting the zone configuration.

Command-Line Interface (CLI)

- On all branch SRX Series devices, in Junos OS Release 11.4 and earlier releases, if an invalid value of reboot_reason was detected, the **show chassis routing-engine** command would indicate a normal shutdown. Because of this, a flash memory corruption would go undetected. This issue is now fixed in Junos OS Release 12.1. The behavior is changed, and the reboot reason displays "Unknown reboot_reason", with the invalid value of reboot_reason, in hexadecimal format.

Deprecated Items for Security Hierarchy

Table 3: Items Deprecated in Release 12.1

Deprecated Item	Replacement	Hierarchy Level or Command Syntax	Additional Information
node	-	**request security idp security-package download**	On all branch SRX Series devices operating in a chassis cluster, the **request security idp security-package download** command with the **node** option is not supported: **request security idp security-package download node primary** **request security idp security-package download node local** **request security idp security-package download node all**

Hardware

- On SRX550 devices, the mini-USB console cable provides a “break” message to the Windows application whenever the console cable is unplugged and re-plugged. If you have configured “debugger-on-break”, the system goes to the **db>** prompt because the system receives a break character. This behavior is specific to the mini-USB console.

Related Documentation

- New Features in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 37

Known Limitations in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers

AppSecure

- **Junos OS application identification**—When you create custom application or nested application signatures for Junos OS application identification, the order value must be unique among all predefined and custom application signatures. The order value determines the application matching priority of the application signature.

  The order value is set with the **set services application-identification application application-name signature order** command. You can also view all signature order values by entering the **show services application-identification | display set | match order** command. You will need to change the order number of the custom signature if it conflicts with another application signature.

- J-Web pages for AppSecure are preliminary.
- Custom application signatures and custom nested application signatures are not currently supported by J-Web.
- AppFW does not operate on ALG data sessions. As a result, the AppFW rules are not applicable to these sessions. Therefore, ALG data sessions are excluded from AppFW counters.

AX411 Access Points

- On SRX210, SRX240, and SRX650 devices, up to four access points (maximum) can be configured and managed.
- On all branch SRX devices, managing AX411 WLAN Access Points through a Layer 3 Aggregated Ethernet (ae) interface is not supported.

Chassis Cluster

- SRX100, SRX210, SRX240, and SRX650 devices have the following chassis cluster limitations:
  - Virtual Router Redundancy Protocol (VRRP) is not supported.
  - In-service software upgrade (ISSU) is not supported.
  - The 3G dialer interface is not supported.
  - On SRX Series device failover, access points on the Layer 2 switch reboot and all wireless clients lose connectivity for 4 to 6 minutes.
  - On very-high-bit-rate digital subscriber line (VDSL) mini-PIM, chassis cluster is not supported for VDSL mode.
  - Queuing on the aggregated Ethernet **(ae)** interface is not supported.
  - Group VPN is not supported.
  - Sampling features like J-FLow, packet capture, and port mirror on the **reth** interface are not supported.
  - Switching is not supported in chassis cluster mode for SRX100 and SRX210.
  - The Chassis Cluster MIB is not supported.
  - Any packet-based services like MPLS and CLNS are not supported.
  - lsq-0/0/0—Link services Multilink Point-to-Point Protocol (MLPPP), Multilink Frame Relay (MLFR), and Compressed Real-Time Transport Protocol (CRTP) are not supported.
  - lt-0/0/0—CoS for real-time performance monitoring (RPM) is not supported.
  - PP0: PPPoE, PPPoEoA is not supported.
- Packet-based forwarding for MPLS and International Organization for Standardization (ISO) protocol familes is not supported.
- Layer 2 Ethernet switching

  The factory default configuration for SRX100 and SRX210 devices automatically enables Layer 2 Ethernet switching. Because Layer 2 Ethernet switching is not supported in chassis cluster mode, for these devices, if you use the factory default configuration, you must delete the Ethernet switching configuration before you enable chassis clustering.

  CAUTION: **Enabling chassis clustering while Ethernet switching is enabled is not a supported configuration and might result in undesirable behavior from the devices, leading to possible network instability.**

The default configuration for other SRX Series devices and all J Series devices does not automatically enable Ethernet switching. However, if you have enabled Ethernet switching, be sure to disable it before enabling clustering on these devices too.

- On all J Series devices, a Fast Ethernet port from a 4-port Ethernet PIM cannot be used as a fabric link port in a chassis cluster.
- On all branch SRX Series devices, only redundant Ethernet interfaces (reth) are supported for IKE external interface configuration in IPsec VPN. Other interface types can be configured, but IPsec VPN might not work.
- On all J Series devices, the ISDN feature on chassis cluster is not supported.

Command-Line Interface (CLI)

- On all branch SRX and all J Series devices, the **clear services flow** command is not supported.
- On all J Series devices, RADIUS accounting is not supported.
- On SRX210 and SRX240 devices, J-Web crashes if more than nine users log in to the device by using the CLI. The number of users allowed to access the device is limited as follows:
  - For SRX210 devices: four CLI users and three J-Web users
  - For SRX240 devices: six CLI users and five J-Web users
- On J6350 devices, there is a difference in the power ratings provided by user documentation (*J Series Services Routers Hardware Guide* and PIM, uPIM, and ePIM Power and Thermal Calculator) and the power ratings displayed by CLI (by a unit of 1). The cause of this issue is a round off error, where the CLI display rounds off the value to a lower integer and the ratings provided in user documentation rounds off the value to the higher integer. As a workaround, follow the user documentation for accurate ratings.

DOCSIS Mini-PIM

- On SRX210 devices, the DOCSIS Mini-PIM delivers speeds up to a maximum of 100 Mbps throughput in each direction.

Dynamic Host Configuration Protocol (DHCP)

- On all branch SRX Series and J Series devices do not support DHCPv6 client authentication is not supported.

Dynamic VPN

SRX100, SRX210, and SRX240 devices have the following limitations:

- The IKE configuration for the Junos Pulse client does not support the hexadecimal preshared key.

- The Junos Pulse client IPsec does not support the Authentication Header (AH) protocol and the Encapsulating Security Payload (ESP) protocol with NULL authentication.
- When you log in through the Web browser (instead of logging in through the Junos Pulse client) and a new client is available, you are prompted for a client upgrade even if the **force-upgrade** option is configured. Conversely, if you log in using the Junos Pulse client with the **force-upgrade** option configured, the client upgrade occurs automatically (without a prompt).
- On all branch SRX Series devices, DH-group 14 is not supported for dynamic VPN.
- On all branch SRX devices, when you download the Pulse client using the Mozilla browser, the “Launching the VPN Client” page is displayed when Junos Pulse is still downloading. However, when you download the Pulse client using Internet Explore, “Launching the VPN Client” page is displayed after Junos Pulse has been downloaded and installed.

Flow and Processing

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, due to a limit on the number of large packet buffers, Routing Engine based sampling might run out of buffers for packet sizes greater than or equal to 1500 bytes and hence those packets will not be sampled. You could run out of buffers when the rate of the traffic stream is high.
- On SRX100 and SRX240 devices, the data file transfer rate for more than 20 megabits per second is reduced by 60 percent with the introduction of Junos Pulse1.0 client as compared to the Acadia client that was used before Junos OS Release 11.1.
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the default authentication table capacity is 10,000; the administrator can increase the capacity to a maximum of 15,000.
- On all branch SRX Series and J Series devices, when devices are operating in flow mode, the Routing Engine side cannot detect the path maximum transmission unit (PMTU) of an IPv6 multicast address (with a large size packet).
- On all branch SRX Series devices, you cannot configure route policies and route patterns in the same dial plan.
- On all branch SRX Series devices, you can configure no more than four members in a station group. Station groups are used for hunt groups and ring groups.
- On all J Series devices, even when forwarding options are set to drop packets for the ISO protocol family, the device forms End System-to-Intermediate System (ES-IS) adjacencies and transmits packets because ES-IS packets are Layer 2 terminating packets.
- On all branch SRX Series and J Series devices, high CPU utilization triggered for reasons such as CPU intensive commands and SNMP walks causes the Bidirectional Forwarding Detection protocol (BFD) to flap while processing large BGP updates.
- On SRX210, SRX240, and J Series devices, broadcast TFTP is not supported when flow is enabled on the device.

- Maximum concurrent SSH, Telnet, and Web sessions — On SRX210, SRX240, and SRX650 devices, the maximum number of concurrent sessions is as follows:

Sessions	SRX210	SRX240	SRX650
ssh	3	5	5
telnet	3	5	5
Web	3	5	5

NOTE: These defaults are provided for performance reasons.

- On SRX210 and SRX240 devices, for optimized efficiency, we recommend that you limit use of CLI and J-Web to the numbers of sessions listed in the following table:

Device	CLI	J-Web	Console
SRX210	3	3	1
SRX240	5	5	1

- On SRX100 devices, Layer 3 control protocols (OSPF, using multicast destination MAC address) on the VLAN Layer 3 interface work only with access switch ports.

Group VPN Interoperability with Cisco's GET VPN for Juniper Networks Security Devices that Support Group VPN

Cisco's implementation of the Group Domain of Interpretation (GDOI) is called *Group Encryption Transport (GET) VPN*. While group VPN in Junos OS and Cisco's GET VPN are both based on RFC 3547, *The Group Domain of Interpretation*, there are some implementation differences that you need to be aware of when deploying GDOI in a networking environment that includes both Juniper Networks security devices and Cisco routers. This topic discusses important items to note when using Cisco routers with GET VPN and Juniper Networks security devices with group VPN.

Cisco GET VPN members and Juniper Group VPN members can interoperate as long as the server role is played by a Cisco GET VPN server, Juniper Networks security devices are group members, and with the following caveats:

The group VPN in Release 12.1 of Junos OS has been tested with Cisco GET VPN servers running Version 12.4(22)T and Version 12.4(24)T.

To avoid traffic disruption, do not enable rekey on a Cisco server when the VPN group includes a Juniper Networks security device. The Cisco GET VPN server implements a proprietary ACK for unicast rekey messages. If a group member does not respond to the unicast rekey messages, the group member is removed from the group and is not able to receive rekeys. An out-of-date key causes the remote peer to treat IPsec packets as

bad security parameter indexes (SPIs). The Juniper Networks security device can recover from this situation by reregistering with the server to download the new key.

Antireplay must be disabled on the Cisco server when a VPN group of more than two members includes a Juniper Networks security device. The Cisco server supports time-based antireplay by default. A Juniper Networks security device will not interoperate with a Cisco group member if time-based antireplay is used because the timestamp in the IPsec packet is proprietary. Juniper Networks security devices are not able to synchronize time with the Cisco GET VPN server and Cisco GET VPN members because the sync payload is also proprietary. Counter-based antireplay can be enabled if there are only two group members.

According to Cisco documentation, the Cisco GET VPN server triggers rekeys 90 seconds before a key expires, and the Cisco GET VPN member triggers rekeys 60 seconds before a key expires. When interacting with a Cisco GET VPN server, a Juniper Networks security device member needs to match Cisco behavior.

A Cisco GET VPN member accepts all keys downloaded from the GET VPN server. Policies associated with the keys are dynamically installed. A policy does not have to be configured on a Cisco GET VPN member locally, but a deny policy can optionally be configured to prevent certain traffic from passing through the security policies set by the server. For example, the server can set a policy to have traffic between subnet A and subnet B be encrypted by key 1. The member can set a deny policy to allow OSPF traffic between subnet A and subnet B not to be encrypted by key 1. However, the member cannot set a permit policy to allow more traffic to be protected by the key. The centralized security policy configuration does not apply to the Juniper Networks security device.

On a Juniper Networks security device, the **ipsec-group-vpn** configuration statement in the permit tunnel rule in a scope policy references the group VPN. This allows multiple policies referencing a VPN to share an SA. This configuration is required to interoperate with Cisco GET VPN servers.

Logical key hierarchy (LKH), a method for adding and removing group members, is not supported with group VPN on Juniper Networks security devices.

GET VPN members can be configured for cooperative key servers (COOP KSs), an ordered list of servers with which the member can register or reregister. Multiple group servers cannot be configured on group VPN members.

Hardware

This section covers filter and policing limitations.

- On SRX650 devices, the T1/E1 GPIMs (2-port or 4-port version) do not work in Junos OS Release 9.6R1. This issue is resolved in Junos OS Release 9.6R2 and later releases, but if you roll back to the 9.6R1 image, this issue is still seen.

Interfaces and Routing

- On SRX100 and J Series devices, dynamic VLAN assignments and guest VLANs are not supported on J Series and SRX100 devices.
- On SRX650 devices, Ethernet switching is not supported on Gigabit Ethernet interfaces (**ge-0/0/0** through **ge-0/0/3** ports).
- On SRX210, SRX220, SRX240, and SRX650 devices, logs cannot be sent to NSM when logging is configured in the stream mode. Logs cannot be sent because, the security log does not support configuring of the source IP address for the **fxp0** interface and the security log destination in stream mode cannot be routed through the **fxp0** interface. This implies that you can not configure the security log server in the same subnet as the **fxp0** interface and the route the log server through the **fxp0** interface.
- On all branch SRX Series devices, the number of child interfaces per node is restricted to 4 on the reth interface and the number of child interfaces per reth interface is restricted to 8.
- On SRX240 High Memory devices, traffic might stop between the SRX240 device and the Cisco switch due to link mode mismatch. We recommend setting autonegotiation parameters on both ends to the same value.
- On SRX100 devices, the link goes down when you upgrade FPGA on 1xGE SFP. As a workaround, run the **restart fpc** command and restart the FPC.
- On SRX210 devices with VDLS2, ATM COS VBR-related functionality cannot be tested.
- On SRX210 devices, Internet Group Management Protocol version 2 (IGMPv2) JOINS messages are dropped on an integrated routing and bridging (IRB) interface. As a workaround, enable IGMP snooping to use IGMP over IRB interfaces.
- On all J Series devices, the DS3 interface does not have an option to configure multilink-frame-relay-uni-nni (MFR).
- On SRX210, SRX220, and SRX240 devices, every time the VDSL2 PIM is restarted in the asymmetric digital subscriber line (ADSL) mode, the first packet passing through the PIM is dropped.
- On SRX240 Low Memory devices and SRX240 High Memory devices, the RPM server operation does not work when the probe is configured with the option **destination-interface**.
- On all J Series devices, Link Layer Discovery Protocol (LLDP) is not supported on routed ports.

- In J Series xDSL PIMs, mapping between IP CoS and ATM CoS is not supported. If the user configures IP CoS in conjunction with ATM CoS, the logical interface level shaper matching the ATM CoS rate must be configured to avoid congestion drops in segmentation and reassembly (SAR).

  Example:
  set interfaces at-5/0/0 unit 0 vci 1.110
  set interfaces at-5/0/0 unit 0 shaping cbr 62400 ATM COS
  set class-of-service interfaces at-5/0/0 unit 0 scheduler-map sche_map IP COS
  set class-of-service interfaces at-5/0/0 unit 0 shaping-rate 62400 ADD IFL SHAPER

- On SRX210, SRX220, and SRX240 devices, 1-port Gigabit Ethernet SFP mini-PIM does not support switching in Junos OS Release 12.1.
- On SRX650 devices, MAC pause frame and frame check sequence (FCS) error frame counters are not supported for the interfaces **ge-0/0/0** through **ge-0/0/3**.
- On SRX240 and SRX650 devices, the VLAN range from 3967 to 4094 falls under the reserved VLAN address range, and the user is not allowed any configured VLANs from this range.
- On SRX650 devices, the last four ports of a 24-Gigabit Ethernet switch GPIM can be used either as RJ-45 or SFP ports. If both are present and providing power, the SFP media is preferred. If the SFP media is removed or the link is brought down, then the interface will switch to the RJ-45 medium. This can take up to 15 seconds, during which the LED for the RJ-45 port might go on and off intermittently. Similarly, when the RJ-45 medium is active and an a small form-factor pluggable transceiver (SFP) link is brought up, the interface will transition to the SFP medium, and this transition could also take a few seconds.
- On SRX210 devices, the USB modem interface can handle bidirectional traffic of up to 19 Kbps. On oversubscription of this amount (that is, bidirectional traffic of 20 Kbps or above), **keepalives** do not get exchanged, and the interface goes down.
- On SRX100, SRX210, SRX240, and SRX650 devices, on the Layer 3 **ae** interface, the following features are not supported:
  - Encapsulations (such as CCC, VLAN CCC, VPLS, and PPPOE) on Layer 3 **ae** interfaces
  - J-Web
  - Layer 3 **ae** for 10-Gigabit Ethernet
- On SRX100 devices, the multicast data traffic is not supported on IRB interfaces.
- On SRX240 High Memory devices, when the **system login deny-sources** statement is used to restrict the access, it blocks a remote copy (rcp) between nodes, which is used to copy the configuration during the commit routine. Use a firewall filter on the lo0.0 interface to restrict the Routing Engine access, However, if you choose to use the **system login deny-sources** statement, check the private addresses that were automatically on lo0.x and sp-0/0/0.x and exclude them from the denied list.
- On SRX100, SRX210, SRX220, SRX240, SRX650, and all J Series devices, on VLAN-tagged routed interfaces, LLDP is not all supported.

Internet Key Exchange Version 2 (IKEv2)

On all branch SRX Series devices, IKEv2 does not include support for:

- Policy-based tunnels
- Dial-up tunnels
- Network Address Translation-Traversal (NAT-T)
- VPN monitoring
- Next-Hop Tunnel Binding (NHTB) for st0—Reusing the same tunnel interface for multiple tunnels
- Extensible Authentication Protocol (EAP)
- IPv6
- Multiple child SAs for the same traffic selectors for each QoS value
- Proposal enhancement features
- Reuse of Diffie-Hellman (DH) exponentials
- Configuration payloads
- IP Payload Compression Protocol (IPComp)
- Dynamic Endpoint (DEP)

Internet Protocol Security (IPsec)

- On all branch SRX Series devices, when you enable VPN, overlapping of the IP addresses across virtual routers is supported with following limitations:
  - An IKE external interface address cannot overlap with any other virtual router.
  - An internal/trust interface address can overlap across virtual routers.
  - An **st0** interface address cannot overlap in route-based VPN in point-to-multipoint tunnels such as NHTB.
  - An **st0** interface address can overlap in route-based VPN in point-to-point tunnels.

Intrusion Detection and Prevention (IDP)

- On all branch SRX Series devices, from Junos OS Release 11.2 and later, the IDP security package is based on the Berkeley database. Hence, when the Junos OS image is upgraded from Junos OS Release 11.1 or earlier to Junos OS 11.2 or later, a migration of IDP security package files needs to be performed. This is done automatically on upgrade when the IDP daemon comes up. Similarly, when the image is downgraded, a migration (secDb install) is automatically performed when the IDP daemon comes up, and previously installed database files get deleted.

  However, migration is dependent on the XML files for the installed database to be present on the device. For first-time installation, full update files are required. If the

last update on the device was an incremental update, migration might fail. In such a case, you have to manually download and install the IDP security package using the **download** or **install** CLI command before using the IDP configuration with predefined attacks or groups.

Workaround: Use the following CLI commands to manually download the individual components of the security package from the Juniper Security Engineering portal and install the full update:

- **request security idp security-package download full-update**
- **request security idp security-package install**

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the **request services application-identification uninstall** command will uninstall all predefined signatures.
- On all branch SRX Series devices, IDP does not allow header checks for nonpacket contexts.
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the maximum supported number of entries in the ASC table for is 100,000 entries. However, because the user land buffer has a fixed size of 1 MB as a limitation, it displays a maximum of 38,837 cache entries.
- On SRX100, SRX210, SRX240, and SRX650 devices, policy compilation takes a long time because:
  - Software DFA is now used for attack signature compilation.
  - The IDPD daemon gets a smaller CPU time slice during compilation.
- The maximum number of IDP sessions supported is 16,384 on SRX210 devices, 32,768 on SRX240 devices, and 13,1072 on SRX650 devices.
- On all branch SRX Series devices, all IDP policy templates are supported except All Attacks. There is a 100-MB policy size limit for integrated mode and a 150-MB policy size limit for dedicated mode. The current IDP policy templates supported are dynamic, based on the attack signatures being added. Therefore, be aware that supported templates might eventually grow past the policy-size limit.

  On all branch SRX Series devices, the following IDP policies are supported:

  - DMZ_Services
  - DNS_Service
  - File_Server
  - Getting_Started
  - IDP_Default
  - Recommended
  - Web_Server

- On all branch SRX Series devices, IDP deployed in both active/active and active/passive chassis clusters has the following limitations:
  - No inspection of sessions that fail over or fail back.
  - The IP action table is not synchronized across nodes.
  - The Routing Engine on the secondary node might not be able to reach networks that are reachable only through a Packet Forwarding Engine.
  - The SSL session ID cache is not synchronized across nodes. If an SSL session reuses a session ID and it happens to be processed on a node other than the one on which the session ID is cached, the SSL session cannot be decrypted and will be bypassed for IDP inspection.
- On all branch SRX Series devices, IDP deployed in active/active chassis clusters has a limitation that for time-binding scope source traffic, if attacks from a source (with more than one destination) have active sessions distributed across nodes, then the attack might not be detected because time-binding counting has a local-node-only view. Detecting this sort of attack requires an RTO synchronization of the time-binding state that is not currently supported.

NOTE: **On SRX100 devices, IDP high availability (HA) is supported in active/backup mode.**

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the IDP policies for each user logical system are compiled together and stored on the data plane memory. To estimate adequate data plane memory for a configuration, consider these two factors:
  - IDP policies applied to each user logical system are considered unique instances because the ID and zones for each user logical system are different. Estimates need to take into account the combined memory requirements for all user logical systems.
  - As the application database increases, compiled policies will require more memory. Memory usage should be kept below the available data plane memory to allow for database increases.

IPv6 IPsec

The IPv6 IPsec implementation has the following limitations:

- IPv6 routers do not perform fragmentation. IPv6 hosts should either perform path maximum transmission unit (PMTU) discovery or send packets smaller than the IPv6 minimum MTU size of 1280 bytes.
- Because IPv6 addresses are 128 bits long compared to IPv4 addresses, which are 32-bits long, IPv6 IPsec packet processing requires more resources. Therefore, a small performance degradation is observed.
- IPv6 uses more memory to set up the IPsec tunnel. Therefore, the IPsec IPv4 tunnel scalability numbers might drop.

- The addition of IPv6 capability might cause a drop in the IPsec IPv4-in-IPv4 tunnel throughput performance.
- The IPv6 IPsec VPN does not support the following functions:
  - 4in6 and 6in4 policy-based site-to-site VPN, IKE
  - 4in6 and 6in4 route-based site-to-site VPN, IKE
  - 4in6 and 6in4 policy-based site-to-site VPN, Manual Key
  - 4in6 and 6in4 route-based site-to-site VPN, Manual Key
  - 4in4, 6in6, 4in6, and 6in4 policy-based dial-up VPN, IKE
  - 4in4, 6in6, 4in6, and 6in4 policy-based dial-up VPN, Manual Key
  - Remote Access—XAuth, config mode, and shared IKE identity with mandatory XAuth
  - IKE authentication—public key infrastructure/digital signature algorithm (PKI/DSA)
  - IKE peer type—Dynamic IP
  - Chassis cluster for basic VPN features
  - IKE authentication—PKI/RSA
  - Network Address Translation-Traversal (NAT-T)
  - VPN monitoring
  - Hub-and-spoke VPNs
  - Next Hop Tunnel Binding Table (NHTB)
  - Dead Peer Detection (DPD)
  - Simple Network Management Protocol (SNMP) for IPsec VPN MIBs
  - Chassis cluster for advanced VPN features
  - IPv6 link-local address

Layer 2 Transparent Mode

- DHCP server propagation is not supported in Layer 2 transparent mode.

IPv6 Support

- **NSM**—Consult the Network and Security Manager (NSM) release notes for version compatibility, required schema updates, platform limitations, and other specific details regarding NSM support for IPv6 addressing on SRX Series and J Series devices.

J-Web

- **SRX Series and J Series browser compatibility**

  - To access the J-Web interface, your management device requires the following software:
    - Supported browsers—Microsoft Internet Explorer version 7.0 or Mozilla Firefox version 3.0
    - Language support—English-version browsers
    - Supported OS—Microsoft Windows XP Service Pack 3
  - If the device is running the worldwide version of the Junos OS and you are using the Microsoft Internet Explorer Web browser, you must disable the Use SSL 3.0 option in the Web browser to access the device.
  - To use the Chassis View, a recent version of Adobe Flash that supports ActionScript and AJAX (Version 9) must be installed. Also note that the Chassis View is displayed by default on the Dashboard page. You can enable or disable it using options in the Dashboard Preference dialog box, but clearing cookies in Internet Explorer also causes the Chassis View to be displayed.

- On all branch SRX Series devices, in the J-Web interface, there is no support for changing the T1 interface to an E1 interface or vice versa. As a workaround, use the CLI to convert from T1 to E1 and vice versa.
- On all branch SRX Series and J Series devices, users cannot differentiate between Active and Inactive configurations on the System Identity, Management Access, User Management, and Date & Time pages.
- On SRX210 devices, there is no maximum length when the user commits the hostname in CLI mode; however, only 58 characters, maximum, are displayed in the J-Web System Identification panel.
- On all J Series devices, some J-Web pages for new features (for example, the Quick Configuration page for the switching features on J Series devices) display content in one or more modal pop-up windows. In the modal pop-up windows, you can interact only with the content in the window and not with the rest of the J-Web page. As a result, online Help is not available when modal pop-up windows are displayed. You can access the online Help for a feature only by clicking the **Help** button on a J-Web page.
- On all branch SRX Series devices, you cannot use J-Web to configure a VLAN interface for an IKE gateway. VLAN interfaces are not currently supported for use as IKE external interfaces.

Network Address Translation (NAT)

- Maximum capacities for source pools and IP addresses have been extended on SRX650 devices, as follows:

Devices	Source NAT Pools	PAT Maximum Address Capacity	Pat Port Number	Source NAT rules number
SRX650	1024	1024	64M	1024

  Increasing the capacity of source NAT pools consumes memory needed for port allocation. When source NAT pool and IP address limits are reached, port ranges should be reassigned. That is, the number of ports for each IP address should be decreased when the number of IP addresses and source NAT pools is increased. This ensures NAT does not consume too much memory. Use the **port-range** statement in configuration mode in the CLI to assign a new port range or the **pool-default-port-range** statement to override the specified default.

  Configuring port overloading should also be done carefully when source NAT pools are increased.

  For source pool with port address translation (PAT) in range (64,510 through 65,533), two ports are allocated at one time for RTP/RTCP applications, such as SIP, H.323, and RTSP. In these scenarios, each IP address supports PAT, occupying 2048 ports (64,512 through 65,535) for Application Layer Gateway (ALG) module use.

- **NAT rule capacity change**—To support the use of large-scale NAT (LSN) at the edge of the carrier network, the device-wide NAT rule capacity has been changed.

  The number of destination and static NAT rules has been incremented as shown in Table 4 on page 61. The limitation on the number of destination-rule-set and static-rule-set has been increased.

  Table 4 on page 61 provides the requirements per device to increase the configuration limitation as well as to scale the capacity for each device.

Table 4: Number of Rules on SRX Series and J Series Devices

NAT Rule Type	SRX100	SRX210	SRX240	SRX650	J Series
Source NAT rule	512	512	1024	1024	512
Destination NAT rule	512	512	1024	1024	512
Static NAT rule	512	512	1024	6144	512

  The restriction on the number of rules per rule set has been increased so that there is only a device-wide limitation on how many rules a device can support. This restriction is provided to help you better plan and configure the NAT rules for the device.

Power over Ethernet (PoE)

- On SRX210-PoE devices, SDK packages might not work.

Security

- J Series devices do not support the authentication order **password radius** or **password ldap** in the **edit access profile** *profile-name* **authentication-order** command. Instead, use **order radius password** or **ldap password**.
- On all branch SRX Series and J Series devices, the limitation on the number of addresses in an address-set has been increased. The number of addresses in an address-set now depends on the device and is equal to the number of addresses supported by the policy.

Table 5: Number of Addresses in an address-set on SRX Series and J Series Devices

Device	address-set
Default	1024
SRX100 High Memory	1024
SRX100 Low Memory	512
SRX210 High Memory	1024
SRX210 Low Memory	512
SRX240 High Memory	1024
SRX240 Low Memory	512
SRX650	1024
J Series	1024

Simple Network Management Protocol (SNMP)

- On all J Series devices, the SNMP NAT-related MIB is not supported in Junos OS Release 12.1.

Switching

- **Layer 2 transparent mode support**—On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the following features are not supported for Layer 2 transparent mode:
  - Gratuitious Address Resolution Protocol (GARP) on the Layer 2 interface
  - Spanning Tree Protocol (STP)

- IP address monitoring on any interface
- Transit traffic through integrated routing and bridging (IRB)
- IRB interface in a routing instance
- Chassis clustering
- IRB interface handling of Layer 3 traffic

NOTE: **The IRB interface is a pseudointerface and does not belong to the reth interface and redundancy group.**

- On SRX100, SRX210, SRX240, and SRX650 devices, Change of Authorization is not supported with 802.1x.
- On SRX100, SRX210, SRX240, and SRX650 devices, on the routed VLAN interface, the following features are not supported:
  - IPv6 (family inet6)
  - ISIS (family ISO)
  - Class of service
  - Encapsulations (Ether circuit cross-connect [CCC], VLAN CCC, VPLS, PPPoE, and so on) on VLAN interfaces
  - CLNS
  - Protocol Independent Multicast (PIM)
  - Distance Vector Multicast Routing Protocol (DVMRP)
  - VLAN interface MAC change
  - Gratuitous Address Resolution Protocol (ARP)
  - Change VLAN-Id for VLAN interface

Unified Threat Management (UTM)

- On all J Series devices, UTM requires 1 GB of memory. If your J2320, J2350, or J4350 device has only 512 MB of memory, you must upgrade the memory to 1 GB to run UTM.

Upgrade and Downgrade

- On all J Series devices, the Junos OS upgrade might fail due to insufficient disk space if the CompactFlash is smaller than 1-GB in size. We recommend using a 1-GB CompactFlash for Junos OS Release 10.0 and later.
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, when you connect a client running Junos Pulse 1.0 to an SRX Series device that is a running a later version

of Junos Pulse, the client will not be upgraded automatically to the later version. You must uninstall Junos Pulse1.0 from the client and then download the later version of Junos Pulse from the SRX Series device.

Virtual Private Networks (VPNs)

- On SRX100, SRX210, SRX240, and SRX650 devices, while configuring dynamic VPN using the Junos Pulse client, when you select the authentication-algorithm as sha-256 in the IKE proposal, the IPsec session might not get established.

Unsupported CLI for Branch SRX Series Services Gateways and J Series Services Routers

Accounting-Options Hierarchy

- On SRX100, SRX210, SRX220, SRX240, SRX650, and all J Series devices, the **accounting**, **source-class**, and **destination-class** statements in the **[accounting-options]** hierarchy level are not supported.

AX411 Access Point Hierarchy

- On SRX100 devices, there are CLI commands for wireless LAN configurations related to the AX411 Access Point. However, at this time, the SRX100 devices do not support the AX411 Access Point.

Chassis Hierarchy

- On SRX100, SRX210, SRX220, SRX240, SRX650, and all J Series devices, the following chassis hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set chassis craft-lockout

set chassis routing-engine on-disk-failure
```

Class-of-Service Hierarchy

- On SRX100, SRX210, SRX220, SRX240, SRX650, and all J Series devices, the following class-of-service hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set class-of-service classifiers ieee-802.1ad

set class-of-service interfaces interface-name unit 0 adaptive-shaper
```

Ethernet-Switching Hierarchy

- On SRX100, SRX210, SRX220, SRX240, SRX650, and all J Series devices, the following Ethernet-switching hierarchy CLI commands are not supported. However, if you enter

these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set ethernet-switching-options bpdu-block disable-timeout

set ethernet-switching-options bpdu-block interface

set ethernet-switching-options mac-notification

set ethernet-switching-options voip interface access-ports

set ethernet-switching-options voip interface ge-0/0/0.0 forwarding-class
```

Firewall Hierarchy

- On SRX100, SRX210, SRX220, SRX240 SRX650, and all J Series devices, the following Firewall hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set firewall family vpls filter

set firewall family mpls dialer-filter d1 term
```

Interfaces CLI Hierarchy

- On SRX100, SRX210, SRX220, SRX240, SRX650, and all J Series devices, the following interface hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.
  - Aggregated Interface CLI on page 65
  - ATM Interface CLI on page 66
  - Ethernet Interfaces on page 67
  - GRE Interface CLI on page 67
  - IP Interface CLI on page 67
  - LSQ Interface CLI on page 68
  - PT Interface CLI on page 68
  - T1 Interface CLI on page 68
  - VLAN Interface CLI on page 69

Aggregated Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
request lacp link-switchover ae0

set interfaces ae0 aggregated-ether-options lacp link-protection

set interfaces ae0 aggregated-ether-options link-protection
```

ATM Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces at-1/0/0 container-options

set interfaces at-1/0/0 atm-options ilmi

set interfaces at-1/0/0 atm-options linear-red-profiles

set interfaces at-1/0/0 atm-options no-payload-scrambler

set interfaces at-1/0/0 atm-options payload-scrambler

set interfaces at-1/0/0 atm-options plp-to-clp

set interfaces at-1/0/0 atm-options scheduler-maps

set interfaces at-1/0/0 unit 0 atm-l2circuit-mode

set interfaces at-1/0/0 unit 0 atm-scheduler-map

set interfaces at-1/0/0 unit 0 cell-bundle-size

set interfaces at-1/0/0 unit 0 compression-device

set interfaces at-1/0/0 unit 0 epd-threshold

set interfaces at-1/0/0 unit 0 inverse-arp

set interfaces at-1/0/0 unit 0 layer2-policer

set interfaces at-1/0/0 unit 0 multicast-vci

set interfaces at-1/0/0 unit 0 multipoint

set interfaces at-1/0/0 unit 0 plp-to-clp

set interfaces at-1/0/0 unit 0 point-to-point

set interfaces at-1/0/0 unit 0 radio-router

set interfaces at-1/0/0 unit 0 transmit-weight
```

```
set interfaces at-1/0/0 unit 0 trunk-bandwidth
```

Ethernet Interfaces

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces ge-0/0/1 gigether-options ignore-l3-incompletes

set interfaces ge-0/0/1 gigether-options mpls

set interfaces ge-0/0/0 stacked-vlan-tagging

set interfaces ge-0/0/0 native-vlan-id

set interfaces ge-0/0/0 radio-router

set interfaces ge-0/0/0 unit 0 interface-shared-with

set interfaces ge-0/0/0 unit 0 input-vlan-map

set interfaces ge-0/0/0 unit 0 output-vlan-map

set interfaces ge-0/0/0 unit 0 layer2-policer

set interfaces ge-0/0/0 unit 0 accept-source-mac

set interfaces fe-0/0/2 fastether-options source-address-filter

set interfaces fe-0/0/2 fastether-options source-filtering

set interfaces ge-0/0/1 passive-monitor-mode
```

GRE Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces gr-0/0/0 unit 0 ppp-options

set interfaces gr-0/0/0 unit 0 layer2-policer
```

IP Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces ip-0/0/0 unit 0 layer2-policer

set interfaces ip-0/0/0 unit 0 ppp-options
```

```
set interfaces ip-0/0/0 unit 0 radio-router
```

LSQ Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces lsq-0/0/0 unit 0 layer2-policer

set interfaces lsq-0/0/0 unit 0 family ccc

set interfaces lsq-0/0/0 unit 0 family tcc

set interfaces lsq-0/0/0 unit 0 family vpls

set interfaces lsq-0/0/0 unit 0 multipoint

set interfaces lsq-0/0/0 unit 0 point-to-point

set interfaces lsq-0/0/0 unit 0 radio-router
```

PT Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces pt-1/0/0 gratuitous-arp-reply

set interfaces pt-1/0/0 link-mode

set interfaces pt-1/0/0 no-gratuitous-arp-reply

set interfaces pt-1/0/0 no-gratuitous-arp-request

set interfaces pt-1/0/0 vlan-tagging

set interfaces pt-1/0/0 unit 0 radio-router

set interfaces pt-1/0/0 unit 0 vlan-id
```

T1 Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces t1-1/0/0 receive-bucket

set interfaces t1-1/0/0 transmit-bucket

set interfaces t1-1/0/0 encapsulation ether-vpls-ppp

set interfaces t1-1/0/0 encapsulation extended-frame-relay
```

```
set interfaces t1-1/0/0 encapsulation extended-frame-relay-tcc

set interfaces t1-1/0/0 encapsulation frame-relay-port-ccc

set interfaces t1-1/0/0 encapsulation satop

set interfaces t1-1/0/0 unit 0 encapsulation ether-vpls-fr

set interfaces t1-1/0/0 unit 0 encapsulation frame-relay-ppp

set interfaces t1-1/0/0 unit 0 layer2-policer

set interfaces t1-1/0/0 unit 0 radio-router

set interfaces t1-1/0/0 unit 0 family inet dhcp

set interfaces t1-1/0/0 unit 0 inverse-arp

set interfaces t1-1/0/0 unit 0 multicast-dlci
```

VLAN Interface CLI

- The following CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set interfaces vlan unit 0 family tcc

set interfaces vlan unit 0 family vpls

set interfaces vlan unit 0 accounting-profile

set interfaces vlan unit 0 layer2-policer

set interfaces vlan unit 0 ppp-options

set interfaces vlan unit 0 radio-router
```

Protocols Hierarchy

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the following CLI commands are not supported. However, if you enter these commands in the CLI editor, they will appear to succeed and will not display an error message.

```
set protocols bfd no-issu-timer-negotiation

set protocols bgp idle-after-switch-over

set protocols l2iw

set protocols bgp family inet flow

set protocols bgp family inet-vpn flow
```

```
set protocols igmp-snooping vlan all proxy
```

Routing Hierarchy

- On SRX100, SRX210, SRX220, SRX240, SRX650, and all J Series devices, the following routing hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set routing-instances  < instance_name > services

set routing-instances  < instance_name > multicast-snooping-options

set routing-instances  < instance_name > protocols amt

set routing-options bmp

set routing-options flow
```

Services Hierarchy

- On SRX100, SRX210, SRX220, SRX240, SRX650, and all J Series devices, the following services hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set services service-interface-pools
```

SNMP Hierarchy

- On SRX100, SRX210, SRX220, SRX240, SRX650, and all J Series devices, the following SNMP hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set snmp community  < community_name > logical-system

set snmp logical-system-trap-filter

set snmp trap-options logical-system

set snmp trap-group d1 logical-system
```

System Hierarchy

- On all SRX100, SRX210, SRX220, SRX240, and SRX650 devices, the following system hierarchy CLI commands are not supported. However, if you enter these commands in the CLI editor, they appear to succeed and do not display an error message.

```
set system diag-port-authentication
```

Related Documentation

- New Features in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 37
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 46
- Outstanding Issues in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 71
- Resolved Issues in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 76
- Errata and Changes in Documentation for Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 85
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 89

Outstanding Issues in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers

The following problems currently exist in Juniper Networks branch SRX Series Services Gateways and J Series Services Routers. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

AX411 Access Point

- On SRX210 PoE devices, the access point reboots when 100 clients are associated simultaneously, with each one transmitting 512-byte packets at 100 pps. [PR/469418]

Command-line Interface (CLI)

- On all branch SRX Series devices, the **show security ike security-associations** and **show security ike security-associations detail** commands outputs are in disorderly-manner. This is a display issue and have no impact on performance. [PR/729804]

Flow and Processing

- On SRX240 devices, when changing the link mode and/or speed while running traffic, the device might send some jabber frames to downstream device. [PR/423334]
- On J2350 devices, the CPU utilization rises sharply with 3000 connections per second due to **rtlogd** and **eventd** daemons consuming high CPU resources. [PR/586224]
- On all branch SRX Series devices, changes in policer, filter, or sampling configuration causes files to be generated during multicast traffic receipt. [PR/613782]
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, activating and deactivating logical interfaces a number of times might result in generation of a flowd core file. [PR/691907: This issue has been resolved.]
- On SRX550 devices, 100BASE-FX source photonics is not usable. [PR/701741]
- On SRX220 devices, GRE and GRE-IPsec performance drops are seen. [PR/706412]

Interfaces and Routing

- On SRX100, SRX110, SRX210, and all J Series devices, out-of-band dial-in access using serial modem does not work. [PR/458114]
- On SRX210 and J6350 devices, the ping operation does not work for higher packet size between dialer interfaces. [PR/484507]
- On SRX240 devices, fragments are dropped when large fragments (that is, those that must be further fragmented with sizes larger than 1514) are received. A workaround is to have egress interface MTU be less than 1514 when the SRX240 device is receiving fragments of larger size. [PR/595955]
- On all branch SRX Series and J Series devices, when the peers are connected directly through the T1 link and Ge links, the ping operation to the peer link local address of the T1 link interface does not go through the T1 link; instead it goes through the Ge link. [PR/684159]
- On SRX550 devices, Gigabit-Backplane Physical Interface Modules (GPIMs) are not supported. [PR/719882]

Intrusion Detection and Prevention (IDP)

- On SRX210, SRX220, SRX240, and SRX650 devices, when a wireless LAN access point is configured through Configure >WirelessLAN >Settings, if an existing name is provided for the new access point, no error will occur, but the existing configuration will be overwritten. [PR/691924]
- On J2350 and J4350 devices, policy compilation fails after downgrading from Junos OS Release 12.1 to any earlier image. As a workaround, after the downgrade, reinstall the IDP signature package by using the **request security idp security-packet download | install** command. [PR/702107]
- On SRX210 devices, the IDPD daemon generates a core file when the Packet Forwarding Engine is offline during the policy load operation. [PR/702321]

J-Web

- On SRX210, and J4350 devices, avoid logging out of the device on the Troubleshoot>CLI Terminal page, because the logout option on the page is hidden in the CLI. [PR/401772]
- On all branch SRX and J Series devices, the “input filter” and the “output filter” options are displayed on the VLAN Configuration page. However, the filter values under these filter options are not available for configuring filters to VLAN. [PR/460244]
- On SRX100, SRX210, SRX240, SRX650, and all J Series devices, if you try to change the position of columns using the drag-and-drop method, only the column header moves to the new position instead of the entire column in the following pages:
  - OSPF Configuration > OSPF Global Settings table
  - BGP Configuration page > Global Information table
  - LACP Configuration page > Add Interface window

[PR/465030]

- On all branch SRX and J Series devices, on the Monitor > Route Information page, if there are more than 50 routes, the system will not refresh back to the first page of the table after any query. To view the results, navigate to page 1 manually. [PR/476338]
- On all branch SRX and J Series devices, if you open configuration pages for class-of-service (CoS) classifiers and drop profiles (Configure > Class of Service > Classifiers and Configure > Class of Service > Drop Profile), and then exit the pages without editing the configuration, no validation messages are displayed and the configuration of the switch proceeds. [PR/495603]
- On SRX100, SRX210, SRX220, and SRX240 devices, in J-Web, policies configured under group global cannot be edited or deleted in the NAT and firewall wizards. [PR/552519]
- On SRX Series devices, the J-Web interface incorrectly displays the Session Expired pop-up window whenever flash storage is full. [PR/569931]
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, when you click Point and click CLI and navigate to any page, after the page loads, when you click the back button of the browser, the “web page has expired” error will be displayed. [PR/608761]
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, in J-Web, switching takes too long to respond and an error message might appear when there is traffic or when you navigate continuously between pages. As a workaround, log into the device again. [PR/612369]
- When you enter the destination port range as 1112 to some invalid value, it displays the following error message:

  Please enter valid ending port 0-65535

  This error message conflicts with the available range (1024 through 64387). [PR/673840]
- On SRX550 and SRX650 devices, the 2-Port 10 Gigabit Ethernet XPIM (SRX-GP-2XE-SFPP-TX) is not visible in the chassis view. [PR/680355]
- On all branch SRX Series devices, you cannot access the Help page directly using Monitor >Wireless LAN. As a workaround, navigate to Monitor>Interfaces and select Help>HelpContents. On the help Page, click the WLAN link in the list of items under Monitor Node. [PR/691915]
- On all branch SRX Series devices, while editing the radio settings for an AX411 Wireless LAN Access Point on Configure >Wireless LAN > Setting, you will not be able to edit the virtual access point, for which the security options configured are static-wep and dot1x. [PR/692195]
- On all branch SRX Series devices, if the device monitors more than one access point, a packet capture is enabled on one access point. When you try to see the details of other access points on the Monitor >Wireless LAN page, you see a Data Refresh Failed error message. As a workaround, enable or disable packet capture uniformly across all the monitored access points. [PR/692344]
- On all branch SRX Series devices, while configuring the security option of a virtual access point under radio settings of a wireless LAN access point with the value WPA

Enterprise, you cannot configure the RADIUS Server fields under the WPA Enterprise security option. [PR/692739]

- On SRX100, SRX210, SRX240, and SRX650 devices, the country code configured for the AX411 Wireless LAN Access Point connected to the device on the Configure > Wireless LAN > Setting page, does not reflect properly on the Monitor > Wireless LAN page. [PR/692740]
- On all branch SRX Series devices, users cannot configure supported rates and supported basic rates with different values on the Configure > Wireless LAN > Setting page. J-Web takes the values while deploying the configuration. [PR/696627]
- On all branch SRX Series devices, the protection field is cleared when a user uses the Edit Radio option button to edit the advanced options on the Configure >Wireless LAN > Setting page. [PR/696629]
- On all branch SRX Series devices, you cannot view the access point details of an active access point from the J-Web Monitor > Wireless LAN page. [PR/700513]
- On all branch SRX and J Series devices, when configuring a NAT rule-set in J-Web interface, security zones can not be displayed if no interfaces are configured for these security zones. [PR/703264]
- On SRX550 devices, there are extra LEDs in the Chassis View and the tooltip for the following two LEDs show incorrect information:
  - External CF need to be changed to 'ACE'
  - ACE needs to be changed to Storage

  [PR/711596]
- On SRX550 devices, VLAN configuration is not be allowed on 2x10 Gigabit ports. [PR/721676]

PPPoE Wizard

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, in order to apply a new PPPoE configuration to a port already in use outside of the PPPoE wizard, it is necessary to remove all existing interface configurations. When the underlying interface is currently configured with VPN, NAT, MLPP, and some other applications, it is not possible to remove the existing configuration within the PPPoE wizard. [PR/685443]
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, PPPoE connections set using the PPPoE wizard are not available for edit or delete options in other J-Web pages. [PR/688421]
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, in J-Web, the PPPoE wizard is not supported if you are using Microsoft Internet Explorer version 9.0. As a workaround, use Microsoft Internet Explorer version 7 or version 8, or use Mozilla Firefox version 3 and above upto version 6.0. [PR/694026]

  Workaround: Use

Software

- On SRX550 devices, the following features are not supported:
  - J-Web enhancements
  - Performance improvement for httpd
  - PPPoE over reth support
  - PPPoE J-Web
  - Track-IP Enhancements
  - J-Web Initial Setup Wizard
  - AX411
  - Syslog/security log setting with J-Web
  - Layer 2 Transparent Mode
  - Supportability SRD
  - JSF crypto enhancements
  - Enhanced Web Filtering
  - Support for UTM in cluster: Active RE on different node than Active Packet Forwarding Engine
  - USB disable
  - DHCP daemon VR support
  - Mac filtering
  - DNS proxy/dynamic DNS/split DNS
  - VC scaling
  - SSD
  - OIR for all PIMs

[PR/693643]

Unified Threat Management (UTM)

- On SRX240 High Memory devices, during UTM Web traffic stress test, some leak of AV scanner contexts is observed in some error pages. [PR/538470]
- On SRX650 devices, UTM EAV throughput performance is dropping by 43 percent because of changes made to the JPME code to avoid forwarding daemon core files. [PR/583630]

Upgrade and Downgrade

- On all branch SRX Series devices, application identification does not support the downgrade of an image when you attempt to downgrade the device from Junos OS Release 12.1 to Release 11.4. You must download and install the signature database once again.

  If you upgrade the device from Junos OS Release 11.4 to Release 12.1, application identification signature will take about 30 seconds to recompile. During these 30 seconds, application identification does not identify the traffic, and traffic is dropped by the application firewall as an unknown session. [PR/689304]

- On SRX550 devices, U-boot upgrade is currently not supported in the beta build. Customers are advised not to upgrade u-boot even if a different version is available. [PR/731819]

Virtual Private Network (VPN)

- On all branch SRX Series and J Series devices, site-to-site policy based VPN in three or more zones scenarios will not work if the policy matches the address "any" instead of specific addresses and all cross-zone traffic policies point to the single site-to-site VPN tunnel. As a workaround, configure address books in different zones to match the source and destination, and use the address book name in the policy to match the source and destination. [PR/441967]

Related Documentation

- New Features in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 37
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 46
- Known Limitations in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 48
- Resolved Issues in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 76
- Errata and Changes in Documentation for Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 85
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 89

Resolved Issues in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers

The following are the issues that have been resolved since Junos OS Release 12.1 for Juniper Networks branch SRX Series Services Gateways and J Series Services Routers. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

Application Layer Gateways (ALGs)

- On SRX650 devices, when receiving frames with TCP data that had been split between multiple packets, flowd placed these into multiple internal buffers. [PR/676431: This issue has been resolved.]

Authentication

- On all branch SRX Series devices, firewall authentication supported a maximum of 64 users or groups in policy “client-match”. [PR/661587: This issue has been resolved.]
- On SRX210 devices, when pass-through authentication was configured, the initial telnet session was closed with the reason "synproxy failure" instead of "TCP FIN". Subsequent sessions were closed with a correct reason. [PR/680048: This issue has been resolved.]

AX411

- On SRX210 devices, after several days the traffic no longer flowed through radio 2. [PR/579520: This issue has been resolved.]

Chassis Cluster

- On SRX100 and J2320 devices in a chassis cluster, after you configured link-speed for the **reth** interface, the **reth** interface went down and stayed down even after you deleted the configuration. [PR/466409: This issue has been resolved.]
- On SRX650 devices, the antivirus feature caused forwarding slowness at traffic peaks. [PR/610336: This issue has been resolved.]
- On SRX Series devices operating in chassis cluster mode, the xml response to the RPC validate command did not return the closing </routing-engine> tag for the second node. [PR/679413: This issue has been resolved.]
- On SRX650 devices, for switching deployment in chassis cluster, multicast traffic would duplicate. [PR/689153: This issue has been resolved.]
- On SRX240 devices, switching did not work. [PR/701539: This issue has been resolved.]

Command-line Interface (CLI)

- On SRX Series devices, deleting the groups at certain hierarchy level could erase **junos-defaults** groups. [PR/689912: This issue has been resolved.]
- On all branch SRX and J Series devices, in operation mode, the description information for screens could not be shown. [PR/712242: This issue has been resolved.]

Dynamic Host Configuration Protocol (DHCP)

- On SRX210 and SRX240 devices, when autoinstallation was configured to run on a particular interface and the default static route was set with the options discard, retain, and no-advertise, the DHCP client running on the interface tried to fetch the configuration files from the TFTP server. During this process, the UDP data port on the

TFTP server were unreachable. Because the TFTP server was unreachable, the autoinstallation process remained in the configuration acquisition state. When autoinstallation was disabled, the TFTP failed. [PR/454189: This issue has been resolved.]

- On SRX210 devices, memory leak occurred in the DHCP client module when the IP address was renewed. This leak was noticed by monitoring memory usage of the dhcpd process. [PR/504471: This issue has been resolved.]
- On SRX210 devices, DHCP packets passed and were not detected as spoofed packets. [PR/681998: This issue has been resolved.]

Flow and Processing

- On SRX210 devices, the packet size of the remote end ping was less than 1480 because the packets were getting dropped on the **at** interface. The default MTU on **at** interface is 1496 and the default MTU of the remote host Ethernet interface is 1514. [PR/469651: This issue has been resolved.]
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices in chassis cluster mode, a powered device connected to both nodes rebooted when there was RG0 failure. This was due to power interruption. [PR/574899: This issue has been resolved.]
- On J4350 devices, the external ICMP redirect packets were dropped. [PR/587948: This issue has been resolved.]
- On SRX210, SRX240, and J6350 devices, OSPF got stuck at the init state over the E1/T1 link when interface configurations were continuously changed. [PR/660264: This issue has been resolved.]
- On SRX240 and J2320 devices, when the LDP-based signaling was used for VPLS neighbor discovery, a restart of routing was required for the LDP-based signaling to work properly (after the configuration was committed). [PR/668555: This issue has been resolved.]
- On SRX220 devices, the throughput dropped to 20 Mbps on a 100 Mbps interface (only in Gigabit Ethernet-to-100 Mbps direction) when a bi-directional traffic was sent between Gigabit Ethernet interface and 100 Mbps interface. [PR/671248: This issue has been resolved.]
- On SRX650 devices, when Layer 2 LAG (4 x 1 Gbps) was configured, traffic was limited to 1 Gbps. [PR/677656: This issue has been resolved.]
- On all branch SRX Series devices, in PPPoE over reth, when the PPPoE session was already established, one node was rebooted, and the underlying **reth** interface would fail over to the newly rebooted node. Multicast traffic did not go through. [PR/678755: This issue has been resolved.]
- On J Series devices, when a certain number of **lt-0/0/0** logical units were configured with encapsulation VLAN, all **lt** logical interfaces were not activated. This was due to a problem with default system interface MAC allocation. [PR/680885: This issue has been resolved.]

- On all branch SRX Series devices, when multicast traffic passed through **pp0 ifl** and its underlying interface was reth, and when you added or deleted a reth member link, multicast route next hops were not updated. [PR/687652: This issue has been resolved.]
- On SRX650 devices, built in ports are not counting the FCS error statistics. [PR/690726: This issue has been resolved.]
- On SRX240 and SRX550 devices, the socket cleanup was not handled properly and caused rtlogd (security log daemon). [PR/691867: This issue has been resolved.]
- On SRX110 devices, the system boot time was high if a usb key was plugged in. [PR/695831: This issue has been resolved.]
- On SRX210 devices, Packet Forwarding Engine core files were observed periodically. [PR/697032: This issue has been resolved.]
- On all branch SRX Series devices, a memory leak occurred during audit event processing. [PR/698907: This issue has been resolved.]
- On all branch SRX Series and J Series devices, the PIM register messages were dropped on the physical interfaces that hosted multiple unnumbered interfaces. [PR/698943: This issue has been resolved.]
- On SRX220 devices, IP monitoring did not remove more than 1 route. [PR/699072: This issue has been resolved.]
- On SRX650 devices, the policer was not policing the configured rates at higher bandwidths. [PR/703003: This issue has been resolved.]
- On SRX240 devices, when you downgraded from Junos Release 11.4 or a later image to Junos Release 11.1 or an earlier image, the security package was deleted. Although it was automatically installed when the IDP daemon came up, the automatic installation failed sometimes due to application identification (AI) installation error. [PR/705113: This issue has been resolved.]
- On SRX210, SRX220, and SRX240 devices, the DSL line started renegotiation with DSLAM when you configured MTU on VDSL interface in VDSL mode. After configuring MTU on VDSL interface, the line took time to train with DSLAM and to come up. [PR/706795: This issue has been resolved.]
- On SRX240, SRX5600, and SRX5800 devices, using ftp to st0 interface for data transfer fails occasionally. [PR/706827: This issue has been resolved.]

Hardware

- On SRX100, SRX110, and SRX210 devices, when you powered on or rebooted the device, the Subscriber Identity Module (SIM) was locked. If the SIM Personal Identification Number (PIN) or the unlock code was configured in the **set interfaces cl-0/0/8 cellular-options gsm-options sim-unlock-code configuration** command, then Junos OS made an attempt to unlock the SIM only once. This was to keep the SIM from being blocked. If the SIM was blocked, you had to provide a PIN Unblocking Key (PUK) obtained from the service provider. If the wrong SIM PIN was configured, the SIM remained locked, and the administrator unlocked it by using the remaining two attempts. [PR/711812: This issue has been resolved.]

Interfaces and Routing

- On SRX240 devices, Junos XML Management protocol RPC parsing failed for configuration groups with wildcard output created with "show | display xml". It contained “<name><*></name>", which the parser could not understand. [PR/683682: This issue has been resolved.]
- On all branch SRX and J Series devices, when the peers were connected directly through the T1 link and Ge links, the ping operation to the peer link local address of the T1 link interface did not go through the T1 link; instead it was through the Ge link. [PR/684159: This issue has been resolved.]
- On SRX210 devices, the G.SHDSL line did not appear when CPE was configured with annex-auto in 2-wire or 4-wire mode with ADTRAN DSLAM, and in 2-wire mode with Cisco DSLAM. [PR/686617: This issue has been resolved.]
- On SRX210 and SRX220 devices, plugging off a cable to an interface disabled the interface at the driver level and the interface never linked up. [PR/694484: This issue has been resolved.]
- On all branch SRX Series devices, idle-timeout configuration did not work. [PR/696617: This issue has been resolved.]

Intrusion Detection and Prevention (IDP)

- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, custom attacks were not getting detected if there was no IDP signature database license available. [PR/710147: This issue has been resolved.]

Installation

- On SRX210 devices, the Image upgrade using the validate option failed when NTP name resolution failed. [PR/692594: This issue has been resolved.]

J-Web

- On all branch SRX Series devices, the wrong page showed up while editing ppd0 and ppe0 pages. [PR/660575: This issue has been resolved.]
- On SRX Series devices, after performing any configuration change in the CLI or J-Web, the pending commit pop-up window did not appear in J-Web interface. [PR/670459: This issue has been resolved.]
- On all branch SRX Series devices, on the configure > interface page, the edit SHDSL interface pop-up window was blank. [PR/671487: This issue has been resolved.]
- On all branch SRX Series devices, PPPoE wizard support was not available when the device was operating in a chassis cluster. [PR/681117: This issue has been resolved.]
- On SRX650 devices, PPPoE wizard support was not available for the 2-Port 10-Gigabit Ethernet XPIM. [PR/681224: This issue has been resolved.]
- On SRX100 devices, editing a physical interface (fe-x/x/x) on the Interfaces > Ports page required the availability of a configured MAC address. [PR/682012: This issue has been resolved.]
- On SRX240 devices, an error message was displayed when users committed DNAT pool configuration with an IP address of 0.0.0.0/0 even though the commit executed successfully. [PR/682915: This issue has been resolved.]
- On all branch SRX Series and J Series devices, deleting the configuration using the Configure>CLI Tools>Point and Click option resulted in session expiration. [PR/684532: This issue has been resolved.]
- On all branch SRX Series devices, field validation for IP network address was missing in the PPPoE wizard, which resulted in commit errors. [PR/684663: This issue has been resolved.]
- On all branch SRX Series devices, context-sensitive Help had formatting problems with use of the PPPoE wizard. [PR/686090: This issue has been resolved.]
- On all branch SRX Series devices, the 'Assign to Zone' option in the zone page of PPPoE wizard was not mapping the actual zone configured in the router. [PR/686843: This issue has been resolved.]
- On SRX110 devices using the Internet Explorer browser, configuring the Global option using Configure > UTM > Anti-virus was not supported. [PR/688890: This issue has been resolved.]

- On SRX210, SRX220, SRX240, and SRX650 devices, when you discarded any available MIB profile, file or predefined object from accounting-options on the Point and Click CLI Configuration page (Configure > CLI Tools > Point and Click CLI), the J-Web session timed out. [PR/689261: This issue has been resolved.]
- On SRX110 devices, the J-Web interface did not work on the SRX110H-VB models. [PR/689614: This issue has been resolved.]
- On SRX100, SRX210, SRX220, and SRX240 devices, the dashboard links were not pointing to the correct tabs in J-Web. When links were open in J-Web, they navigated only up to the top tabs. Ex: If link "sessions" in "security resource" panel was clicked, it navigated only to top "monitor tab". [PR/689682: This issue has been resolved.]
- On all branch SRX Series devices, while creating a PPPoE connection, the wizard failed to create a security policy with a new zone. Without the security policy, the traffic did not flow through the PPPoE interface. [PR/689731: This issue has been resolved.]
- On SRX550 devices, Enhanced Web Filtering (EWF) was not supported. [PR/690446: This issue has been resolved.]
- On all branch SRX Series devices, when you configured an AX411 Wireless LAN Access Point using Configure >Wireless LAN > Setting, you could not set Bolivia as a country. [PR/691824: This issue has been resolved.]
- On all branch SRX Series devices, upgrading access points using J-Web (Configure > Wireless LAN > Firmware Upgrade) did not work. [PR/694627: This issue has been resolved.]
- On all branch SRX Series devices, the value "Privacy settings" of the "Neighboring Access Points" were not listed in the Wireless LAN Monitor page (J-Web >Monitor >Wireless LAN >Neighboring Access Points). [PR/697360: This issue has been resolved.]
- On all branch SRX Series devices, after a software upgrade of the device, when users committed the configuration changes using the Configure > Wireless Lan > Settings page, the following message was displayed: “warning: requires 'ax411-wlan-ap' license”. [PR/697531: This issue has been resolved.]
- On all branch SRX Series devices, when users edited an uncommitted PPPoE connection that had a zone without a firewall policy, the J-Web page blocked the zone page of the PPPoE wizard, and a warning was displayed. [PR/697891: This issue has been resolved.]
- On SRX100 and SRX110 devices, VLAN assignment was not supported under Configure > security > 802.1x > Exclusion list. [PR/698929: This issue has been resolved.]
- On SRX110 devices, when users edited physical interfaces, the OK button in the dialog box did not work. [PR/700501: This issue has been resolved.]
- On all branch SRX Series devices, in Internet Explorer, the dashboard panels did not show any data until they were refreshed. [PR/703958]
- On SRX110 devices, the Chassis View was not visible on the Dashboard page. [PR/717743: This issue has been resolved.]
- On all branch SRX Series devices, the CPU data graph was not working. [PR/719042: This issue has been resolved.]

- On all branch SRX Series devices in a chassis cluster, the primary node did not show security resources details on the **Dashboard** page and the message log "Security Resources:error: invalid value: firewall-policies" was generated. [PR/720435: This issue has been resolved.]
- On SRX100, SRX210, SRX220, SRX240, and SRX650 devices, after configuring the interface speed and duplex on J-Web interface, the page showed the speed and duplex values as following:
  - Speed:10Mbps/100Mbps/1Gbps
  - Duplex:Full Duplex/Half Duplex

  When you go to another page and come back to this page again, the display changed as following:
  - Speed:10m/100m/1g
  - Duplex:full duplex/half duplex

  [PR/721679: This issue has been resolved.]
- On SRX210 devices, when the CLI option to delete a DHCP pool was used, the J-Web interface Monitor page (Monitor > Services > DHCP > Pools) did not display the correct value in the "Excluded address" field. It displayed the text "[objec object]" in the table. [PR/723555: This issue has been resolved.]
- On all branch SRX Series devices, changes to URL category value caused value deletion in the Web-filtering profile. [PR/723884: This issue has been resolved.]
- On all branch SRX Series devices, the Application Tracking monitor page displayed a blank table instead of a warning message, when there was no data to display. [PR/724985: This issue has been resolved.]

Network Address Translation (NAT)

- On SRX650 devices, when you configured source NAT with PAT and a static NAT prefix and generate an FTP connection from the IPv4 FTP client to the IPv6 address of the device, the source NAT rule was not applied to the FTP data session, and the source address of the data session was not translated correctly. [PR/558460: This issue has been resolved.]
- On SRX240 devices, while processing an interface state change, nsd encountered an error and printed a log message indicating the error type and the interface in question. However, it was not able to handle that error condition properly and followed a null pointer. This led to a crash and a core file being generated. [PR/687465: This issue has been resolved.]
- On SRX240 devices, using the **show security nat source persistent-nat-table all family inet6** command resulted in display error and MGD core dump. [PR/711541: This issue has been resolved.

Switching

- On SRX210 devices, the switch fabric did not work when configured on the ge-0/0/0 and ge-0/0/1 interfaces. [PR/694631: This issue has been resolved.]

Unified Threat Management (UTM)

- On SRX650 devices, there was drop in UTM EAV throughput performance. [PR/583630: This issue has been resolved.]
- On SRX650 devices, a commit error occurred when the policy used UTM "application-services'warning: license not installed for". This was only a display issue. [PR/600941: This issue has been resolved.]
- On SRX220 devices, the maximum number of connections per second supported by the Enhanced Web Filtering solution was less than that supported by the Surf Control solution. [PR/609094: This issue has been resolved.]
- On all branch SRX Series devices, performance drop was observed. [PR/671777: This issue has been resolved.]
- On SRX240 and SRX650 devices, the resident set size memory of the UTM daemon increased during host-inbound traffic when the UTM feature was configured. [PR/675114: This issue has been resolved.]
- On SRX550 devices, USB Modem was not supported. [PR/678657: This issue has been resolved.]
- On all branch SRX Series devices, while configuring UTM on J-Web interface, validation went to an infinite loop when the engine type was not chosen in Anti Virus > Global options. Also, configuring and then clicking on the OK button in global options in Configure>UTM> Anti Spam page resulted in inaccessibility of the J-Web. [PR/683649: This issue has been resolved.]
- On all branch SRX Series devices, when users configured UTM features, using the Configure > UTM > web filtering > global options page, the interface button did not work. Also, the custom objects page on UTM, sometimes rejected certain values while configuring the URL category name. [PR/685534: This issue has been resolved.]
- On SRX210 PoE devices, whenever the SMTP client issued a pipeline command, it caused errors in tagging spam e-mails. [PR/696109: This issue has been resolved.]
- On SRX550 devices, UTM EWF functionality was not supported. [PR/733527: This issue has been resolved.]

Virtual Private Network (VPN)

- On SRX100 devices, the SCEP enrollment request to non-Microsoft CA was rejected due to an invalid RSA signature. [PR/567846: This issue has been resolved.]
- On SRX220 devices with IPsec route-based VPN configured, ST interface input counters did not increment. The traffic worked fine over the VPN, but it was not counted in the interface statistics. [PR/672738: This issue has been resolved.]

- On SRX240 devices, the packets containing more than 1667 bytes passing through the Layer3 VPN on the st0 interface failed. [PR/681057: This issue has been resolved.]

Related Documentation

- New Features in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 37
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 46
- Known Limitations in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 48
- Outstanding Issues in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 71
- Errata and Changes in Documentation for Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 85
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 89

Errata and Changes in Documentation for Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers

Errata for the Junos OS Software Documentation

This section lists outstanding issues with the software documentation.

J Series Services Router Advanced WAN Access Configuration Guide

- The example given in the “Configuring Full-Cone NAT” section in the guide available at http://www.juniper.net/techpubs/software/jseries/junos85/index.html is incorrect. The correct and updated example is given in the revised guide available at http://www.juniper.net/techpubs/software/jseries/junos90) .

J2320, J2350, J4350, and J6350 Services Router Getting Started Guide

- The “Connecting to the CLI Locally” section states that the required adapter type is DB-9 female to DB-25 male. This is incorrect; the correct adapter type is DB-9 male to DB-25 male.

J-Web

- **J-Web Security Package Update Help page**—This Help page does not contain information about the download status.
- **J-Web pages for stateless firewall filters**—There is no documentation describing the J-Web pages for stateless firewall filters. To find these pages in J-Web, go to **Configure>Security>Firewall Filters**, and then select **IPv4 Firewall Filters** or **IPv6 Firewall Filters**. After configuring the filters, select **Assign to Interfaces** to assign your configured filters to interfaces.
- **J-Web configuration Instructions**— Because of ongoing J-Web interface enhancements, some of the J-Web configuration example instructions in the Junos administration and

configuration guides became obsolete and thus were removed. For examples that are missing J-Web instructions, use the provided CLI instructions.

Junos OS Security Configuration Guide

- This guide incorrectly states that Release 12.1 supports security chains, which validate a certificate path upward through eight levels of CA authorities in the PKI hierarchy. Release 12.1 does not support security chains.

Junos OS WLAN Configuration and Administration Guide

- This guide is missing information that the AX411 Access Point can be managed from SRX100 and SRX110 devices.
- This guide is missing the information that on all branch SRX devices, managing AX411 WLAN Access Points through an Layer 3 Aggregated Ethernet (ae) interface is not supported.

Errata for the Junos OS Hardware Documentation

This section lists outstanding issues with the hardware documentation.

AX411 Access Point Hardware Guide

- This guide incorrectly documents the maximum number of supported access points on the SRX Series devices. It should state that on the SRX210, SRX240, and SRX650 devices, you can configure and manage up to four access points (maximum).
- This guide is missing information that the AX411 Access Point can be managed from SRX100 and SRX110 devices.

J Series Services Routers Hardware Guide

- The procedure “Installing a DRAM Module” omits the following condition:

  All DRAM modules installed in the router must be the same size (in megabytes), type, and manufacturer. The router might not work properly when DRAM modules of different sizes, types, or manufacturer are installed.
- This guide incorrectly states that only the J2350 Services Router complies with Network Equipment Building System (NEBS) criteria. It should state that the J2350, J4350, and J6350 routers comply with NEBS criteria.
- This guide is missing information about 100Base-LX connector support for 1-port and 6-port Gigabit Ethernet uPIMs.

SRX Series Services Gateways for the Branch Physical Interface Modules Hardware Guide

- In the "SRX Series Services Gateway Interfaces Power and Heat Requirements" section, the PIM Power Consumption Values table contains the power consumption value for the 1-port Gigabit Ethernet Small Form-Factor Pluggable (SFP) Mini-PIM value as 3:18 W.

  The correct power consumption value for the 1-port Gigabit Ethernet Small Form-Factor Pluggable (SFP) Mini-PIM is 4:4 W.

SRX100 Services Gateway Hardware Guide

- In the "Connecting an SRX100 Services Gateway to the J-Web Interface" section, the following information is missing in the note:

  NOTE: Microsoft Internet Explorer version 6.0 is also supported as backward compatible from Microsoft Internet Explorer version 7.0.

SRX210 Services Gateway Hardware Guide

- In the "Connecting an SRX210 Services Gateway to the J-Web Interface" section, the following information is missing in the note:

  NOTE: Microsoft Internet Explorer version 6.0 is also supported as backward compatible from Microsoft Internet Explorer version 7.0.

SRX240 Services Gateway Hardware Guide

- In the "Connecting the SRX240 Services Gateway to the J-Web Interface" section, the following information is missing in the note:

  NOTE: Microsoft Internet Explorer version 6.0 is also supported as backward compatible from Microsoft Internet Explorer version 7.0.

SRX550 Services Gateway Hardware Guide

- This guide incorrectly states that the GPIMs are hot-swappable. The document should state that GPIMs are not hot-swappable on SRX550 Services Gateway.

SRX210 Services Gateway 3G ExpressCard Quick Start

- Several tasks are listed in the wrong order. "Task 6: Connect the External Antenna" should appear before "Task 3: Check the 3G ExpressCard Status," because the user needs to connect the antenna before checking the status of the 3G ExpressCard. The correct order of the tasks is as follows:

1. Install the 3G ExpressCard
2. Connect the External Antenna
3. Check the 3G ExpressCard Status
4. Configure the 3G ExpressCard
5. Activate the 3G ExpressCard Options

- In "Task 6: Connect the External Antenna," the following sentence is incorrect and redundant: "The antenna has a magnetic mount, so it must be placed far away from radio frequency noise sources including network components."
- In the "Frequently Asked Questions" section, the answer to the following question contains an inaccurate and redundant statement:

  Q: Is an antenna required? How much does it cost?

  A: The required antenna is packaged with the ExpressCard in the SRX210 Services Gateway 3G ExpressCard kit at no additional charge. The antenna will have a magnetic mount with ceiling and wall mount kits within the package.

  In the answer, the sentence "The antenna will have a magnetic mount with ceiling and wall mount kits within the package" is incorrect and redundant.

SRX210 Services Gateway Quick Start Guide

- The section on installing software packages is missing the following information:

  On SRX210 devices, the **/var** hierarchy is hosted in a separate partition (instead of the *root* partition). If Junos OS installation fails as a result of insufficient space:

  1. Use the **request system storage cleanup** command to delete temporary files.
  2. Delete any user-created files both in the *root* partition and under the **/var** hierarchy.

Related Documentation

- New Features in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 37
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 46
- Known Limitations in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 48
- Outstanding Issues in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 71
- Resolved Issues in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 76
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 89

Upgrade and Downgrade Instructions for Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers

In order to upgrade to Junos OS Release 12.1 or later, your device must be running one of the following Junos OS Releases:

- 9.1S1
- 9.2R4
- 9.3R3
- 9.4R3
- 9.5R1 or later

If your device is running an earlier release, upgrade to one of these releases and then to the 12.1 release. For example, to upgrade from Release 9.2R1, first upgrade to Release 9.2R4 and then to Release 12.1.

For additional upgrade and download information, see the *Junos OS Initial Configuration Guide for Security Devices* and the *Junos OS Migration Guide*.

- Upgrade and Downgrade Scripts for Address Book Configuration on page 89
- Hardware Requirements for Junos OS Release 12.1 for SRX Series Services Gateways and J Series Services Routers on page 92

Upgrade and Downgrade Scripts for Address Book Configuration

Beginning with Junos OS Release 12.1, you can configure address books under the **[security]** hierarchy and attach security zones to them (zone-attached configuration). In Junos OS Release 11.1 and earlier, address books were defined under the **[security zones]** hierarchy (zone-defined configuration).

You can either define all address books under the **[security]** hierarchy in a zone-attached configuration format or under the **[security zones]** hierarchy in a zone-defined configuration format; the CLI displays an error and fails to commit the configuration if you configure both configuration formats on one system.

Juniper Networks provides Junos operation scripts that allow you to work in either of the address book configuration formats (see Figure 1 on page 91).

- About Upgrade and Downgrade Scripts on page 89
- Running Upgrade and Downgrade Scripts on page 91
- Upgrade and Downgrade Support Policy for Junos OS Releases on page 92

About Upgrade and Downgrade Scripts

After downloading Junos OS Release 12.1, you have the following options for configuring the address book feature:

- **Use the default address book configuration**—You can configure address books using the zone-defined configuration format, which is available by default. For information

on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

- **Use the upgrade script**—You can run the upgrade script available on the Juniper Networks support site to configure address books using the new zone-attached configuration format. When upgrading, the system uses the zone names to create address books. For example, addresses in the trust zone are created in an address book named **trust-address-book** and are attached to the trust zone. IP prefixes used in NAT rules remain unaffected.

  After upgrading to the zone-attached address book configuration:

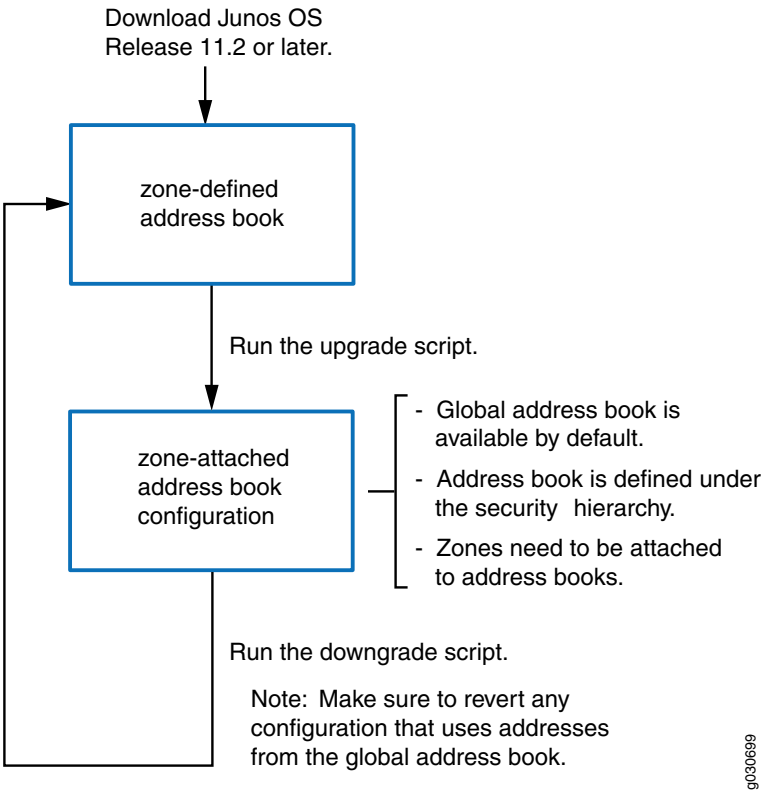
  - You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.
  - You cannot configure address books using the J-Web interface.

  For information on how to configure zone-attached address books, see the Junos OS Release 12.1 documentation.

- **Use the downgrade script**—After upgrading to the zone-attached configuration, if you want to revert to the zone-defined configuration, use the downgrade script available on the Juniper Networks support site. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

NOTE: Before running the downgrade script, make sure to revert any configuration that uses addresses from the global address book.

Figure 1: Upgrade and Downgrade Scripts for Address Books



Running Upgrade and Downgrade Scripts

The following restrictions apply to the address book upgrade and downgrade scripts:

- The scripts cannot run unless the configuration on your system has been committed. Thus, if the zone-defined address book and zone-attached address book configurations are present on your system at the same time, the scripts will not run.
- The scripts cannot run when the global address book exists on your system.
- If you upgrade your device to Junos OS Release 12.1 and configure logical systems, the master logical system retains any previously-configured zone-defined address book configuration. The master administrator can run the address book upgrade script to convert the existing zone-defined configuration to the zone-attached configuration. The upgrade script converts all zone-defined configurations in the master logical system and user logical systems.

NOTE: You cannot run the downgrade script on logical systems.

For information about implementing and executing Junos operation scripts, see the *Junos OS Configuration and Operations Automation 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 10.0, 10.4, and 11.4 are EEOL releases. You can upgrade from Junos OS Release 10.0 to Release 10.4 or even from Junos OS Release 10.0 to Release 11.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind. For example, you cannot directly upgrade from Junos OS Release 10.3 (a non-EEOL release) to Junos OS Release 11.4 or directly downgrade from Junos OS Release 11.4 to Junos OS Release 10.3.

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 http://www.juniper.net/support/eol/junos.html .

Hardware Requirements for Junos OS Release 12.1 for SRX Series Services Gateways and J Series Services Routers

Transceiver Compatibility for SRX Series and J Series Devices

We strongly recommend that only transceivers provided by Juniper Networks be used on SRX Series and J Series interface modules. Different transceiver types (long-range, short-range, copper, and others) can be used together on multiport SFP interface modules as long as they are provided by Juniper Networks. We cannot guarantee that the interface module will operate correctly if third-party transceivers are used.

Please contact Juniper Networks for the correct transceiver part number for your device.

Power and Heat Dissipation Requirements for J Series PIMs

On J Series Services Routers, the system monitors the PIMs and verifies that the PIMs fall within the power and heat dissipation capacity of the chassis. If power management is enabled and the capacity is exceeded, the system prevents one or more of the PIMs from becoming active.

CAUTION: Disabling the power management can result in hardware damage if you overload the chassis capacities.

You can also use CLI commands to choose which PIMs are disabled. For details about calculating the power and heat dissipation capacity of each PIM and for troubleshooting procedures, see the *J Series Services Routers Hardware Guide*.

Supported Third-Party Hardware

The following third-party hardware is supported for use with J Series Services Routers running Junos OS.

- **USB Modem**

  We recommend using a U.S. Robotics USB 56K V.92 Modem, model number USR 5637.

- **Storage Devices**

  The USB slots on J Series Services Routers accept a USB storage device or USB storage device adapter with a CompactFlash card installed, as defined in the *CompactFlash Specification* published by the CompactFlash Association. When the USB device is installed and configured, it automatically acts as a secondary boot device if the primary CompactFlash card fails on startup. Depending on the size of the USB storage device, you can also configure it to receive any core files generated during a router failure. The USB device must have a storage capacity of at least 256 MB.

  Table 6 on page 93 lists the USB and CompactFlash card devices supported for use with the J Series Services Routers.

Table 6: Supported Storage Devices on the J Series Services Routers

Manufacturer	Storage Capacity	Third-Party Part Number
SanDisk—Cruzer Mini 2.0	256 MB	SDCZ2-256-A10
SanDisk	512 MB	SDCZ3-512-A10
SanDisk	1024 MB	SDCZ7-1024-A10
Kingston	512 MB	DTI/512KR
Kingston	1024 MB	DTI/1GBKR
SanDisk—ImageMate USB 2.0 Reader/Writer for CompactFlash Type I and II	N/A	SDDR-91-A15
SanDisk CompactFlash	512 MB	SDCFB-512-455
SanDisk CompactFlash	1 GB	SDCFB-1000.A10

J Series CompactFlash and Memory Requirements

Table 7 on page 94 lists the CompactFlash card and DRAM requirements for J Series Services Routers.

Table 7: J Series CompactFlash Card and DRAM Requirements

Model	Minimum CompactFlash Card Required	Minimum DRAM Required	Maximum DRAM Supported
J2320	1 GB	1 GB	1 GB
J2350	1 GB	1 GB	1 GB
J4350	1 GB	1 GB	2 GB
J6350	1 GB	1 GB	2 GB

Related Documentation

- New Features in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 37
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 46
- Known Limitations in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 48
- Outstanding Issues in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 71
- Resolved Issues in Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 76
- Errata and Changes in Documentation for Junos OS Release 12.1 for Branch SRX Series Services Gateways and J Series Services Routers on page 85

Junos OS Release Notes for High-End SRX Series Services Gateways

Powered by Junos OS, Juniper Networks high-end SRX Series Services Gateways provide robust networking and security services. High-end SRX Series Services Gateways are designed to secure enterprise infrastructure, data centers, and server farms. The high-end SRX Series Services Gateways include the SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices.

New Features in Junos OS Release 12.1 for High-End SRX Series Services Gateways

The following features have been added to Junos OS Release 12.1. Following the description is the title of the manual or manuals to consult for further information.

NOTE: **For the latest updates about support and issues on Junos Pulse, see the** Junos Pulse Release Notes **.**

Software Features

AppSecure

- **Hit-count tracking**—This feature is supported on all high-end SRX Series devices.

  The new **show security policies hit-count** command displays the utility rate of security policies according to the number of hits they receive. You can use this feature to determine which policies are being used on the device, and how frequently they are used. Depending on the command options that you choose, the number of hits can be listed without order or sorted in either ascending or descending order, and they can be restricted to the number of hits that fall above or below a specific count or within a range. Data is shown for all zones associated with the policies or named zones.

  [*Junos OS CLI Reference*, *Junos OS Security Configuration Guide*]

- **Security enhancement between a Junos Pulse Access Control Service and an Infranet Enforcer**—This feature is supported on all high-end SRX Series devices with UAC enabled.

  To improve security for a UAC configuration, a message appears if the Junos Pulse Access Control Service's certificate cannot be verified on the SRX Series device. To ensure that the Access Control Service and the Enforcer are connected securely, configure the ca-profile on the SRX Series device to verify the Access Control Service's certificate.

  [*Security Configuration Guide*]

- **User role integration into AppTrack logs**—This feature is supported on all high-end SRX Series devices.

  User identity details such as user name and user role have been added to the AppTrack session create, session close, and volume update logs. These fields will contain the user name and role associated with the policy match. The logging of username and roles are enabled only for security policies that provide UAC enforcement. For security policies without UAC enforcement, the username and roles is displayed as N/A. The user name is displayed as unauthenticated-user and user role is displayed as N/A, if the device cannot retrieve information for that session because there is no authentication table entry for that session or because logging of this information is disabled. The user-role field in the log will contain the list of all the roles performed by the user if match criteria is specific, authenticated-user, or any and the user name field in the log contains the correct username. The user-role field in the log will contain N/A if the match criteria and the username field in the log contains un-authenticated user or unknown user.

  [*Junos OS Security Configuration Guide*]

Chassis Cluster

- **Logical interfaces on redundant Ethernet interface scaling**—This feature is supported on all high-end SRX Series devices.

  The total number of logical interfaces that you can configure across all the redundant Ethernet (reth) interfaces in a chassis cluster deployment has been increased to 4096.

  [*Junos OS Security Configuration Guide*]

Class of Service

- **High-priority queue on SPC**—This feature is supported on all high-end SRX Series devices.

  Junos OS Release 12.1 provides a configuration option to enable packets with specific Differentiated Services (DiffServ) code points (DSCP) precedence bits to enter a high-priority queue on the Services Processing Card (SPC) on high-end SRX Series devices. The Services Processing Unit (SPU) draws packets from the high-priority queue and only draws packets from the low-priority queue when the high-priority queue is empty. This feature can reduce overall latency for real-time traffic, such as voice traffic.

  To designate packets for the high-priority or low-priority queues, use the **spu-priority** configuration statement at the [**edit class-of-service forwarding-classes *class***] hierarchy level. A value of **high** places packets into the high-priority queue, and a value of **low** places packets into the low-priority queue.

  [*Junos OS Class of Service Configuration Guide for Security Devices*]

Denial of Service (DoS)

- **Whitelists**—This feature is supported on all high-end SRX Series devices.

  You can configure a whitelist of IP addresses that are to be exempt from the SYN cookie and SYN proxy mechanisms that occur during the SYN flood screen protection process. To do so, use the new **white-list** statement at the [**edit security screen ids-option screen-name tcp syn-flood**] hierarchy level.

  Both IP version 4 (IPv4) and IP version 6 (IPv6) whitelists are supported. Addresses in a whitelist must be all IPv4 or all IPv6. Each whitelist can have up to 32 IP address prefixes.

  [*Junos OS CLI Reference*, *Junos OS Security Configuration Guide*]

General Packet Radio Service (GPRS)

- **Customized IE removal**—This feature is supported on all high-end SRX Series devices.

  You can now configure the GPRS tunneling protocol (GTP) firewall to remove specific information elements (IE) using the user-configured IE number. When you configure the IE-removal, the GTP firewall deletes the corresponding IEs of the GTPv1 messages; updates the length of the GTP, the UDP, and the IP; and then passes the GTPv1 message. The GTP firewall also updates the cyclic redundancy check (CRC) code.

  [*Junos OS CLI Reference*,*Junos OS Security Configuration Guide*]

Intrusion Detection and Prevention (IDP) and AppSecure

- **Synchronizing application identification package in a chassis cluster**—This feature is supported on all high-end SRX Series devices.

  The existing application identification package download feature is modified to download the security package on the primary node and synchronize it on the secondary node.

  When you download the application signature package on a device operating in chassis cluster mode, this feature enables you to download and install the package to the primary node, after which the primary and secondary nodes are automatically synchronized. This synchronization helps maintain the same version of the security package on both the primary node and the secondary node.

  You can use the command **request services application-identification download** to download the application identification package to the primary node and use the command **request services application-identification download status** to verify the download status of the application package and the status of the synchronization to the secondary node.

  [*Junos OS Security Configuration Guide*]

- **Synchronizing IDP security package in a chassis cluster**—This feature is supported on all high-end SRX Series devices.

  The existing IDP security package download feature has been modified to download the security package on the primary node and synchronize it on secondary node.

  When you download the IDP security package on a device operating in chassis cluster mode, this feature enables you to download and install the IDP signature database to the primary node, after which the primary and secondary nodes are automatically synchronized. This synchronization helps maintain the same version of the security package on both the primary node and the secondary node.

  You can use the **request security idp security-package download** command to download the IDP signature database to the primary node.

  When you check the security package download status using the **request security idp security-package download status** command, a message is displayed confirming that the downloaded security package is being synchronized on the primary and secondary nodes.

  [*Junos OS Security Configuration Guide*]

J-Web

- **J-Web support for IPv6 stage 3 security features** —This feature is supported on all high-end SRX Series devices.

  The following J-Web pages have been added to support the IPv6 feature:

  - Proxy ND Configuration page
  - DS-Lite Configuration page

The following J-Web pages have been updated to include IPv6 support:

- Source NAT Pool Configuration page
- Static NAT Rule Configuration page
- Source NAT Rule Configuration page
- Destination NAT Pool Configuration page
- Destination NAT Rule Configuration page

[*Junos OS Security Configuration Guide*]

- **J-Web support for services offloading**—This feature is supported on all high-end SRX Series devices.

  Services offloading is a mechanism for processing fast-path packets in the network processor instead of in the Services Processing Unit (SPU). This method reduces the long packet processing latency that arises when packets are forwarded from network processors to SPUs for processing and back to I/O cards (IOCs) for transmission.

  This feature can now be enabled or disabled on a chassis through the J-Web user interface. You can use the Chassis configuration page in J-Web to enable or disable services offloading on a chassis.

  [*Junos OS Security Configuration Guide*]

Logical Systems

- **IPv6 addresses in logical systems**—This feature is supported on all high-end SRX Series devices.

  In Junos OS Release 12.1, IPv6 addresses can be configured in logical systems for the following features:

  - Firewall authentication
  - BGP routing

  [*Junos OS Logical Systems Configuration Guide for Security Devices*]

- **IPv6 dual-stack lite (DS-Lite)**—This feature is supported on all high-end SRX Series devices.

  DS-Lite allows migration to an IPv6 access network without changing end user software. IPv4 users can continue to access IPv4 Internet content using their current hardware, while IPv6 users are able to access IPv6 content. A DS-Lite softwire initiator at the customer edge encapsulates IPv4 packets into IPv6 packets while a softwire concentrator decapsulates the IPv4-in-IPv6 packets and also performs IPv4 NAT translations.

  The master administrator allocates the number of softwire initiators that can be configured in a logical system. The master administrator configures maximum and reserved values for the **dslite-softwire-initiator** configuration statement at the [**edit system security-profile *profile-name***] hierarchy level. The master administrator or user

logical system administrator can configure softwire concentrators at the [**edit security softwires**] hierarchy level.

[*Junos OS Logical Systems Configuration Guide for Security Devices*]

Routing

- **Equal-cost multipath (ECMP) flow-based forwarding**—This feature is supported on all high-end SRX Series devices.

  An equal-cost multipath (ECMP) set is formed when the routing table contains multiple next-hop addresses for the same destination with equal cost. (Routes of equal cost have the same preference and metric values.) If there is an ECMP set for the active route, the Junos OS software uses a hash algorithm to choose *one* of the next-hop addresses in the ECMP set to install in the forwarding table.

  You can configure Junos OS so that multiple next-hop entries in an ECMP set are installed in the forwarding table. On Juniper Networks devices, per-packet or per-flow load balancing can be performed to spread traffic across multiple paths between routing devices. On Juniper Networks security devices, source and destination IP addresses and protocols are examined to determine individual traffic flows. Packets for the same flow are forwarded on the same interface; the interface does not change when there are additions or changes to the ECMP set. This is important for features such as source NAT, where the translation is performed only during the first path of session establishment; IDP; ALG; and route-based VPN tunnels. If a packet arrives on a given interface in an ECMP set, the security device ensures that reverse traffic is forwarded through the same interface.

  NOTE: ECMP flow-based forwarding on security devices applies only to IPv4 unicast traffic flows. Multicast and IPv6 flows are not supported.

  In a chassis cluster deployment, a *local* interface is an interface that is on the same node as the interface on which a packet arrives, and a *remote* interface is an interface that is on the other chassis cluster node. If an ECMP route has both local and remote interfaces in a chassis cluster, then the local interface is favored for the next hop.

  To configure ECMP flow-based forwarding on Juniper Networks security devices, first define a load-balancing routing policy by including one or more **policy-statement** configuration statements at the [**edit policy-options**] hierarchy level, with the action **load-balance per-packet**. Then apply the routing policy to routes exported from the routing table to the forwarding table. To do this, include the **forwarding-table** and **export** configuration statements at the [**edit routing-options**] hierarchy level.

  [*Junos OS Routing Protocols and Policies Configuration Guide for Security Devices*]

SSL Proxy

- **SSL proxy**—This feature is supported on all high-end SRX Series devices.

  SSL proxy is a transparent proxy; that is, it performs SSL encryption and decryption between the client and the server, but neither the server nor the client can detect its presence. SSL offload and SSL inspection features require the servers to share their

secret keys to be able to decrypt the SSL traffic. However, sharing server keys is sometimes not feasible or might not be available in certain circumstances , in which case, the SSL traffic cannot be decrypted.

SSL proxy addresses this problem by ensuring that it has the keys to encrypt and decrypt the payload. Decryption and encryption take place in each direction (client and server), and the keys are different for both encryption and decryption.

- **Application firewall, IDP, and application tracking with SSL proxy**—With the implementation of SSL proxy, application ID can identify applications encrypted in SSL. SSL proxy can be enabled as an application service in a regular firewall policy rule. IDP, application firewall, and application tracking services can use the decrypted content from SSL proxy. On the SSL payload, IDP can inspect attacks and anomalies; for example, HTTP chunk length overflow on HTTPS. On encrypted applications, such as Facebook, application firewall can enforce policies and application tracking (when configured in the from and to zones) can report logging issues based on dynamic application and nested application.

NOTE: If none of the services (application firewall, IDP, or application tracking) are configured, then SSL proxy services are bypassed even if an SSL proxy profile is attached to a firewall policy.

User Role Firewalls

- **User role firewall providing flexibility and higher security**—This feature is supported on all high-end SRX Series devices.

  Network security enforcement, monitoring, and reporting based solely on IP information soon will not be sufficient for today's dynamic and mobile workforce. By integrating user firewall policies, administrators can permit or restrict network access of employees, contractors, partners, and other users based on the roles they are assigned.

  A new match criteria, source-identity, defines applicable roles for each policy. In this way, traffic can be permitted or denied access based on the role of the user, as well as the zone pair, source and destination IP addresses, and application.

  To enhance a user role firewall implementation, the SRX Series device can be configured to interact with a Junos Pulse Access Control Service, providing a source of dynamic user role information. The Access Control Service can also be configured as a relay between a third-party authentication server and the SRX Series device. In this configuration, SPNEGO and Kerberos protocols provide a single sign-on environment for dynamic role provisioning.

  [*Junos OS Security Configuration Guide*, *Unified Access Control Solution Guide for SRX Series Services Gateways*]

Related Documentation

- Outstanding Issues in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 117
- Resolved Issues in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 122

- Errata and Changes in Documentation for Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 130
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 102
- Known Limitations in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 105

Changes in Default Behavior and Syntax in Junos OS Release 12.1 for High-End SRX Series Services Gateways

The following current system behavior, configuration statement usage, and operational mode command usage might not yet be documented in the Junos OS documentation:

AppSecure Application Package Upgrade Changes

- On SRX1400, SRX3400, SRX3600, SRX5600, and SRX5800 devices, application tracking is enabled by default. You can disable application tracking with the **set security application-tracking disable** command. This command disables application tracking without deleting the zone configuration.
- **Application signatures removed after upgrading to Junos OS Release 11.4**—This change applies to all high-end SRX Series devices that use the application identification signature package.

  As of Junos OS Release 11.4, the application signature package is downloaded and installed in a separate database, not in the Junos OS configuration file as in previous Junos OS releases.

  When you upgrade an SRX Series device from Junos OS Release 11.2 to Junos OS Release 11.4 or later, any predefined application signatures and signature groups from the Junos OS Release 11.2 configuration will be removed when you install the latest predefined signatures and signature groups by using the **request services application-identification install** command. However, the upgrade will not remove custom signatures and signature groups from the Junos OS configuration.

  For information about using the **request services application-identification download** and **request services application-identification install** commands, see the *Junos OS CLI Reference*.

CLI

- The **client-match** *match-name* option under security hierarchy [**edit security policies from-zone** *zone-name* **to-zone** *zone-name* **policy** *policy-name* **then permit firewall-authentication**] now supports a maximum of 64 users or user groups in the policy.
- On all high-end SRX Series devices, the **show interface** *interface-name* **statistics detail** command was showing incorrect FCS statistics. Additional 4 bytes in the FCS were counted in input statistics but not counted in output statistics. Now the FCS is included in both input and output Ethernet statistics and the **show interface** *interface-name* **statistics detail** command displays correct output.

- On all high-end SRX Series devices, a new command the **clear security flow statistics**, has been introduced to clear the flow-related system statistics.

Deprecated Items for High-End SRX Series Services Gateways

Table 8 on page 103 lists deprecated items (such as CLI statements, commands, options, and interfaces).

CLI statements and commands are deprecated—rather than immediately removed—to provide backward compatibility and a chance to bring your configuration into compliance with the new configuration. We strongly recommend that you phase out deprecated items and replace them with supported alternatives.

Table 8: Items Deprecated in Release 12.1

Deprecated Item	Replacement	Hierarchy Level or Command Syntax	Additional Information
node	-	**request security idp security-package download**	On all high-end SRX Series devices operating in a chassis cluster, the following **request security idp security-package download** commands with the **node** option is not supported: • **request security idp security-package download node primary** • **request security idp security-package download node local** • **request security idp security-package download node all**

Logical Systems

- The **logical-systems all** option can now be specified for the **show security screen statistics** operational command.

Management Information Base (MIB)

- On all high-end SRX Series devices, in a chassis cluster environment, the calculation of the primary and secondary node sessions in the **JnxJsSPUMonitoringObjectsTable** object of the SPU monitoring MIB is incorrect because the MIB **jnxJsSPUMonitoringCurrentTotalSession** incorrectly displays total sessions. A doubled session count is displayed because the active and backup nodes are treated as separate sessions, although they are not.

  Count only the session numbers on the local node, thereby avoiding a double count, and local total sessions are displayed.

  In a chassis cluster environment, the **SPUMonitoringCurrentTotalSession** object of the MIB adds information per each SPU from the local node.

[*MIB Reference for SRX1400, SRX3400, and SRX3600 Services Gateways*; *MIB Reference for SRX5600 and SRX5800 Services Gateways*]

Security

- Public key infrastructure (PKI) objects include certificates, key pairs, and certificate revocation lists (CRLs). PKI objects are read from the PKI database when the PKI Daemon starts. The PKI daemon database loads all certificates into memory at boot time.

  When an object is read into memory from the PKI database, the following new log message is created:

  PKID_PV_OBJECT_READ: A PKI object was read into memory from <location>

Related Documentation

- New Features in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 95
- Outstanding Issues in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 117
- Resolved Issues in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 122
- Errata and Changes in Documentation for Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 130
- Known Limitations in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 105

Known Limitations in Junos OS Release 12.1 for High-End SRX Series Services Gateways

AppSecure

- J-Web pages for AppSecure are preliminary.
- Custom application signatures and custom nested application signatures are not currently supported by J-Web.
- AppFW does not operate on ALG data sessions. As a result, the AppFW rules are not applicable to these sessions. Therefore, ALG data sessions are excluded from AppFW counters.

Chassis Cluster

- On all high-end SRX Series devices in a chassis cluster, only four QoS queues are supported per **reth/ae** interface.
- In large chassis cluster configurations on SRX3400 or SRX3600 devices, you need to increase the wait time before triggering failover. In a full-capacity implementation, we recommend increasing the wait to 8 seconds by modifying **heartbeat-threshold** and **heartbeat-interval** values in the **[edit chassis cluster]** hierarchy.

  The product of the **heartbeat-threshold** and **heartbeat-interval** values defines the time before failover. The default values (**heartbeat-threshold** of 3 beats and **heartbeat-interval** of 1000 milliseconds) produce a wait time of 3 seconds.

  To change the wait time, modify the option values so that the product equals the desired setting. For example, setting the **heartbeat-threshold** to 8 and maintaining the default value for the **heartbeat-interval** (1000 milliseconds) yields a wait time of 8 seconds. Likewise, setting the **heartbeat-threshold** to 4 and the **heartbeat-interval** to 2000 milliseconds also yields a wait time of 8 seconds.
- Packet-based forwarding for MPLS and International Organization for Standardization (ISO) protocol familes is not supported.
- On SRX5600 and SRX5800 devices, only two of the 10 ports on each PIC of 40-port 1-Gigabit Ethernet I/O cards (IOCs) can simultaneously enable IP address monitoring. Because there are four PICs per IOC, this permits a total of eight ports per IOC to be monitored. If more than two ports per PIC on 40-port 1-Gigabit Ethernet IOCs are configured for IP address monitoring, the commit will succeed but a log entry will be generated, and the accuracy and stability of IP address monitoring cannot be ensured. This limitation does not apply to any other IOCs or devices.
- On all high-end SRX Series devices devices, IP address monitoring is not permitted on redundant Ethernet interface link aggregation groups (LAGs) or on child interfaces of redundant Ethernet interface LAGs.
- On all high-end SRX Series devices in chassis clusters, screen statistics data can be gathered on the primary device only.

- On all high-end SRX Series devices, ISSU does not support version downgrading.
- On all high-end SRX Series devices, only redundant Ethernet interfaces (reth) are supported for IKE external interface configuration in IPsec VPN. Other interface types can be configured, but IPsec VPN might not work.

Dynamic Host Configuration Protocol (DHCP)

- On all high-end SRX Series devices, DHCPv6 client authentication is not supported.

Dynamic VPN

- On all high-end SRX Series devices, DH-group 14 is not supported for dynamic VPN.

Flow and Processing

- On all high-end SRX Series devices, when packet-logging functionality is configured with an improved pre-attack configuration parameter value, the resource usage increases proportionally and might affect the performance.
- On all high-end SRX Series devices, SRX5600 and SRX5800 devices, services offloading has the following limitations:
  - Transparent mode is not supported. If transparent mode is configured, a normal session is installed.
  - Link aggregation group (LAG) is not supported. If a LAG is configured, a normal session is installed.
  - Only multicast sessions with one fan-out are supported. If a multicast session with more than one fan-out exists, a normal session is installed.
  - Only active/passive chassis cluster (HA) configuration is supported. Active/active chassis cluster configuration is not supported.
  - Fragmented packets are not supported. If fragmented packets exist, a normal session is installed.
  - Ingress and egress interfaces on different network processors are not supported. If an ingress interface and the related egress interface do not belong to the same network processor, a normal session is installed on the network processor.
  - IP version 6 (IPv6) is not supported. If IPv6 is configured, a normal session is installed.

NOTE: A normal session forwards packets from the network processor to the Services Processing Unit (SPU) for fast-path processing, while a services-offload session processes fast-path packets in the network processor and the packets exit out of the network processor itself.

- On SRX3400, SRX3600, SRX5600, and SRX5800 devices, the default authentication table capacity is 45,000; the administrator can increase the capacity to a maximum of 50,000.

On SRX1400 devices, the default authentication table capacity is 10,000; the administrator can increase the capacity to a maximum of 15,000.

- On all high-end SRX Series devices, when devices are operating in flow mode, the Routing Engine side cannot detect the path maximum transmission unit (PMTU) of an IPv6 multicast address (with a large size packet).
- On all high-end SRX Series devices, you cannot configure route policies and route patterns in the same dial plan.
- On all high-end SRX Series devices, high CPU utilization triggered for reasons such as CPU intensive commands and SNMP walks causes the Bidirectional Forwarding Detection protocol (BFD) to flap while processing large BGP updates.
- On all high-end SRX Series devices, downgrading is not supported in low-impact ISSU chassis cluster upgrades (LICU).
- On SRX5800 devices, network processing bundling is not supported in Layer 2 transparent mode.

Hardware

This section covers filter and policing limitations.

- On SRX1400, SRX3400, and SRX3600 devices, the following feature is not supported by a simple filter:
  - Forwarding class as match condition
- On SRX1400, SRX3400 and SRX3600, devices, the following features are not supported by a policer or a three-color-policer:
  - Color-aware mode of a three-color-policer
  - Filter-specific policer
  - Forwarding class as action of a policer
  - Logical interface policer
  - Logical interface three-color policer
  - Logical interface bandwidth policer
  - Packet loss priority as action of a policer
  - Packet loss priority as action of a three-color-policer
- On all high-end SRX Series devices, the following features are not supported by a firewall filter:
  - Policer action
  - Egress filter-based forwarding (FBF)

  - Forwarding table filter (FTF)
- SRX3400 and SRX3600 devices have the following limitations of a simple filter:
  - Forwarding class as match condition
  - In the packet processor on an IOC, up to 400 logical interfaces can be applied with simple filters.
  - In the packet processor on an IOC, the maximum number of terms of all simple filters is 2000.
  - In the packet processor on an IOC, the maximum number of policers is 2000.
  - In the packet processor on an IOC, the maximum number of three-color-policers is 2000.
  - The maximum burst size of a policer or three-color-policer is 16 MB.
- On SRX3400 and SRX3600 devices, when you enable the monitor traffic option using the **monitor traffic** command to monitor the FXP interface traffic, interface bounce occurs. You must use the **monitor traffic interface fxp0 no-promiscuous** command to avoid the issue.

Interfaces and Routing

- On all high-end SRX Series devices, the **set protocols bgp family inet flow** and **set routing-options flow** CLI statements are no longer available, because BGP flow spec functionality is not supported on these devices.
- On all high-end SRX Series devices, the Link Aggregation Control Protocol (LACP) is not supported on Layer 2 interfaces.
- On all high-end SRX Series devices, BGP-based virtual private LAN service (VPLS) over aggregated Ethernet (**ae**) interfaces is not supported. It works on child ports and physical interfaces.

Internet Key Exchange Version 2 (IKEv2)

On all high-end SRX Series devices, IKEv2 does not include support for:

- Policy-based tunnels
- Dial-up tunnels
- Network Address Translation-Traversal (NAT-T)
- VPN monitoring
- Next-Hop Tunnel Binding (NHTP) for st0—Reusing the same tunnel interface for multiple tunnels
- Extensible Authentication Protocol (EAP)
- IPv6
- Multiple child SAs for the same traffic selectors for each QoS value

- Proposal enhancement features
- Reuse of Diffie-Hellman (DH) exponentials
- Configuration payloads
- IP Payload Compression Protocol (IPComp)
- Dynamic Endpoint (DEP)

Intrusion Detection and Prevention (IDP)

- On all high-end SRX Series devices, from Junos OS Release 11.2 and later, the IDP security package is based on the Berkeley database. Hence, when the Junos OS image is upgraded from Junos OS Release 11.1 or earlier to Junos OS 11.2 or later, a migration of IDP security package files needs to be performed. This is done automatically on upgrade when the IDP daemon comes up. Similarly, when the image is downgraded, a migration (secDb install) is automatically performed when the IDP daemon comes up, and previously installed database files get deleted.

  However, migration is dependent on the XML files for the installed database to be present on the device. For first-time installation, full update files are required. If the last update on the device was an incremental update, migration might fail. In such a case, you have to manually download and install the IDP security package using the **download** or **install** CLI command before using the IDP configuration with predefined attacks or groups.

  Workaround: Use the following CLI commands to manually download the individual components of the security package from the Juniper Security Engineering portal and install the full update:

  - **request security idp security-package download full-update**
  - **request security idp security-package install**

- On all high-end SRX Series devices, the IDP policies for each user logical system are compiled together and stored on the data plane memory. To estimate adequate data plane memory for a configuration, consider these two factors:

  - IDP policies applied to each user logical system are considered unique instances because the ID and zones for each user logical system are different. Estimates need to take into account the combined memory requirements for all user logical systems.
  - As the application database increases, compiled policies will require more memory. Memory usage should be kept below the available data plane memory to allow for database increases.

- On all high-end SRX Series devices, ingress as ge-0/0/2 and egress as ge-0/0/2.100 works with flow showing both source and destination interface as ge-0/0/2.100.
- IDP does not allow header checks for nonpacket contexts.
- On all high-end SRX Series devices, application-level distributed denial-of-service (application-level DDoS) detection does not work if two rules with different application-level DDoS applications process traffic going to a single destination application server. When setting up application-level DDoS rules, make sure that you

do not configure rulebase-ddos rules that have two different application-ddos objects when the traffic destined to one application server can process more than one rule. Essentially, for each protected application server, you have to configure the application-level DDoS rules so that traffic destined for one protected server processes only one application-level DDoS rule.

NOTE: **Application-level DDoS rules are terminal, which means that once traffic is processed by one rule, it will not be processed by other rules.**

The following configuration options can be committed, but they will not work properly:

source-zone	destination-zone	destination-ip	service	application-ddos	Application Server
source-zone-1	dst-1	any	http	http-appddos1	1.1.1.1:80
source-zone-2	dst-1	any	http	http-appddos2	1.1.1.1:80

- On all high-end SRX Series devices, application-level DDoS rule base (rulebase-ddos) does not support port mapping. If you configure an application other than default, and if the application is from either predefined Junos OS applications or a custom application that maps an application service to a nonstandard port, application-level DDoS detection will not work.

  When you configure the application setting as default, intrusion detection and prevention (IDP) uses application identification to detect applications running on standard and nonstandard ports; thus, the application-level DDoS detection would work properly.

- On all high-end SRX Series devices, all IDP policy templates are supported except All Attacks. There is a 100-MB policy size limit for integrated mode and a 150-MB policy size limit for dedicated mode. The current IDP policy templates supported are dynamic, based on the attack signatures being added. Therefore, be aware that supported templates might eventually grow past the policy-size limit.

  On all high-end SRX Series devices, the following IDP policies are supported:

  - DMZ_Services
  - DNS_Service
  - File_Server
  - Getting_Started
  - IDP_Default
  - Recommended
  - Web_Server

- IDP deployed in both active/active and active/passive chassis clusters has the following limitations:
  - No inspection of sessions that fail over or fail back.
  - The IP action table is not synchronized across nodes.
  - The Routing Engine on the secondary node might not be able to reach networks that are reachable only through a Packet Forwarding Engine.
  - The SSL session ID cache is not synchronized across nodes. If an SSL session reuses a session ID and it happens to be processed on a node other than the one on which the session ID is cached, the SSL session cannot be decrypted and will be bypassed for IDP inspection.
- IDP deployed in active/active chassis clusters has a limitation that for time-binding scope source traffic, if attacks from a source (with more than one destination) have active sessions distributed across nodes, then the attack might not be detected because time-binding counting has a local-node-only view. Detecting this sort of attack requires an RTO synchronization of the time-binding state that is not currently supported.

IPv6 IPsec

IPv6 IPsec implementation has the following limitations:

- IPv6 routers do not perform fragmentation. IPv6 hosts should either perform path maximum transmission unit (PMTU) discovery or send packets smaller than the IPv6 minimum MTU size of 1280 bytes.
- Because IPv6 addresses are 128 bits long compared to IPv4 addresses, which are 32-bits long, IPv6 IPsec packet processing requires more resources. Therefore, a small performance degradation is observed.
- IPv6 uses more memory to set up the IPsec tunnel. Therefore, the IPsec IPv4 tunnel scalability numbers might drop.
- The addition of IPv6 capability might cause a drop in the IPsec IPv4-in-IPv4 tunnel throughput performance.
- The IPv6 IPsec VPN does not support the following functions:
  - 4in6 and 6in4 policy-based site-to-site VPN, IKE
  - 4in6 and 6in4 route-based site-to-site VPN, IKE
  - 4in6 and 6in4 policy-based site-to-site VPN, Manual Key
  - 4in6 and 6in4 route-based site-to-site VPN, Manual Key
  - 4in4, 6in6, 4in6, and 6in4 policy-based dial-up VPN, IKE
  - 4in4, 6in6, 4in6, and 6in4 policy-based dial-up VPN, Manual Key
  - Remote Access—XAuth, config mode, and shared IKE identity with mandatory XAuth
  - IKE authentication—public key infrastructure/digital signature algorithm (PKI/DSA)

- IKE peer type—Dynamic IP
- Chassis cluster for basic VPN features
- IKE authentication—PKI/RSA
- Network Address Translation-Traversal (NAT-T)
- VPN monitoring
- Hub-and-spoke VPNs
- Next Hop Tunnel Binding Table (NHTB)
- Dead Peer Detection (DPD)
- Simple Network Management Protocol (SNMP) for IPsec VPN MIBs
- Chassis cluster for advanced VPN features
- IPv6 link-local address
- All high-end SRX Series devices dependency

IPv6 Support

- **NSM**—Consult the Network and Security Manager (NSM) release notes for version compatibility, required schema updates, platform limitations, and other specific details regarding NSM support for IPv6 addressing on all high-end SRX Series devices.
- **Security policy**—Only IDP for IPv6 sessions is supported only for all high-end SRX Series devices. UTM for IPv6 sessions is not supported. If your current security policy uses rules with the IP address wildcard any, and UTM features are enabled, you will encounter configuration commit errors because UTM features do not yet support IPv6 addresses. To resolve the errors, modify the rule returning the error so that it uses the any-ipv4 wildcard; and create separate rules for IPv6 traffic that do not include UTM features.

J-Web

- On all high-end SRX Series devices, if the device is running the worldwide version of the Junos OS and you are using the Microsoft Internet Explorer Web browser, you must disable the Use SSL 3.0 option in the Web browser to access the device.
- To use the Chassis View, a recent version of Adobe Flash that supports ActionScript and AJAX (Version 9) must be installed. Also note that the Chassis View is displayed by default on the Dashboard page. You can enable or disable it using options in the Dashboard Preference dialog box, but clearing cookies in Internet Explorer also causes the Chassis View to be displayed.
- On all high-end SRX Series devices, users cannot differentiate between Active and Inactive configurations on the System Identity, Management Access, User Management, and Date & Time pages.

Logical Systems

- The master logical system must not be bound to a security profile that is configured with a 0 percent reserved CPU quota because traffic loss could occur. When upgrading all high-end SRX Series devices from Junos OS Release 11.2, make sure that the reserved CPU quota in the security profile that is bound to the master logical system is configured for 1 percent or more. After upgrading from Junos OS Release 11.2, the reserved CPU quota is added to the default security profile with a value of 1 percent.
- Starting with Junos OS Release 11.2, address books can be defined under the [**security**] hierarchy level instead of the [**security zones**] hierarchy level. This enhancement makes configuring your network simpler by allowing you to share IP addresses in address books when configuring features such as security policies and NAT. You can attach zones to address books—this is known as zone-attached configuration.

  Junos OS Release 12.1 continues to support address book configuration under the [**security zones**] hierarchy level—this is known as zone-defined configuration. However, we recommend that zone-attached address book configuration be used in the master logical system and user logical systems.

  If you upgraded your high-end SRX Series devices to this Junos OS Release 12.1, and are configuring logical systems on the device, the master logical system retains any previously configured zone-defined address book configuration. The master administrator can run the address book upgrade script to convert zone-defined configuration to zone-attached configuration. The upgrade script converts all zone-defined configurations in the master logical system and user logical systems. See the section, "Upgrade and Downgrade Scripts for Address Book Configuration" of "Upgrade and Downgrade Instructions for Junos OS Release 12.1 for High-End SRX Series Services Gateways" on page 130.
- On all high-end SRX Series devices, the logical systems feature does not support ALGs for user logical systems because ALGs are configured globally. If you enable ALGs at the root master logical system level, they are also enabled for user logical systems in Junos OS Release 12.1. In this case, user logical system traffic is processed by the ALGs, and corresponding ALG flow sessions are initiated under the user logical system. You can only enable and disable ALGs at the root master logical system level.
- On all high-end SRX Series devices, in Junos OS Release 12.1, the IPv6 forwarding and the logical system configuration are mutually exclusive. If you enable the IPv6 forwarding options (packet mode or flow mode), the logical system configuration related commit will fail and vice versa.

  You can still configure certain IPv6 objects under the root logical system and the user logical system if the system is in default mode (DROP). However, you cannot forward IPv6 traffic in this case.
- On all high-end SRX Series devices, quality-of-service (QoS) classification across interconnected logical systems does not work.
- On all high-end SRX Series devices, the number of logical system security profiles you can create is constrained by an internal limit on security profile IDs. The security profile ID range is from 1 through 32 with ID 0 reserved for the internally configured default security profile. When the maximum number of security profiles is reached, if you want

to add a new security profile, you must first delete one or more existing security profiles, commit the configuration, and then create the new security profile and commit it. You cannot add a new security profile and remove an existing one within a single configuration commit.

If you want to add more than one new security profile, the same rule is true. You must first delete the equivalent number of existing security profiles, commit the configuration, and then create the new security profiles and commit them.

- **User and administrator configuration for logical systems**—Configuration for users for all logical systems and all user logical systems administrators must be done at the root level by the master administrator. A user logical system administrator cannot create other user logical system administrators or user accounts for their logical systems.
- **Name-space separation**—The same name cannot be used in two logical systems. For example, if logical-system1 includes the username “Bob” then other logical systems on the device cannot include the username “Bob”.
- **Commit rollback**—Commit rollback is supported at the root level only.
- **Trace and debug**—Trace and debug are supported at the root level only.
- **Class of service**—You cannot configure class of service on logical tunnel (lt-0/0/0) interfaces.
- **ALGs**—The master administrator can configure ALGs at the root level. The configuration is inherited by all user logical systems. It cannot be configured discretely for user logical systems.

Network Address Translation (NAT)

- On all high-end SRX Series devices, in case of SSL proxy, sessions are whitelisted based on the actual IP address and not on the translated IP address. Because of this, in the whitelist configuration of the SSL proxy profile, the actual IP address should be provided and not the translated IP addresses.

  Example:

  Consider a destination NAT rule that translates destination IP address 20.20.20.20 to 5.0.0.1 using the following commands:

  - **set security nat destination pool d1 address 5.0.0.1/32**
  - **set security nat destination rule-set dst-nat rule r1 match destination-address 20.20.20.20/32**
  - **set security nat destination rule-set dst-nat rule r1 then destination-nat pool d1**

  In the above scenario, to exempt a session from SSL proxy inspection, the following IP address should be added to the whitelist:

  - **set security address-book global address ssl-proxy-exempted-addr 20.20.20.20/32**
  - **set services ssl proxy profile ssl-inspect-profile whitelist ssl-proxy-exempted-addr**

- Maximum capacities for source pools and IP addresses have been extended on all high-end SRX Series devices as follows:

Pool/PAT Maximum Address Capacity	SRX1400	SRX3400 SRX3600	SRX5600 SRX5800
Source NAT pools	8192	8192	12288
IP addresses supporting port translation	8192	8192	12288
PAT port number	256M	256M	384M

  Increasing the capacity of source NAT pools consumes memory needed for port allocation. When source NAT pool and IP address limits are reached, port ranges should be reassigned. That is, the number of ports for each IP address should be decreased when the number of IP addresses and source NAT pools is increased. This ensures NAT does not consume too much memory. Use the **port-range** statement in configuration mode in the CLI to assign a new port range or the **pool-default-port-range** statement to override the specified default.

  Configuring port overloading should also be done carefully when source NAT pools are increased.

  For source pool with port address translation (PAT) in range (64,510 through 65,533), two ports are allocated at one time for RTP/RTCP applications, such as SIP, H.323, and RTSP. In these scenarios, each IP address supports PAT, occupying 2048 ports (64,512 through 65,535) for Application Layer Gateway (ALG) module use. On SRX5600 and SRX5800 devices, if all of the 4096 source pool is configured, a port allocation of 8,388,608 is reserved for twin port use.

- **NAT rule capacity change**—To support the use of large-scale NAT (LSN) at the edge of the carrier network, the device-wide NAT rule capacity has been changed.

  The number of destination and static NAT rules has been incremented as shown in Table 9 on page 115. The limitation on the number of destination-rule-set and static-rule-set has been increased.

  Table 9 on page 115 provides the requirements per device to increase the configuration limitation as well as to scale the capacity for each device.

Table 9: Number of Rules on all High-End SRX Series Devices

NAT Rule Type	SRX1400	SRX3400 SRX3600	SRX5600 SRX5800
Source NAT rule	8192	8192	8192
Destination NAT rule	8192	8192	8192
Static NAT rule	20480	20480	20480

The restriction on the number of rules per rule set has been increased so that there is only a device-wide limitation on how many rules a device can support. This restriction is provided to help you better plan and configure the NAT rules for the device.

Security

- On all high-end SRX Series devices, the current SSL FP implementation has the following connectivity limitations:
  - The SSLv2 protocol is not supported. SSL sessions using SSLv2 are dropped.
  - SSL sessions where client certificate authentication is mandatory are dropped.
  - SSL sessions where renegotiation is requested are dropped.
- On all high-end SRX Series devices, for a particular session, the SSL proxy is only enabled if a relevant feature related to SSL traffic is also enabled. Features that are related to SSL traffic are Intrusion Detection and Prevention (IDP), application identification, application firewall, and application tracker. If none of the above listed features are active on a session, the SSL proxy bypasses the session and no logs are generated in this scenario.
- On all high-end SRX Series devices, the Secure Sockets Layer- Forward Proxy (SSL-FP) does not support key size of length greater than 2048 bits. The SSL-FP drops the connection when the key size in the server certificate is greater than 2048 bits.
- On all high-end SRX Series devices, the limitation on the number of addresses in an address-set has been increased to 1024. The default value of address-set is 1024. The number of addresses in an address-set, which depends on the device, is equal to the number of addresses supported by the policy.

Simple Network Management Protocol (SNMP)

- On all high-end SRX Series devices, the **show snmp mib** CLI command will not display the output for security related MIBs. We recommend that you use an SNMP client and prefix **logical-system-name@** to the community name. For example, if the community is **public**, use **default@public** for default root logical system.

Virtual Private Networks (VPNs)

- On all high-end SRX Series devices, when you enable VPN, overlapping of the IP addresses across virtual routers is supported with the following limitations:
  - An IKE external interface address cannot overlap with any other virtual router.
  - An internal/trust interface address can overlap across any other virtual router.

  - An **st0** interface address cannot overlap in route-based VPN in point-to-multipoint tunnels such as NHTB.
  - An **st0** interface address can overlap in route-based VPN in point-to-point tunnels.
- On all high-end SRX Series devices, the DF-bit configuration for VPN only works if the original packet size is smaller than the **ST0** interface MTU, and larger than the **external interface - ipsec overhead**.
- The local-IP feature is not supported on the following:
  - All SRX Series devices in chassis cluster configuration
  - All high-end SRX Series devices
- On all high-end SRX Series devices, the IPsec NAT-T tunnel scaling and sustaining issues are as follows:
  - For a given private IP address, the NAT device should translate both 500 and 4500 private ports to the same public IP address.
  - The total number of tunnels from a given public translated IP cannot exceed 1000 tunnels.

Related Documentation

- New Features in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 95
- Resolved Issues in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 122
- Outstanding Issues in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 117
- Errata and Changes in Documentation for Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 130
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 102

Outstanding Issues in Junos OS Release 12.1 for High-End SRX Series Services Gateways

The following problems currently exist in Juniper Networks SRX Series Services Gateways. The identifier following the descriptions is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

Application Layer Gateway (ALG)

- On SRX3400 devices, in active/backup chassis cluster mode, after routing group failover, Avaya phones cannot hang up. Some messages sent by Avaya phones are dropped by the device. If you want to make another call, you should unregister the phone and register again. [PR/581917]

Chassis Cluster

- On SRX5600 devices in a chassis cluster, using the **set system processes chassis-control disable** command might result in chassisd crash. [PR/296022]
- On SRX5600 and SRX5800 devices, the disable node does not reboot automatically when the **control-link-recovery** is enabled. [PR/451852]
- On all high-end SRX Series devices, IP status remaining cannot be tracked at the secondary node after the reth interface's child interfaces are disabled. [PR/488890]
- On SRX5600 devices in a chassis cluster, some central point binding entries are not aged out after stress test. [PR/611827]
- On all high-end SRX Series devices, the **graceful-restart** option needs to be configured in multicast chassis cluster deployment to avoid multicast flow session being rebuilt after RG0 failover. [PR/663525]
- On SRX3600 devices in a chassis cluster, you must use the default directory /var/tmp when loading a trusted CA certificate. If the file is in a different location, you must specify the full path, even if the current working directory and the file are available in the same location.

  Example:

  - Loading CA certificate without providing full path for directory.

    root@dut# run request security pki ca-certificate load filename sample.crt ca-profile sample_profile

    ```
    node0:
    --------------------------------------------------------------------------
    error: Failed to read the certificate file /var/tmp/sample.crt. The
    certificate might not exist or it might be corrupted
    ```

  - Loading CA certificate by providing full path for directory.

    root@dut# run request security pki ca-certificate load filename /cf/root/sample.crt ca-profile sample_profile

    ```
    node0:
    --------------------------------------------------------------------------
    Fingerprint:
      a0:c3:8e:4f:80:e6:73:a2:f7:63:e8:21:52:fa:79:82:c1:0f:f7:5c (sha1)
      6a:8d:aa:e1:22:73:b2:ec:fe:8e:2d:82:97:75:c5:38 (md5)
    CA certificate for profile sample_profile loaded successfully
    ```

  As a workaround, use full path of directory to load the certificate.

  [PR/672166]

Command-line Interface (CLI)

- On SRX3400 devices, the **show security flow session summary** displays an incorrect service-offload session number when a service-offload multicast session exists. [PR/696828]
- On all high-end SRX Series devices, under certain conditions, session numbers displayed by the **show security flow session summary** and **show security flow session services-offload** commands might not be consistent. [PR/700461]
- On all high-end SRX Series devices, description of the screen is displayed in operational mode. [PR/712242]
- On all high-end SRX Series devices, the **show security ike security-associations** and **show security ike security-associations detail** commands outputs are in disorderly-manner. This is a display issue and have no impact on performance. [PR/729804]

Flow and Processing

- On all high-end SRX Series devices, RG0 failover incorrectly triggers the traps for IFLs. [PR/418684]
- On all high-end SRX Series devices, the active SA number on the Routing Engine and SPU does not match if many tunnels are established at the same time. [PR/591991]
- On SRX3400 and SRX3600 devices, the diagnostic test (diagtest) for recb_i2c_rep_clk_generator and recb_i2c_chassis_ideeprom fails. [PR/602621, PR/704967]
- On all high-end SRX Series devices, changes in policer, filter, or sampling configuration cause core files to be generated when multicast traffic is received. [PR/613782]
- On SRX3400 and SRX3600 devices, the CPU utilization is higher by 75 to 85 percent on FPCs when 4000 IFLs are configured on redundant Ethernet interfaces (reth). [PR/670925]
- On SRX5600 devices, PPTP RM leak-related issues are seen during long sessions of traffic. [PR/684432]
- When certificate key size is 2048 bytes and total combined certificate request size is greater than 4096 bytes, the PKID service might crash on certificate enrollment. As a workaround, use a shorter 'Subject' field to get the total certificate request size smaller than 4096 bytes. [PR/698846]
- On SRX3600 devices, where large volume of firewall-authentication requests and changes of security policy happen at exactly same time, device may crash due to race condition. As a workaround, avoid changing security policy, when device is receiving large volume of firewall-authentication requests. [PR/726940]

Interfaces and Routing

- On SRX1400 devices, RTSP interleave data packets cannot be passed when the RTP length is greater than 3000 bytes. [PR/703663]

IPV6

- On all high-end SRX Series devices, the input packets and bytes counter shows random values both in traffic statistics and IPv6 transit statistics, when VLAN tagging is added or removed from the IPv6 address configured interface. [PR/489171]

J-Web

- On all high-end SRX Series devices, on the Monitor > Events and Alarms> View Events page, if you try to generate a report by using the Generate Report option, the report opens in the same webpage. [PR/433883]
- On all high-end SRX Series devices, the MGCP configuration page does not display the default values. [PR/599996]
- On all high-end SRX Series devices, the SCCP configuration page does not display the default values. [PR/607455]
- On all high-end SRX Series devices, the right-click option to navigate to chassis information or system information in the Chassis View page is not working properly. To access these pages, you have to navigate to the respective pages by clicking on that page itself from the Monitor page instead of using right-click option. [PR/684849]
- On all high-end SRX Series devices, when configuring a NAT rule-set in J-Web interface, security zones can not be displayed if no interfaces are configured for those security zones. As a workaround, you must configure the interfaces for the zones before using the zones in NAT rule-set. [PR/703264]
- On all high-end SRX Series devices, automatic refresh on the Application Tracking monitor page does not clear the pop-up window with the message **Data is very minimal to display in PIE Chart**, even when the chart gets loaded with data on refresh. [PR/724995]

Logical Systems

- On all high-end SRX Series devices, multiple logical systems that have All Attack policies fail to compile in the Routing Engine due to memory limit.

  The IDP policies for each user logical system are compiled together and stored on the data plane memory. To estimate adequate data plane memory for a configuration, consider these two factors:

  - IDP policies applied to each user logical system are considered unique instances because the ID and zones for each user logical system are different. Estimates need to take into account the combined memory requirements for all user logical systems.

- As the application database increases, compiled policies will require more memory. Memory usage should be kept below the available data plane memory to allow for database increases. [PR/667983]

Network Address Translation (NAT)

- On SRX3600 devices, when the destination NAT is enabled on the device, AI cache entries for both external NAT IP and actual IP are displayed for the same session as shown in the following sample:

  show services application-identification application-system-cache

  ```
  Application System Cache Configurations:
    application-cache: on
    nested-application-cache: on
    cache-unknown-result: on
    cache-entry-timeout: 3600 seconds
  pic: 2/0
  Logical system name: root-logical-system
  IP address: 5.0.0.1                                Port: 443    Protocol:
   TCP
  Application: HTTP                                    Encrypted: Yes

  Logical system name: root-logical-system
  IP address: 20.20.20.100                           Port: 443    Protocol:
   TCP
  Application: SSL                                     Encrypted: Yes
  ```

  [PR/687311]

- On SRX5600 and SRX5800 devices, using a same source NAT pool by both NAT and NAT-PT traffic causes a core file to be generated. As a workaround, use different source NAT pools for NAT and NAT-PT rules. [PR/736374]

Upgrade and Downgrade

- On all high-end SRX Series devices, application identification does not support downgrade of the image. When you attempt to downgrade the device, you must download and install the signature database again.

  If you upgrade the image from Junos OS Release 11.4 to 12.1, application identification signature requires about around 30 seconds to do recompile. During this period, application identification cannot identify traffic and application firewall drops the traffic as unknown session. [PR/689304]

- On all high-end SRX Series devices, upgrade failed for Junos OS Release 11.1R6.4 to 11.4R2.3 build due to AI installation failure without xcommit result. As a workaround, use the following steps before upgrading the image:

  set system processes idp-policy disable

  commit

  Once the device comes up after reboot, delete the configuration to enable idp daemon to start:

  delete system processes idp-policy

commit

[PR/729625]

Virtual Private Network (VPN)

- On all high-end SRX Series devices, site-to-site policy-based VPN in three or more zones configuration does not work if the policies match the address "any" instead of specific addresses and all cross-zone traffic policies are pointing to the single site-to-site VPN tunnel. As a workaround, configure address books in different zones to match the source and destination and use the address book name in the policy to match the source and destination. [PR/441967]
- On SRX5600 devices, the Key Management daemon (KMD) might restart when you change the configuration from dynamic end point (DEP) to shared IKE. As a workaround, deactivate security policies before switching the configuration from DEP to shared IKE. [PR/702222]

Related Documentation

- New Features in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 95
- Known Limitations in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 105
- Errata and Changes in Documentation for Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 130

Resolved Issues in Junos OS Release 12.1 for High-End SRX Series Services Gateways

The following are the issues that have been resolved in Junos OS Release 12.1 for Juniper Networks SRX Series Services Gateways. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

Application Layer Gateways (ALGs)

- On SRX3400 and SRX5600 devices, calls per second (CPS) of RTSP ALG traffic in both Layer 2 and Layer 3 mode were dropped to 300 per SPU. [PR/676053: This issue has been resolved.]

Authentication

- On all branch SRX Series devices, firewall authentication supported a maximum of 64 users or groups in policy “client-match”. [PR/661587: This issue has been resolved.]

Chassis Cluster

- On SRX5800 devices in chassis cluster, when both devices in a cluster had RG1+ priority 0 (when cold-sync was not completed), it was not possible to predict which node would assume the primary role. [PR/678019: This issue has been resolved.]
- On all high-end SRX Series devices operating in a chassis cluster, the XML response to the RPC validate command did not return the closing </routing-engine> tag for the second node. [PR/679413 : This issue has been resolved.]
- On SRX3600 devices, in rare instances, the primary Routing Engine might not send the deletion of the destination route pointing to the decoupled next hop to the secondary Routing Engine. This caused a system panic, and a VMcore file was created on the secondary Routing Engine. [PR/684981: This issue has been resolved.]
- On SRX3400 devices, when a service-offload session was set up in a multicast session on the primary node, it acted as a normal session in the backup node. This occurred because the services-offload flag was not correctly synchronized to the backup node. During a chassis cluster failover, a route change was triggered, and the service-offload session was reinstalled. [PR/696819: This issue has been resolved.]
- On SRX3400 devices, during failover, there was a small window of time in which the SPU did not detect whether an NP was in services-offload mode or not. This might cause a small number of the services-offload sessions to change to normal sessions. [PR/697426: This issue has been resolved.]
- On SRX1400 devices in a chassis cluster, unwanted timed out data path trace messages were seen. [PR/703272: This issue has been resolved.]
- On SRX5800 devices in a chassis cluster, if ALG traffic was too high and both the ports were used, some single ports on backup caused traffic outflow. [PR/705799: This issue has been resolved.]
- On SRX1400 devices in a chassis cluster, the primary control link heartbeats were not seen and were causing inconsistent system behavior. This happened when a 16-Port SFP Gigabit Ethernet I/O card or a 16-Port Copper Ethernet/Fast Ethernet/Gigabit Ethernet I/O card was on the device. [PR/718054: This issue has been resolved.]
- On all high-end SRX Series devices operating in a chassis cluster, if an ECMP (equal-cost multipath) route had both local and remote interfaces, then the local interface was favored for the next hop to avoid the performance-related issues that involved forwarding the traffic across the fabric link. [PR/718807: This issue has been resolved.]

Command-line Interface (CLI)

- On SRX5800 devices, the configuration knob **set security pki ca-profile *profile-name* revocation-check crl disable on-download-failure** could not prevent a revocation check even when the PKI server was unreachable. [PR/605042: This issue has been resolved]
- On all high-end SRX Series devices, the **clear services application-identification application-system-cache** command was missing including the following options:
  - node- Clears the cache entry from both the nodes

- node local- Clears the cache entry from the local device
- node primary- Clears the cache entry from the primary node

[PR/678624: This issue has been resolved.]

- On all high-end SRX Series devices, deleting the groups at certain hierarchy level could erase junos-defaults groups. [PR/689912: This issue has been resolved.]
- On all high-end SRX Series devices, the **set security zones security-zone zone tcp-rst** command had an incorrect configuration description as **Send RST for TCP SYN packet not matching session**. The correct description is **Send RST for TCP non-SYN packet not matching existing session**. [PR/703196: This issue has been resolved.]
- On all high-end SRX Series devices, the show command for ntp (**show ntp status**) was not working. [PR/722537: This issue has been resolved.]

Dynamic Host Configuration Protocol (DHCP)

- On SRX3600 devices, the DHCP relay server was required to have DNS configuration for DHCP clients. The DHCP daemon read the DNS configuration and the daemon was stopped when there was an invalid dns-server value (for example, 0.0.0.0). [PR/706615: This issue has been resolved.]

Flow and Processing

- On all high-end SRX Series devices, when packet-logging functionality was configured with an improved pre-attack configuration parameter value, the resource usage increased proportionally and affected the performance. [PR/526155: This issue has been resolved.]
- On all high-end SRX Series devices, if the maximum number of leaves on a multicast distribution tree was exceeded, the multicast sessions were created up to the maximum number of leaves, and any multicast sessions that exceeded the maximum number of leaves were ignored. In previous releases, no multicast traffic was forwarded if the maximum number of leaves on the multicast distribution tree was exceeded. The maximum number of leaves on a multicast distribution tree is device specific. [PR/561442: This issue has been resolved]
- On SRX5600 devices, in certain cases, loading an IDP detector caused a flowd crash, showing memcpy as the top of the stack. [PR/570361: This issue has been resolved]
- On SRX5800 devices, the message log **ipc_msg_write: %PFE-3: IPC message type: 27, subtype: 2 exceeds MTU, mtu 3216, length 3504** appeared occasionally due to internal communication. [PR/612757: This issue has been resolved.]
- On all high-end SRX Series devices, the BFD session on routing protocols was not working. [PR/671444: This issue has been resolved.]
- On all high-end SRX Series devices, additional neighbor solicitation packets sent were corrupted. The packet had zeroed destination MAC address and the entire packet was prefixed by two random bytes. [PR/671658: This issue has been resolved.]

- On SRX3400 devices, failover with the RG0 and RG1 generated a VM core file. [PR/675860: This issue has been resolved.]
- On SRX1400, SRX3400, SRX3600, SRX5600 devices, the **Link failure happened for DPC%d PFE%d** log message displays incorrect FPC number. [PR/683371: This issue has been resolved.]
- On SRX5600 devices, SIP calls were not getting cleared for memory leak. [PR/684000: This issue has been resolved.]
- On SRX3400 and SRX3600 devices, over 4 Gbps EF(TOS 101) queue traffic caused SPU crash. [PR/686133: This issue has been resolved.]
- On SRX3400 and SRX3600 devices, adding and deleting IKE gateways multiple times when SAs were active resulted in a KMD core file. [PR/689470: This issue has been resolved.]
- On all high-end SRX Series devices, a data plane failover resulted in a traffic loss for a short period when the device was active with a large number of routes. [PR/690004: This issue has been resolved.]
- On SRX3400 and SRX3600 devices, the incorrect value for the **error mbuf statistics** option was displayed in the **show xlr pkt_mbuf use** vty command on the SPU. [PR/693200: This issue has been resolved]
- On SRX5800 devices, under certain conditions, deleting an **fxp0** configuration and rolling it back set the **fxp0** forcefully to nonnegotiated, 100m/full duplex mode. [PR/696733: This issue has been resolved.]
- On SRX5600 devices, when IKE and IPsec configuration or security configuration was removed and added back frequently, KMD core files were generated. [PR/698718: This issue has been resolved.]
- On SRX3400 and SRX3600 devices, the **reth** interface did not work properly when you changed the **reth** member interfaces to other interfaces using different speeds and the link speeds were mismatched. [PR/698837: This issue has been resolved]
- On all high-end SRX Series devices, a memory leak occurred during the audit event processing. [PR/698907: This issue has been resolved.]
- On all high-end SRX Series devices, the PIM register messages were dropped on the physical interfaces that hosted multiple unnumbered interfaces. [PR/698943: This issue has been resolved.]
- On SRX5600 devices, the message vector create_pdp_rsp changed tunnel state from half to active and inserted it into active timer wheel. These actions resulted in no tunnel lock protection. When del_pdp_rsp deleted the user tunnel or clear path, this led to a change in both the aging flag and the timer wheel entry pointer. [PR/699147: This issue has been resolved.]
- On SRX3600 devices, a session drop due to not being authenticated, was logged as RT_FLOW_SESSION_CLOSE and had the wrong close reason other than **unset**. [PR/701971: This issue has been resolved.]
- On SRX5600 devices, sending the ALG traffic and changing configuration to delete related policy resulted in flowd core files. [PR/702418: This issue has been resolved.]

- On SRX1400 devices, RTSP interleave data packets could not be passed when the RTP length was greater than 3000 bytes. [PR/703663: This issue has been resolved.]
- On SRX5600 devices, the JSRPD used the IIC device to set HA LED. The JSRPD, who's function is jsrpd_a2a10_set_led_color() function was trigged when the **ge-0/0/2** interface was down. The jsrpd_a2a10_set_led_color() function did not close when the LED color set function was done. This behavior caused the FD leak and eventually resulted in generation JSRPD core file. [PR/703799: This issue has been resolved.]
- On all high-end SRX Series devices, the following warning messages were not displayed when heap and/or arena memory utilization reached a certain critical level
  - `Warning: Heap utilization reaches critical level!`
  - `Warning: Arena utilization reaches critical level!`

  Messages were displayed after the memory utilization fell back below the critical level:

  Default values for heap warning_level is 95%, and arena warning_level is 90%.

  - `Heap utilization falls back to normal level`
  - `Arena utilization falls back to normal level`

  vty commands to set the critical level

  - `set xlr heap warning_level [0:100]`
  - `set xlr arena warning_level [0:100]`

  [PR/705118: This issue has been resolved.]
- On SRX5600 devices, packets with packet length of 500 bytes were corrupted when only packet capture of data path debug was present without configuration of the **record-pic-history** and event **np-egress**. [PR/706858: This issue has been resolved.]
- On all high-end SRX Series devices, configuring the **tcp-options** under individual policy resulted in commit failing with the following error message:

  ```
  error reading services-offload attribute
  ```

  [PR/726059: This issue has been resolved.]
- On SRX3400, SRX3600, SRX5600, SRX5800 devices, sometimes, traffic sent by authenticated users (authenticated by web authentication) was not passing through the firewall. This is because, authentication entry created in CP was not passed along to SPU. [PR/734869: This issue has been resolved.]
- On SRX5600 devices, NSD core files were generated. [PR/735152: This issue has been resolved.]
- On SRX3600 devices, flowd core files are generated. [PR/735924: This issue has been resolved.]

Hardware

- On all high-end SRX Series devices, during cyclic redundancy check (CRC), an alarm were not generated, when a dip4 hardware error occurred on the central point (CP). [PR/683212: This issue has been resolved.]

Installation

- On all high-end SRX Series devices, while downgrading from Junos Release 11.4 or a later image to Junos Release 11.1 or an earlier image, the security package was deleted. Although it was automatically installed when the IDP daemon came up, this automatic installation failed sometimes due to application identification (AI) installation error. [PR/705113: This issue has been resolved.]

Intrusion Detection and Prevention (IDP)

- On SRX3400 devices, heap memory usage increased slightly after you performed multiple pushes of IDP policies with multiple rules. [PR/684630: This issue has been resolved.]

Interfaces and Routing

- On SRX1400 devices, when system was rebooted for the first time, if the physical connections for the VPN gateways were down, the **st0** interfaces were up even though VPNs were never established. This situation led to "black holing" traffic when static routes were used over those **st0** interfaces. [PR/669833: This issue has been resolved.]
- On SRX3400 devices, the TX lockup of the **em0** interface caused the **em0** interface to go down and caused all field-replaceable units (FRU) to go offline. [PR/685451: This issue has been resolved.]
- On SRX5600 and SRX5800 devices, using ftp to **st0** interface for data transfer fails occasionally. [PR/706827: This issue has been resolved.]

Internet Protocol Security (IPsec)

- On SRX3400 and SRX3600 devices, initial contact notification sent from peer for the IKEv1 protocol was not getting processed. Because of this, stale IKE and IPsec security association were displayed. However functionality was not affected. [PR/705123: This issue has been resolved.]
- On all high-end SRX Series devices, occasionally, when keys are generated incorrectly for IPsec, VPN to go down due to encapsulation security payload (ESP) failures. [PR/717969: This issue has been resolved.]

J-Web

- On all high-end SRX Series devices, on the **Configure>Security>Policy>Define AppFW Policy> Add Rule Set** page in the J-Web interface , the Default Rule was getting displayed, leading to the incorrect configurations. [PR/593551: This issue has been resolved.]
- On SRX 3400 devices in a chassis cluster, while monitoring the device through J-Web, the dashboard incorrectly displayed the session utilization value. The displayed value was above 100 percent and activated or maximum sessions were displayed as 3M or 2.5M. This was due to The dashboard incorrectly displayed the combined values of both primary and secondary nodes. [PR/666489: This issue has been resolved.]
- On SRX3600 devices, the policy validating pop-up window in the J-Web was not cleared after it was dragged. [PR/675554: This issue has been resolved.]
- On all high-end SRX Series devices, when using the CLI you could configure only an AppQoS rule set without configuring any other diff-services. However, in J-Web, you could configure at least one diff-service for a new AppQoS rule set configuration. [PR/686462: This issue has been resolved.]
- On SRX1400 devices, when you modified an existing policy or created a new policy with junos-host zone, there was no junos-host zone available in the from-zone or to-zone list. [PR/697863: This issue has been resolved.]
- On SRX1400 devices, authentication through J-Web failed if password contained the special characters: **'** , **"**, **+**, ****

  [PR/725901: This issue has been resolved.]
- On all high-end SRX Series devices, the Application Tracking monitor page does not display the warning **no data to display**, when there is no data to display in the table. [PR/724985: This issue has been resolved.]

Management Information Base (MIB)

- On all high-end SRX Series devices, when you polled the device with five SPCs and three SPCs, the device reported the wrong number of sessions for the object ID jnxJsSPUMonitoringMaxTotalSession (1.3.6.1.4.1.2636.3.39.1.12.1.3.0). [PR/488653: This issue has been resolved.]

Logical Systems

- The **logical-systems all** option was not available in some of the operational commands such as **show security screen statistics**. [PR/598032: This issue has been resolved.]
- On SRX3400 devices, when you configured LSYS and then loaded override configuration with a different LSYS configuration (both having the old and new LSYS), the proxy-ndp route might fail to push to the Packet Forwarding Engine. If you deleted old LSYS and added new LSYS in one commit, the proxy-ndp route failed to push to the Packet Forwarding Engine. [PR/673930: This issue has been resolved.]

- On SRX3400 devices, when NAT64 was used in the logical system (LSYS), the binding did not age out and the reversed binding did not match successfully. The NAT64 in LSYS function did not work. [PR/675052: This issue has been resolved.]
- On SRX5600 devices in a chassis cluster, some NAT sessions kept invalidated status after multiple failovers. [PR/676385: This issue has been resolved.]
- On SRX3400 devices, in J-Web, you could not edit the **lt** interface for LSYS. [PR/700354: This issue has been resolved.]
- On SRX1400 devices, the LSYS capacity number for nat-rule-referenced-prefix lsys profile was displayed incorrectly. [PR/707108: This issue has been resolved.]
- On all high-end SRX Series devices running Junos OS Release 11.2, when a logical system feature was added, diagnostic information was sent to a specific file without rotation control, causing core files to be generated. [PR/721104: This issue has been resolved.]

Network Address Translation (NAT)

- On SRX3600 devices, when there was heavy SIP traffic and a share gate was involved, NAT translation-context might leak. [PR/675869: This issue has been resolved.]
- On all high-end SRX Series devices, the static NAT with a default routing instance was not working. [PR/706183: This issue has been resolved.]
- On all high-end SRX Series devices, when two static NAT rules were configured with the same prefix and all the interfaces were in the default routing-instance, and only one rule was configured with the **static-nat prefix routing-instance default** option, the commit completed successfully without prompting about the overlapping information. [PR/708433: This issue has been resolved.]
- On SRX5600 devices, during high-rate NAT session creation, high CPU usage might be seen on the central point on the backup node. [PR/720010: This issue has been resolved.]

Virtual Private Network (VPN)

- On SRX5600 devices in a large configuration with heavy traffic, after reboot failover in chassis cluster, the Routing Engine on the new primary node became very busy. As a result, the FPC was detached, causing traffic to fail when passing through the firewall device. [PR/698150: This issue has been resolved.]

Related Documentation

- New Features in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 95
- Known Limitations in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 105
- Errata and Changes in Documentation for Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 130

Errata and Changes in Documentation for Junos OS Release 12.1 for High-End SRX Series Services Gateways

Errata for the Junos OS Software Documentation

This section lists outstanding issues with the software documentation.

J-Web

- **J-Web pages for stateless firewall filters**—There is no documentation describing the J-Web pages for stateless firewall filters. To find these pages in J-Web, go to **Configure>Security>Firewall Filters**, and then select **IPv4 Firewall Filters** or **IPv6 Firewall Filters**. After configuring the filters, select **Assign to Interfaces** to assign your configured filters to interfaces.

Junos OS Security Configuration Guide

- This guide incorrectly states that the Junos OS Release 12.1 supports security chains, which validate a certificate path upward through eight levels of CA authorities in the PKI hierarchy. The Junos OS Release 12.1 does not support security chains.

Related Documentation

- New Features in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 95
- Known Limitations in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 105
- Outstanding Issues in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 117
- Resolved Issues in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 122

Upgrade and Downgrade Instructions for Junos OS Release 12.1 for High-End SRX Series Services Gateways

In order to upgrade to Junos OS Release 12.1, your device must be running one of the following Junos OS Releases:

- 9.1S1
- 9.2R4
- 9.3R3
- 9.4R3
- 9.5R1 or later

If your device is running an earlier release, upgrade to one of these releases and then to the 12.1 release. For example, to upgrade from Release 9.2R1, first upgrade to Release 9.2R4 and then to Release 12.1.

For additional upgrade and download information, see the *Junos OS Initial Configuration Guide for Security Devices* and the *Junos OS Migration Guide*.

Upgrade and Downgrade Scripts for Address Book Configuration

Beginning with Junos OS Release 11.4 or later, you can configure address books under the **[security]** hierarchy and attach security zones to them (zone-attached configuration). In Junos OS Release 11.1 and earlier, address books were defined under the **[security zones]** hierarchy (zone-defined configuration).

You can either define all address books under the **[security]** hierarchy in a zone-attached configuration format or under the **[security zones]** hierarchy in a zone-defined configuration format; the CLI displays an error and fails to commit the configuration if you configure both configuration formats on one system.

Juniper Networks provides Junos operation scripts that allow you to work in either of the address book configuration formats (see Figure 2 on page 132).

About Upgrade and Downgrade Scripts

After downloading the Junos OS Release 12.1, you have the following options for configuring the address book feature:

- **Use the default address book configuration**—You can configure address books using the zone-defined configuration format, which is available by default. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.
- **Use the upgrade script**—You can run the upgrade script available on the Juniper Networks support site to configure address books using the new zone-attached configuration format. When upgrading, the system uses the zone names to create address books. For example, addresses in the trust zone are created in an address book named **trust-address-book** and are attached to the trust zone. IP prefixes used in NAT rules remain unaffected.

  After upgrading to the zone-attached address book configuration:

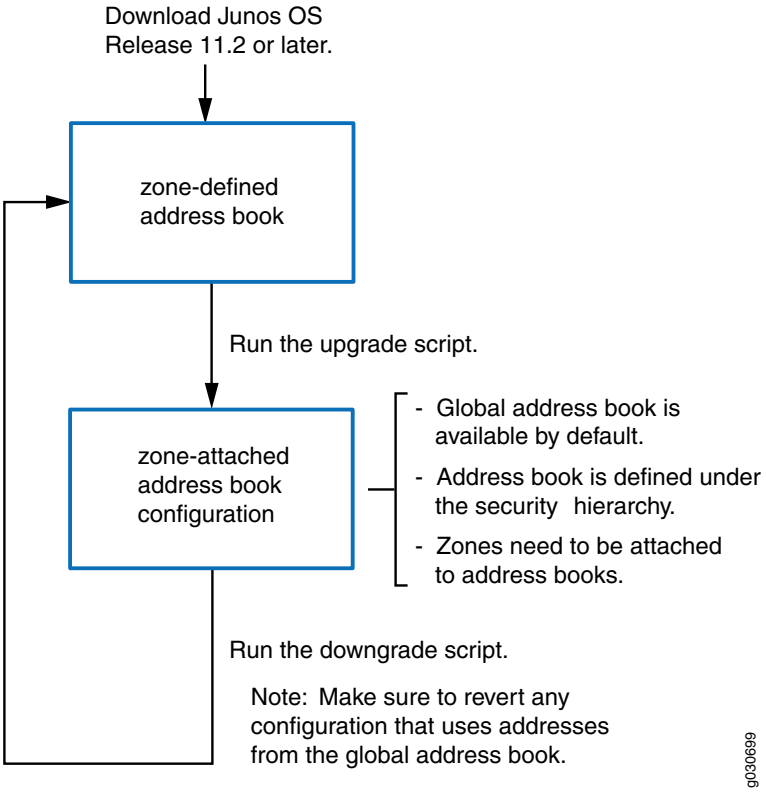
  - You cannot configure address books using the zone-defined address book configuration format; the CLI displays an error and fails to commit.
  - You cannot configure address books using the J-Web interface.

  For information on how to configure zone-attached address books, see the Junos OS Release 11.4 documentation.

- **Use the downgrade script**—After upgrading to the zone-attached configuration, if you want to revert to the zone-defined configuration, use the downgrade script available on the Juniper Networks support site. For information on how to configure zone-defined address books, see the Junos OS Release 11.1 documentation.

NOTE: Before running the downgrade script, make sure to revert any configuration that uses addresses from the global address book.

Figure 2: Upgrade and Downgrade Scripts for Address Books



Running Upgrade and Downgrade Scripts

The following restrictions apply to the address book upgrade and downgrade scripts:

- The scripts cannot run unless the configuration on your system has been committed. Thus, if the zone-defined address book and zone-attached address book configurations are present on your system at the same time, the scripts will not run.
- The scripts cannot run when the global address book exists on your system.
- If you upgrade your device to Junos OS Release 11.4 or later and configure logical systems, the master logical system retains any previously configured zone-defined address book configuration. The master administrator can run the address book upgrade script to convert the existing zone-defined configuration to the zone-attached

configuration. The upgrade script converts all zone-defined configurations in the master logical system and user logical systems.

NOTE: You cannot run the downgrade script on logical systems.

For information about implementing and executing Junos operation scripts, see the *Junos OS Configuration and Operations Automation Guide*.

Upgrade Policy for Junos OS 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 10.0, 10.4, and 11.4 are EEOL releases. You can upgrade from Junos OS Release 10.0 to Release 10.4 or even from Junos OS Release 10.0 to Release 11.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind. For example, you cannot directly upgrade from Junos OS Release 10.3 (a non-EEOL release) to Junos OS Release 11.4 or directly downgrade from Junos OS Release 11.4 to Junos OS Release 10.3.

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 http://www.juniper.net/support/eol/junos.html .

Hardware Requirements for Junos OS Release 12.1 for High-End SRX Series Services Gateways

Transceiver Compatibility for SRX Series Devices

We strongly recommend that only transceivers provided by Juniper Networks be used on high-end SRX Series Services Gateways interface modules. Different transceiver types (long-range, short-range, copper, and others) can be used together on multiport SFP interface modules as long as they are provided by Juniper Networks. We cannot guarantee that the interface module will operate correctly if third-party transceivers are used.

Please contact Juniper Networks for the correct transceiver part number for your device.

Related Documentation

- New Features in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 95
- Errata and Changes in Documentation for Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 130

- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for High-End SRX Series Services Gateways on page 102

Junos OS Release Notes for M Series Multiservice Edge Routers, MX Series 3D Universal Edge Routers, and T Series Core Routers

New Features in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers

The following features have been added to Junos OS Release 12.1. Following the description is the title of the manual or manuals to consult for further information:

Class of Service

- **Support for set forwarding class and DSCP value (MX Series routers with MPC/MIC interfaces)**—The set forwarding class and DSCP value for Routing Engine generated traffic is now supported on MX Series routers with MPC/MIC interfaces. For example, use **b100110** instead of **100110**. This notation is applicable in all places where a binary DSCP value is specified under the **[edit firewall]** hierarchy level.

  [*Class of Service*]

- **Class-of-service features on an ATM MICs (MX Series routers)**—The following class-of-service features are now supported on an ATM MIC:

  - Traffic shaping and scheduling—Traffic shaping determines the maximum amount of traffic that can be transmitted on an interface. To configure traffic shaping and

scheduling profile for ATM MICs, you must configure the service category by including the **atm-service** statement at the following hierarchy level:

[edit class-of-service traffic-control-profiles *traffic-control-profile-name*]

You can configure three different categories of ATM service: constant bit rate (cbr), non-real-time variable bit rate (nrvbr), and real-time variable bit rate (rtvbr). The service category works in conjunction with ATM cell parameters **peak-rate**, **sustained-rate**, and **max burst-size** to impose traffic shaping, transmit-rate, shaping-rate, and default excess-rate for an ATM queue.

- Policing—Policing, or rate limiting, enables you to limit the amount of traffic that passes into or out of the interface. It works with firewall filters to thwart denial-of-service (DoS) attacks. You can enable the input or output transmission rate of ATM traffic by including the **atm-policier** statement at the following hierarchy level:

  [edit firewall]

  Networks police traffic by limiting the input or output transmission rate of a class of traffic on the basis of user-defined criteria. The ATM policer controls the maximum rate of traffic sent or received on the interface on which it is applied. To apply the policer at the interface level, you must include the **atm-policer** statement at the following hierarchy level:

  [edit interface at-*fpc/pic/port* unit *unit number*]

  To apply limits to the traffic flow, configure the **cdvt** and **peak-rate** parameters within the policer. Define the **policing-action** parameter as **discard**, **discard-tag**, and **count** to set a consequence for the packets that exceed these limits. The consequence is usually a higher loss priority so that if the packets encounter downstream congestion, they are discarded first.

[Class of Service]

- **Policer support for aggregated Ethernet bundles (MX Series routers with MPC/MIC Interfaces)**—Aggregated interfaces support single-rate policers, single-rate three-color marking policers, two-rate three-color marking policers, and hierarchical policers. By default, policer bandwidth and burst size applied on aggregated bundles are not matched to the user-configured bandwidth and burst size. Because an aggregated Ethernet interface is a bundle of Ethernet links of the same speed, if the user-configured bandwidth on aggregated bundles is 40 Mbps, each link has 40 Mbps. As a result, the effective bandwidth and burst size available to the aggregated interface are a lot higher than the value configured.

  You can now configure interface-specific policers applied on an aggregated Ethernet bundle to match the effective bandwidth and burst size to user-configured values.

  To configure this feature, include the **shared-bandwidth-policer** statement at the following hierarchy levels:

  [edit firewall policer *policer-name*]

  [edit firewall three-color-policer *policer-name*]

  [edit firewall hierarchical-policer *policer-name*]

This capability applies to all interface-specific policers of the following types: single-rate policers, single-rate three-color marking policers, two-rate three-color marking policers, and hierarchical policers. This capability does not apply to policers, hierarchical policers, and three-color policers used inside filters that are not interface-specific. It also does not apply to implicit policers and prefix-specific action policers.

[*Class of Service*]

- **Class-of-service features supported on T4000 Core Router**—The following class-of-service (CoS) features are supported on the T4000 Core Router:
  - Behavior aggregate (BA) classifiers:
    - Differentiated Services code point (DSCP) for IP DiffServ
    - DSCP for IPv6 DiffServ
    - IP precedence
    - MPLS EXP
    - IEEE 802.1p CoS
    - IEEE 802.1ad drop eligible indicator (DEI)
  - Fixed classification—You can configure fixed classification on a logical interface by specifying a forwarding class to be applied to all packets received by the logical interface, regardless of the packet contents.

    NOTE: **On the T4000 Core Router, BA classification and fixed classification are mutually exclusive. That is, only one of the classification can be configured.**
  - Tricolor marking (TCM)—By default, TCM is enabled. On the T1600 Enhanced Scaling FPC4 (T1600-FPC4-ES), the **[TCP,PLP]** bits are used when TCM is enabled to identify four drop profiles, whereas on the T4000 Type 5 FPC (T4000-FPC5-3D), only **[PLP1,PLP0]** bits are used.
  - IEEE 802.1p CoS bit rewrite and IEEE 802.1ad DEI rewrite.
  - Rewrite rules—The T4000 Type 5 FPC supports rewrite rules on the basis of the forwarding class and packet loss priority.
  - A maximum of 16 forwarding classes and four types of packet loss priorities: **low**, **high**, **medium-low**, and **medium-high**.
  - Low and high levels of fabric queuing priorities.
  - Default scheduler—By default, the best effort forwarding class receives 95 percent of the bandwidth and buffer space for the output link, and the network control forwarding class receives 5 percent. The default drop profile causes the buffer to fill and then discard all packets until it has space.

- The lowest of the scaling numbers associated with MX Series and T Series routers.
- On the T4000 Type 5 FPC, excess bandwidth is shared in the ratio of the transmit rates. This distribution can be updated by configuring the **excess-rate** statement at the **[edit class-of-service schedulers scheduler-name]** hierarchy level. You can specify the excess rate sharing by percentage or by proportion.

[*Class of Service*]

- **Extends filter and policer feature support on T4000 Type 5 FPC (T4000-FPC5-3D)**—The filter and policer features supported on the T1600 Enhanced Scaling Type 4 FPC (T1600-FPC4-ES) are also supported on the T4000 Type 5 FPC (T4000-FPC5-3D), with the following exceptions:
  - Service PIC–related filters
  - Logical interface policer as filter action
  - Physical interface policers
  - Applying a policer at the logical interface level
  - Hierarchical policers
  - Label-switched path (LSP) policers
  - Address Resolution Protocol (ARP) policers
  - Tricolor marking policers
  - Forwarding table filters
  - Filter-based forwarding
  - Prefix-specific actions
  - Sampling and port-mirror features
  - Filter actions such as **ipsec-sa**, **service-accounting**, and **service-filter-hit**
  - The **dscp 0** action is not supported during the interoperation between a T1600 Enhanced Scaling Type 4 FPC and T4000 Type 5 FPC.
  - Shared bandwidth policer
  - A filter attached at the Layer 2 application point (that is, at the logical interface level) is unable to match with the forwarding class of a packet that is set by a Layer 3 classifier such as DSCP, DSCP V6, **inet-precedence**, and **mpls-exp**.
  - Using **interface-group** and **interface-group-except** as match conditions for the VPLS family filter
  - The ability to filter MPLS-tagged IPv4 packets based on IP parameters

- Applying filters at **set interfaces lo0 unit 0 family any filter input *filter-name***
- Using source class usage (SCU) or destination class usage (DCU) as filter match conditions

[*Network Interfaces*], [*Firewall Filters and Traffic Policers*]

- **Extends support for tunnel services features on T4000 Type 5 FPC (T4000-FPC5-3D)**—Starting with Junos OS Release 12.1, all the tunnel services features supported on Modular Port Concentrators (MPCs) and Modular Interface Cards (MICs) on MX Series routers are now supported on the T4000 Type 5 FPC.

  [*Services Interfaces*, *System Basics*]

- **Set IPv6 DiffServ code point (DSCP) and MPLS EXP independently (MX Series routers with MPC/MIC interfaces)**—You can now set the packet DSCP and MPLS EXP bits independently on IPv6 packets with MPC/MIC interfaces. To enable this feature, include the **protocol mpls** statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit* rewrite-rules dscp-ipv6 *rule-name*]** hierarchy level.

  You can set DSCP IPv6 values only at the ingress MPLS node.

  Class of Service

High Availability

- **Support extended for Layer 3 features (MX Series routers with MPC/MIC interfaces)**—Junos OS Release 12.1 extends supports for the following Layer 3 features on MX Series routers with MPC/MIC interfaces:
  - **Fragmentation support for GRE-encapsulated packets**—Enables the Packet Forwarding Engine to update the IP identification field in the outer IP header of packets encapsulated with generic routing encapsulation (GRE), so that reassembly of the packets is possible after fragmentation.
  - **Pseudowire redundancy**—Enables you to configure redundant Layer 2 circuit pseudowires between devices. Layer 2 circuit and VPLS services can be maintained between devices connected using pseudowires in the network even after certain failures in the control or data plane. Backup pseudowires can be configured between Layer 2 devices in the customer's network and PE routers within the service provider's network.
  - **Distributed PPM support for LACP**—Enables you to switch between distributed and centralized periodic packet management (PPM). By default, distributed PPM is active.
  - **External/Internal BGP VPN load balancing and egress filtering support**—Enables you to load-balance traffic across external and internal BGP paths and simultaneously configure egress filters and policers on the VRF interfaces.
  - **Egress filtering of PIMv4/v6 messages**—Enables you to filter PIM join and prune messages at the egress interfaces for IPv4 and IPv6 in the upstream direction. The messages can be filtered based on the group address, source address, outgoing interface, PIM neighbor, or a combination of these values. This is useful when the

core of your network is using a mix of IP and MPLS. You can use this feature to selectively filter PIM join and prune messages and forward them to PIM neighbors.

These features can now interoperate between an MPC and a DPC when both are present on the same MX Series router.

[*Services Interfaces*, *High Availability*, *Network Interfaces*, *Multicast*]

- **Faster commit process**—Enables faster commit and commit synchronization because of the addition of two configuration statements at the **[edit system]** hierarchy level.
  - **commit fast-synchronize**—Run the commits in parallel on both master and backup Routing Engines to reduce the time taken for commit synchronization.
  - **commit flatten-groups**—Enable the use of a flattened configuration file for faster commit process.

  [*High Availability*, *System Basics*, *CLI User Guide*]

Interfaces and Chassis

- **Sanity polling for FPCs on T Series routers**—Sanity polling is supported for FPCs on T Series routers. You can configure the **sanity-poll** statement for a particular FPC to start a periodic sanity check for error conditions in the FPC.

  NOTE: **Currently, periodic sanity check is performed only on the routing chip register.**

  You can configure the **sanity-poll** statement for the FPC at the **[edit chassis fpc *slot-number*]** hierarchy level. On a TX Matrix or TX Matrix Plus router, you can configure the statement at the **[edit chassis lcc *number* fpc *number*]** hierarchy level.

  The **sanity-poll** statement detects an error condition and generates an emergency system log message in the FPC. You can configure the **retry-count** statement to perform rechecks for a specified number of times after detecting an error. If you do not configure the **retry-count** statement, then by default, the **sanity-poll** statement checks the detected error 10 times for a particular FPC.

  If an error persists after all rechecks, sanity polling reports an error and takes appropriate actions. You can configure the **on-error** statement to perform the appropriate actions:

  - **raise-alarm** generates the chassis alarm.
  - **power cycle** reboots the FPC after generating a core file.
  - **power off** halts the FPC, which is useful in case of permanent hardware failure.
  - **write-coredump** triggers the core file.

  [*System Basics*]

- **Display IPv6 statistics for MLPPP bundles**—Starting with Junos OS Release 12.1, the **show interfaces lsq-*fpc/pic/port*** command displays the packet and byte counters for

IPv6 data for Multilink Point-to-Point Protocol (MLPPP) bundles on link services intelligent queuing (LSQ) interfaces.

[*Interfaces Command Reference*]

- **IPv6 support for inline flow monitoring**—Starting with Junos OS Release 12.1, all MX Series routers with Modular Port Concentrators (MPCs) support monitoring and sampling services inline for IPv6 packets. To configure inline flow monitoring for IPv6, include the **inline-jflow** statement at the **[edit forwarding-options sampling instance *instance-name* family inet6 output]** hierarchy level. Inline sampling exclusively supports a new format called IP_FIX that uses UDP as the transport protocol. When you configure inline sampling, include the **version-ipfix** statement at the **[edit forwarding-options sampling instance *instance-name* family inet6 output flow-server *address*]** hierarchy level.

  [*Services Interfaces*]

- **Support for multilink-based protocols on channelized MICs (MX240, MX480, and MX960 routers)**—Starting with Junos OS Release 12.1, multilink-based protocols are extended to the following channelized Modular Interface Cards (MICs) on MX240, MX480, and MX960 routers:

  - 4-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP (MIC-3D-4CHOC3-2CHOC12)
  - 8-port Channelized SONET/SDH OC3/STM1 (Multi-Rate) MIC with SFP (MIC-3D-8CHOC3-4CHOC12)
  - 8-port Channelized DS3/E3 MIC (MIC-3D-8CHDS3-E3-B)

  The following encapsulations and protocols are also supported on the aforementioned MICs:

  - Multilink Point-to-Point Protocol (MLPPP)
  - Multiclass MLPPP
  - Multilink Frame Relay (MLFR) end-to-end (FRF.15)
  - Multilink Frame Relay (MLFR) UNI NNI (FRF.16) (also referred to as MFR)
  - Compressed Real-Time Transport Protocol (CRTP)

  [*Services Interfaces Configuration Guide*]

- **Support for combined operation of Synchronous Ethernet and Precision Time Protocol or hybrid mode (MX Series 3D Universal Edge Routers)**—Combined operation of Synchronous Ethernet and Precision Time Protocol (PTP), also known as hybrid mode, is supported on the MX80 3D Universal Edge Routers with precision timing support (MX80-P). It is also supported on MX240, MX480, and MX960 routers. On the MX240, MX480, and MX960 routers, the combined operation is possible only when the PTP client and the Synchronous Ethernet source are on the same enhanced MPC and are traceable to the same master clock.

In hybrid mode, the synchronous Ethernet Equipment Clock (EEC) on the Modular Port Concentrator (MPC) derives the frequency from Synchronous Ethernet and the phase from PTP (also known as IEEE 1588v2) for time synchronization.

NOTE: MX80-P routers, when acting as PTP client nodes, can accept any external Synchronous Ethernet clock as reference and do not support building-integrated timing supply (BITS) input as frequency source in hybrid mode of operation. Only Synchronous Ethernet sources are allowed in hybrid mode.

To configure hybrid mode, include the **hybrid synchronous-ethernet-mapping clock-source <*ip-address*> interface <*interface-name1*> interface <*interface-name2*>** statement at the **[edit protocols ptp slave]** hierarchy level.

To set the Ethernet Synchronization Message Channel (ESMC) from the PTP clock class, include the **convert-clock-class-to-quality-level** statement at the **[edit protocols ptp slave]** hierarchy level.

To override the default PTP clock class to ESMC mapping, include the **clock-class-to-quality-level-mapping quality-level <*ql-value*> clock-class <*clock-class-value*>** statement at the **[edit protocols ptp slave]** hierarchy level.

Clock class is a variable (values range from 80 through 109), which indicates the present state of the master clock. Quality level or ***ql*** is the clock type.

Note that when the selected Synchronous Ethernet reference fails, the system continues to work in PTP mode. You can use the **show ptp hybrid status** operational command to find the current operating mode.

NOTE: Unified in-service software upgrade (unified ISSU) is currently not supported when hybrid mode is configured on MX80-P, MX240, MX480, and MX960 routers.

NOTE: To switch between the PTP and Synchronous Ethernet modes, you must first deactivate the configuration for the current mode and then commit the configuration. Wait for a short period of 30 seconds, configure the new mode and its related parameters, and then commit the configuration.

[*System Basics*, *System Basics and Services Command Reference*]

- **Support for FlowTapLite**—Starting with Junos OS Release 11.2R3, all MX Series routers with MPC/MIC interfaces support FlowTapLite for IPv4 and IPv6.
- **ATM PWE3 support on ATM MICs with SFP (MX Series routers)**—The new ATM MIC (model number: MIC-3D-8OC3-2OC12-ATM) enables support for ATM Pseudowire Emulation Edge to Edge (PWE3) on MX Series routers. The MIC is rate-selectable at the following rates: 2 OC12 ports or 8 OC3 ports.

The ATM MIC with SFP is supported on the following MPCs:

- 30-Gigabit Ethernet Queuing MPC (MX-MPC1-3D-Q)
- 60-Gigabit Ethernet Queuing MPC (MX-MPC2-3D-Q)
- 60-Gigabit Ethernet Enhanced Queuing MPC (MX-MPC2-3D-EQ)

The ATM MIC with SFP is not supported on the following MPCs:

- 30-Gigabit Ethernet MPC (MX-MPC1-3D)
- 60-Gigabit Ethernet MPC (MX-MPC2-3D)

The following features are supported on the ATM MIC (model number: MIC-3D-8OC3-2OC12-ATM) with SFP:

- Default framing mode on all ports is SONET. The MIC supports both SONET and SDH framing mode. The mode can be set at the MIC level or at the port level. To enable SONET or SDH framing at the port level, you need to set the framing statement at the **[chassis fpc *MPC-slot-number* pic *MIC-slot-number* port *port-number*]** hierarchy level. To enable SONET or SDH framing at the MIC level, you must set the framing statement at the **[chassis fpc *MPC-slot-number* pic *MIC-slot-number*]** hierarchy level.
- ATM pseudowire encapsulation. The pseudowire encapsulation can be either cell-relay or AAL5 transport mode. Both modes enable sending of ATM cells between the MIC and a Layer2 network.
- Cell relay VPI/VCI swapping. The ATM MIC can now overwrite the values for VPI/VCI on egress and on both ingress and egress. The ATM MIC can also pass the value transparently (no-rewrite).

  To configure the ATM MIC to modify both the VPI and VCI header values on both ingress and egress, you must specify the **psn-vci** statement at the following hierarchy level:

  [edit interface at-*interface-name/pic/port* unit *logical-unit-number*]

  NOTE: **Cell relay VPI/VCI swapping on both ingress and egress is not compatible with the ATM policing feature.**

  To configure the ATM MIC to modify only the VPI values on both ingress and egress, you must specify the **psn-vpi** statement at the following hierarchy level:

  [edit interface at-*interface-name/pic/port* unit *logical-unit-number*]

  NOTE: **Cell relay VPI swapping on both ingress and egress is not compatible with the ATM policing feature.**

  To configure the ATM MIC to pass the value transparently, you must specify the **no-vpivci-swapping** statement at the following hierarchy level:

  [edit interface at-*interface-name/pic/port* unit *logical-unit-number*]

If none of the configuration statements mentioned earlier are included, for VP pseudowires, VPI values are modified on egress. For VC pseudowires, both VPI and VCI values are modified on egress. The ATM policing feature is compatible with cell relay VPI/VCI swapping on egress.

[*Network Interfaces*]

- **Static mapping for port forwarding**—You can now configure port forwarding without translation of destination ports. Port forwarding now also supports EIM (endpoint-independent mapping), EIF (endpoint-independent filltering), and APP (address pooling paired).

  Port forwarding changes the destination port , destination address, or both, which are contained in a packet entering a NAT gateway. The translation facilitates reaching a host within a masqueraded, typically private, network, based on the port number on which it was received from the originating host. Port forwarding allows remote computers such as public machines on the Internet, to connect to a non-standard port (port other than 80) of a specific computer within a private network. An example of this type of destination is the host of a public HTTP server within a private network, Port forwarding supports only IPv4 addresses.

  To configure port forwarding with port translation only:

  - Include the **destined-port** *port-id* **translated-port** *port-id* statement at the **[edit services nat port-forwarding** *map-id***]** hierarchy level. You can specify up to 32 port mappings under a single **map-id**.
  - Include the following statements at the **edit services nat rule** *rule-name* **term** *term-name* **then]** hierarchy level:
    - **port-mappings** *map-name*
    - **no-translation**

  [*Services Interfaces*, *Next-Generation Network Addressing*, *Systems Basics and Services Command Reference*]

- **Configuring parameters for offloading flows**—Starting with Junos OS Release 12.1, you can set the parameters for flow offloading by configuring the **set trio-flow-offload minimum bytes** and **set trio-flow-offload minimum-age** statements under the **[edit interfaces ms-***fpc/pic/port* **service-options]** hierarchy level. Offloading is supported on all MX Series routers with Modular Port Concentrator (MPCs)/Modular Interface Cards (MICs). The configuration allows any plug-in or daemon on a PIC to generate a flow offload request and offload the flows to the Packet Forwarding Engine (PFE).

  The **show services sessions** command displays flow offload status for each session.

  [*Services Interfaces*]

- **New 100-Gigabit Ethernet 3D Modular Port Concentrator (MPC) with two Modular Interface Card (MIC) slots (100-Gigabit CFP MIC and a 20-port 1-Gigabit Ethernet MIC) on MX Series routers**—MX960, MX480, and MX240 routers now support a 100-Gigabit Ethernet MPC (model number MX-MPC3E-3D), and two MICs (MIC-3D-1X100GE-CFP and MIC-3D-20GE-SFP) as field-replaceable units (FRUs). The MPC provides packet-forwarding services that deliver up to 120 Gbps of full-duplex

traffic. The MPC is inserted into a slot in a router. MICs provide the physical interface and are installed into the MPCs. The 100-Gigabit Ethernet MPC has two separate slots for the MICs and requires the Enhanced MX Switch Control Board (SCBE) for fabric redundancy, but you can continue to use existing SCBs without fabric redundancy. The MPC interoperates with existing MX Series line cards, including Dense Port Concentrators (DPCs) and other MPCs. The 100-Gigabit Ethernet MPC is based on a new Junos OS chipset for increased scalability for bandwidth, subscribers, and service capabilities of the routers.

The following are the key features of the 100-Gigabit Ethernet 3D MPC:

- Supports 100-Gigabit Ethernet interfaces
- Supports two separate slots for MICs (MIC-3D-1X100GE-CFP and MIC-3D-20GE-SFP)
- Supports one 100-Gigabit Ethernet port per MIC
- Supports up to 120 Gbps of full-duplex traffic
- Supports up to 200 Gpbs aggregate WAN bandwidth connectivity for the two MIC slots; the line card is oversubscribed in the ratio of 2:1.
- Supports one full-duplex 10-Gigabit tunnel interface for each Packet Forwarding Engine
- Supports intelligent oversubscription services

The 100-Gigabit Ethernet 3D MPC supports feature parity with the following Junos OS Release 10.4 software features:

- Basic Layer 2 features and virtual private LAN service (VPLS) functionality, except for Operation, Administration, and Maintenance (OAM)
- Layer 3 routing protocols
- MPLS
- Multicast forwarding
- Firewall filters and policiers
- Class-of-service (CoS) support
- Tunnel support
- Interoperability with existing DPCs and MPCs

The following features are not supported on the 100-Gigabit Ethernet 3D MPC:

- Fine-grained queuing and input queuing
- Unified in-service software upgrade (ISSU)
- Multilink services

- Internet Group Management Protocol (IGMP) snooping with bridging, integrated routing and bridging (IRB), or VPLS
- Intelligent hierarchical policers
- Layer 2 trunk port
- MPLS-fast reroute (FRR) VPLS instance prioritization
- Precision Time Protocol (IEEE 1588)
- Synchronous Ethernet
- J-Flow monitoring and services
- Virtual chassis support

For more information about the supported and unsupported Junos OS software features for this MPC, see "Protocols and Applications Supported by MX Series MPCs" in the *MX Series Line Card Guide*.

[*MX Series Line Card*]

- **100-Gigabit Ethernet Modular Port Concentrator (MPC) on MX Series routers**—MX Series routers with the 100-Gigabit Ethernet MPC and a 20 port 1-Gigabit Ethernet MIC or a 100-Gigabit CFP MIC provide tunnel support parity, replacing traditional tunnel and services PICs with tunnels that were supported on a "virtual" port on the MX Series Packet Forwarding Engine. The 100-Gigabit Ethernet MPC has the model number MX-MPC3E-3D.

  The 100-Gigabit Ethernet MPC supports all of the features of the existing Modular Port Concentrators (MPCs) and supports two new features:

  - GRE keys
  - GRE clear-dont-fragment

  The 100-Gigabit Ethernet MPC extends the supported bandwidth values from 1 gigabit per second and 10 gigabits per second, adding 20 gigabits per second and 40 gigabits per second options when used with the 100-Gigabit CFP MIC or 40-Gigabit Ethernet MIC.

  [*Services Interfaces*, *System Basics*, *Hardware Guide*]

- **LAG/LACP for 10-port 10-Gigabit Ethernet PICs**—10-port 10-Gigabit Ethernet PICs support link aggregation from the following Type 3 10-Gigabit Ethernet PICs: 1x10-Gigabit Ethernet IQ2, 1x10-Gigabit Ethernet IQ2E and 10-Gigabit Ethernet-XENPAK. For bandwidth aggregation, load sharing, and link protection, LAG can be enabled. After aggregated Ethernet is enabled, LACP protocol forms an aggregated bundle of member links.

  [*Network Interfaces*]

- **New switch fabric module to support fabric bandwidth for T4000 router**—The T4000 router is an upgraded version of the T1600 router. The T4000 router consists of a new switch fabric module with fabric bandwidth double the capacity of the T1600 router.

As a result of the new switch fabric module to support the fabric bandwidth for the T4000 router, the output of the **show chassis fabric topology *<sib-slot>*** command is changed. This command displays the connectivity and the link status between the Packet Forwarding Engine and the Switch Interface Board (SIB). The following commands related to switch fabric management are also supported on T4000 routers:

- **show chassis fabric sibs**—Displays the state of the electrical switch fabric links between the SIB and the Packet Forwarding Engine.
- **show chassis fabric fpcs**—Displays the state of the electrical switch fabric links between the Flexible PIC Concentrators (FPCs) and the SIBs.

[*System Basics and Services Command Reference*]

- **Command output changes for Type 5 FPC (T4000 routers)**—Starting with Release 12.1, Junos OS supports the Type 5 FPCs, thereby resulting in the following command output changes:
  - **show chassis environment fpc** *<slot>* command displays the temperatures and voltages on various sensors on the FPC. The actual information displayed might differ from the existing output format.
  - **show chassis hardware** command additionally displays the Type 5 FPC output with the existing output fields.

  [*T4000 PIC Guide*, *System Basics and Services Command Reference*]

- **Support for 100-Gigabit Ethernet PIC on Type 5 FPC (T4000 Routers)**—Starting with Junos OS Release 12.1, the T4000 Core Router supports the 1-port 100-Gigabit Ethernet PIC on Type 5 FPC.

  The 100-Gigabit Ethernet PIC is a 1-port 100-Gigabit Ethernet Type 5 PIC with 100-Gigabit C form-factor pluggable transceiver (CFP) (model number PF-1CGE-CFP).

  The 100-Gigabit Ethernet PIC on Type 5 FPC supports the following software features:

  - Access to all 100-Gigabit Ethernet port counters through SNMP.
  - Interrupt-driven link down detection mechanism—An interrupt-driven link-down notification is generated to trigger locally attached systems to declare the interface down within a few milliseconds of failure.
  - Juniper Networks enterprise-specific Ethernet Media Access Control (MAC) MIB.
  - Interoperability with the 100-Gigabit Ethernet PIC on Type 4 FPC through configuration in **sa-multicast** forwarding mode. The VLAN steering mode is not supported on the 100-Gigabit Ethernet PIC on Type 5 FPC.

  All the software features and CLI commands available for 100-Gigabit Ethernet PIC on Type 4 FPC are also supported.

  NOTE: Graceful Routing Engine switchover (GRES) and unified in-service software upgrade (unified ISSU) are not supported on T4000 Core Routers in Junos OS Release 12.1.

[*Ethernet Interfaces*]

- **Support for 10-Gigabit Ethernet LAN/WAN PIC with SFP+ on Type 5 FPC (T4000 Router)**—Starting with Junos OS Release 12.1, the 12-port 10-Gigabit Ethernet LAN/WAN PIC with SFP+ (model number PF-12XGE-SFPP) is supported on T4000 routers.

  The following software features are supported on the 12-port 10-Gigabit Ethernet LAN/WAN PIC with SFP+:

  - Access to all 10-Gigabit Ethernet port counters through SNMP.
  - Interrupt-driven link down detection mechanism—An interrupt-driven link-down notification is generated to trigger locally attached systems to declare the interface down within a few milliseconds of failure.
  - LAN PHY mode

  All the software features and CLI commands available for the 10-Gigabit Ethernet LAN/WAN PIC with SFP+ on Type 4 FPC are also supported.

  NOTE: WAN-PHY mode is not supported in Junos OS Release 12.1 on 10-Gigabit Ethernet LAN/WAN PIC on Type 5 FPC.

  [*Ethernet Interfaces*]

- **New VJX1000 Virtual Router**—Introducing the VJX Series family of Junos OS-based virtual routers that run within the Junosphere environment. Junosphere is a cloud-based, on-demand networking environment that enables network design, testing, and training using routers running Junos OS and security systems. The VJX Series delivers the software functionality of Juniper Networks routers including command-line interfaces (CLIs), control plane behavior, protocol operation, and forwarding functions.

  For more information about Junosphere and VJX1000, see http://www.juniper.net/techpubs/en_US/release-independent/junosphere/information-products/pathway-pages/junosphere/product/index.html.

- **Display Layer 2 statistics for MLPPP, FRF.15, and FRF.16 bundles**—Starting with Junos OS Release 12.1, the **show interfaces lsq-*fpc/pic/port*** command has a **l2-statistics** option that displays Layer 2 queue statistics for the link services intelligent queuing (LSQ) and redundant LSQ interfaces. The queue statistics are displayed for Multilink Point-to-Point Protocol (MLPPP), FRF.15, and FRF.16 bundles on Multiservices PICs.

  [*Interfaces Command Reference*]

- **Aggregated Ethernet interfaces support hierarchical queuing and shaping (MX Series routers with MPC/MIC interfaces)**—Extends support for aggregated Ethernet interfaces in non-link-protect mode through Junos OS Release 10.2 on MX Series routers with MPC/MIC interfaces. The scheduler functions supported are per-unit scheduler, hierarchical scheduler, and shaping at the physical and logical interface (aggregated interface) level.

  [*Network Interfaces*]

- **Support for managing HTTP subscriber sessions based on request URI or domain name of a site**—You can configure a service set to set up an URL rule or a collection of URL rules that enable clients logging in to the router using HTTP sessions to be allowed or denied access. This functionality uses the capabilities of the High-Availability Chassis Manager (HCM) component. The URL rule or rule set contains a sequence of parameters that enable or discard access to HTTP clients for the website or server to which they want to access. You can configure the host name or the domain name of websites for which you want to monitor and manage access by HTTP clients. When an HTTP client sends a GET request to the router, if the host portion or the uniform resource identifier (URI) portion of the HTTP request header matches the configured values in the defined URL rule in the service set, an action is taken as specified in the URL rule. You can specify an action to perform one of the following tasks when a match is found for the incoming HTTP request:

  - Accept—Causes the HTTP requests to be processed and enables access to the requested site.
  - Accept and Log Requests—Causes the HTTP requests to be processed and stores a system logging entry for each client session that was established.
  - Accept and Count Requests—Enables access for the client that sends the HTTP GET request and saves each request from the client in a counter. This counter displays the cumulative value of all service sets that contain URL rules with the matching domain name or the IP address of the client's HTTP request that enabled access.
  - Discard—Causes the HTTP requests to be dropped and disables access to the requested site.
  - Discard and Log Requests—Causes the HTTP requests to be processed and stores a system logging entry for each client session that was terminated.

  To configure the URL rule for processing of HTTP requests from clients, include the **url-rule** statement at the **[edit services hcm]** hierarchy level. To group a set of URL rules in a set, include the **url-rule-set** statement at the **[edit services hcm]** hierarchy level.

  Each MultiServices DPC network processing unit (NPU) can service up to 50,000 requests or transactions per second from HTTP clients if the only operation that is running on the service plane is the URL monitoring process.

  If more than one request URL or hostname is configured in a URL rule of a service set, the client that sends the HTTP request is enabled access when the first match is found for the domain name or URI portion of the HTTP request. The remaining host names or URIs are disregarded in the URL rule or rule set. If a host name is not specified, "any" hostname is assumed which is specified by an asterisk (*) in the URL rule. Similarly, if a request URI is not specified, "any" URI is assumed.

  The HTTP URL management and monitoring feature for client requests works only for Services SDK applications.

  [*Services Interfaces*]

- **Support for L-PDF and AACL on aggregated multiservices interfaces**—Aggregated multiservice PICs (ams interfaces) enable multiple multiservices- interfaces grouped together in a single bundle and cause the traffic destined for this ams group to be

distributed over the member service PICs of the group. This capability enables load-balancing of traffic across various service PICs in an ams group.

You can configure the application identification (APPID) service and the intrusion detection and prevention (IDP) functionality on M120 or M320 routers equipped with Aggregated Multiservices PICs. AMS interfaces enable an N:1 redundancy mechanism to cluster together N number of ms- interfaces in an ams group that supports load sharing. Flows to be handled by APPID and IDP are distributed dynamically to all multiservices PICs in an ams group using the Packet Forwarding Engine. This method of dynamic dispersion of packet flows avoids the limitations of throughput and scaling that might occur with a single multiservices PIC.

[*Services Interfaces*]

- **Support for L-PDF and AACL on aggregated multiservices interfaces**—Aggregated Multiservice PICs (ams interfaces) enable multiple multiservice interfaces grouped together in a single bundle and cause the traffic destined for this ams group to be distributed over the member service PICs of the group. Junos Trio chipsets enable the calculation of a symmetric hash for the forward and reverse flows, and support a microcode map in the forwarding plane. This capability enables load-balancing of traffic across various service PICs in an ams group.

  You can configure the application-aware access list (AACL) service and the local policy decision functionality (L-PDF) on M120 or M320 routers equipped with Aggregated Multiservices PICs. Ams interfaces enable an N:1 redundancy mechanism to cluster together N number of multiservice interfaces in an ams group that supports load sharing.

  Traffic policers are instantiated on a per-service PIC basis. As a result, if the traffic for one L-PDF subscriber is distributed over multiple multiservice interfaces, the traffic policer functionality does not operate consistently.

  The N:1 load sharing on ams- interfaces is stateless. After a failover from one multiservice interface that encounters a fault to another multiservice interface in the ams group, the state is rebuilt on the multiservice interface that assumes the role of a primary PIC for the flows that are routed through it. For ms- and rms- interfaces, the collection of statistics entries in the bulk statistics file is performed using the statistics reports received from the multiservice PICs. For the ams- interfaces, this method of retrieval and storage of statistics is not possible because of multiple PICs containing statistics for the same subscriber. For interfaces in an ams group, statistics from the different multiservice PICs in the ams group are collected and aggregated on the Routing Engine. On the Routing Engine, a timer control is activated and statistics are saved in the bulkstats file based on this timer. This method of collection causes the statistics records in the bulkstats file to be displayed with a small delay period.

  NOTE: L-PDF uses the Berkerley database for management of configured settings. Because Junos OS Release 12.1 uses a database format that is different from the Berkerley database, when you upgrade from a Junos OS release that uses the Berkerley database to a Junos OS release in which L-PDF is supported on aggregated multiservices interfaces, the previously stored settings in the database are deleted along with the statistical details.

[*Services Interfaces*]

- **NAT with deterministic port block allocation**—You can configure NAT algorithm-based allocation of blocks of destination ports. By specifying this method, you ensure that an incoming (source) IP address and port always maps to the same destination IP address and port, thus eliminating the need for the logging of address translations. Other benefits include:
  - Configuration of source IP address prefix matching in the **from** clause of a NAT rule provides a high degree of scalability.
  - Junos OS -supported ALGs, including FTP, RTSP, ICMP, PPTP, and SIP, are supported.

  To configure deterministic port block allocation, include the **deterministic-port-block-allocation block-size *block-size*** statement at the **[edit services nat pool *pool-name* port]** hierarchy level and include the **translation-type deterministic-napt44** statement at the **[edit services nat rule *rule-name* term *term-name* then translated]** hierarchy level.

  You can use the following new commands to display information:
  - **show services nat deterministic-nat nat-port-block internal-host *ip-address***
  - **show services nat deterministic-nat internal-host nat-address *ip-address* nat-port *port-number***

- **Distributed PPM support for LACP (T Series and M320 routers)**—Enables you to switch between distributed and centralized periodic packet management (PPM). By default distributed PPM is active. To enable centralized PPM, include the **ppm centralized** statement at the **[edit interfaces *interface-name* fastether-options 802.3ad lacp]** hierarchy level or the **[edit interfaces *interface-name* gigether-options 802.3ad lacp]** hierarchy level. To reenable distributed PPM, include the **ppm distributed** statement at the **[edit interfaces *interface-name* fastether-options 802.3ad lacp]** hierarchy level or the **[edit interfaces *interface-name* gigether-options 802.3ad lacp]** hierarchy level. You can use the **show lacp interfaces** command to display LACP Statistics output.

  [*Ethernet Interfaces*, *Interfaces Command Reference*]

- **Support for reducing APS switchover time in Layer 2 Circuits (M320 routers with Channelized OC3/STM1 Circuit Emulation PIC with SFP)**—Starting in Junos OS Release 12.1, you can configure the **fast-aps-switch** statement at the **[edit interfaces *interface-name* sonet-options aps]** hierarchy level. The **fast-aps-switch** statement can be configured on M320 routers with Channelized OC3/STM1 Circuit Emulation PIC with SFP to reduce the Automatic Protection Switching (APS) switchover time in Layer 2 circuits only. Additionally, to achieve reduction in the APS switchover time, the Layer 2 circuit encapsulation type for the interface receiving traffic from a Layer 2 circuit neighbor must be Structure Agnostic Time Division Multiplexing (TDM) over Packet (SAToP).

  NOTE: The fast-aps-switch statement must be configured on both working and protect circuits.

The output of the **show l2circuit connections** operational command now includes the **APS-active** and **APS-inactive** flags. These flags indicate the APS state of the interface. The **APS-active** flag indicates that the interface belongs to the working path. Similarly, the **APS-inactive** flag indicates that the interface belongs to the protective path.

[*Interfaces Command Reference*, *VPNs*]

Junos OS XML API and Scripting

- **Event policy support for configuration changes using Junos OS configuration mode commands**—Starting with Junos OS Release 12.1, you can configure an event policy to modify the configuration using Junos OS configuration mode commands and then commit the updated configuration. To configure an event policy to modify the configuration, include the **change-configuration** statement at the **[edit event-options policy *policy-name* then]** hierarchy level, and specify the configuration mode commands that are executed upon receipt of one or more configured events. The commands are executed in the order in which they appear in the event policy configuration. The commands update the candidate configuration, which is then committed, provided that no commit errors occur.

  Configure the **commit-options** child statement to customize the event policy commit operation. Configure the **retry** statement to have the system attempt the change configuration event policy action a specified number of times if the first attempt fails. The **user-name** statement specifies the user under whose privileges the configuration changes and commit are made.

  [*Junos OS Configuration and Operations Automation Guide*]

- **Event policy support to override the system log priority of the triggering event**—Starting with Junos OS Release 12.1, you can configure an event policy to override the default system log priority of a triggering event so that the system logs the event with a different facility type, severity level, or both. To override the priority of the triggering event, configure the **priority-override** statement at the **[edit event-options policy *policy-name* then]** hierarchy level. To override the facility type with which the triggering event is logged, include the **facility** statement and the new facility type. To override the severity level with which the triggering event is logged, include the **severity** statement and the new severity level.

  [*Junos OS Configuration and Operations Automation Guide*]

Layer 2 Ethernet Services

- **Support for Layer 2 Ethernet interface service features on T4000 routers**—Starting with Junos OS Release 12.1, all Layer 2 features are supported on T4000 routers, with the following exceptions:

- Media access control (MAC) filtering .

NOTE: Because destination MAC filtering is not supported, the hardware is configured to accept all the multicast packets. This enables the OSPF protocol to work.

- MAC learning.
- MAC policing.
- MAC accounting.

[*Network Interfaces*]

MPLS Applications

- **Nonstop active routing support for RSVP point-to-multipoint ingress LSPs**—Starting Release 12.1, Junos OS extends the nonstop active routing support to RSVP point-to-multipoint ingress LSPs. Nonstop routing support for RSVP point-to-multipoint egress and transit routers was added in Junos OS Release 11.4.

  During the switchover, the LSP comes up on the backup Routing Engine that shares and synchronizes the state information with the master Routing Engine before and after the switchover. Nonstop active routing support for point-to-multipoint LSPs ensures that the switchover remains transparent to the network neighbors, and preserves the LSP information across the switchover.

  However, the Junos OS nonstop active routing support for RSVP point-to-multipoint LSPs does not include support for dynamically created point-to-multipoint LSPs, such as VPLS and next-generation MVPNs.

  [*MPLS*]

- **MPLS label removal on T Series routers**—T Series routers in passive-monitor-mode now support removing up to five MPLS labels.

  [*MPLS*]

- **MPLS Transport Profile (MPLS-TP)**—The MPLS Transport Profile (MPLS-TP) introduces new capabilities for operations and management (OAM) when MPLS is used for transport services and transport network operations. This includes a generic mechanism to send OAM messages. This mechanism contains two main components:

  Generic Alert Label (GAL)—A special label that enables an exception mechanism that informs the egress label-switching router (LSR) that a packet it receives on an LSP belongs to an associated control channel or the control plane.

  Generic Associated Control Channel Header (G-Ach)—A special header field that identifies the type of payload contained in the MPLS label-switched paths (LSPs). G-Ach has the same format as a pseudo-wire associated control channel header.

  For more information about MPLS-TP, see RFC 5654, *Requirements of an MPLS Transport Profile*. For more information about GAL and G-Ach, see RFC 5586, *MPLS Generic Associated Channel*.

The following capabilities are supported in the Junos OS implementation of MPLS-TP:

- MPLS-TP OAM can send and receive packets with GAL and G-Ach, without IP encapsulation.
- Two unidirectional RSVP LSPs between a pair of routers can be associated with each other to create an associated bidirectional LSP for binding a path for the GAL and G-Ach OAM messages. The associated bidirectional LSP model is only supported for associating the primary paths. A single Bidirectional Forwarding Detection (BFD) session is established for the associated bidirectional LSP.

The current Junos OS implementation of MPLS-TP does not support:

- P2MP RSVP LSPs and BGP LSPs
- Loss Measurement (LM) and Delay Measurement (DM)

To enable GAL/G-Ach OAM operation without IP encapsulation on all LSPs, include the **mpls-tp-mode** configuration statement at the **[edit protocols mpls oam]** hierarchy level.

```
[edit protocols mpls oam]
mpls-tp-mode;
```

To enable GAL/G-Ach OAM operation without IP encapsulation on a specific LSP, include the **mpls-tp-mode** statement at the **[edit protocols mpls label-switched-path *lsp-name* oam]** hierarchy level.

```
[edit protocols mpls label-switched-path lsp-name oam]
mpls-tp-mode;
```

NOTE: Include this statement at the **[edit protocols mpls oam]** hierarchy level only if all the LSPs are point-to-point LSPs.

To configure associated LSPs on the two ends of the LSP, include the **associate-lsp *lsp-name* from *from-address*** statement at the **[edit protocols mpls lsp *lsp-name*]** hierarchy level:

```
[edit protocols mpls lsp lsp-name oam]
associate-lsp lsp-name {
   from from-ip-address;
}
```

The **from *from-address*** configuration for the LSP is optional. If omitted, it is derived from the **to** address of the LSP configuration.

To associate two LSPs at a transit router, include the **transit-lsp-association** statement at the **[edit protocols mpls]** hierarchy level:

```
[edit protocols mpls]
transit-lsp-association transit-association-lsp-group-name {
   lsp-name-1 name-of-associated-lsp-1;
   from-1 address-of-associated-lsp-1;
   lsp-name-2 name-of-associated-lsp-2;
   from-2 address-of-associated-lsp-2;
}
```

The association in the transit nodes is useful for the return LSP path for TTL-expired LSP ping packets or traceroute.

To view details of associated-bidirectional LSPs, issue the **show mpls lsp** command. To view detailed information, issue the command with the **detail** or **extensive** option. In addition, you can also use the **show mpls lsp bidirectional** command to view associated bi-directional LSP information.

[*MPLS*]

- **MPLS support on Type 5 FPC (T4000 routers)**—Starting with Junos OS Release 12.1, MPLS support is extended to the Type 5 FPC on T4000 Core Routers.

  The existing MPLS labels **push**, **pop**, **swap**, **multiple push**, and **swap and push** are supported on T4000 routers.

  The Type 5 FPC on T4000 routers supports the following features, which are also supported on aggregated Ethernet interfaces:

  - Layer 2 VPNs, Layer 2 circuits, and Layer 2 switching cross-connects (with circuit cross-connect (CCC) and VLAN CCC encapsulation)
  - Layer 3 VPNs applicable on IPv4 and IPv6 routes:
    - With a Tunnel Services PIC
    - With the **vrf-table-label** statement with LSI and no Tunnel Services PIC
    - With per-prefix load balancing with no Tunnel Services PIC
  - Interprovider and carrier-of-carriers VPNs and BGP MPLS multicast VPNs
  - MPLS LSP tunnel cross-connects and LSP stitching cross-connects
  - Ethernet translational cross-connect (TCC) and VLAN TCC encapsulation
  - IPv4, MPLS, and ISO packets for TCC
  - Point-to-multipoint CCC support (ingress and egress) using RSVP point-to-multipoint LSPs
  - Class-of-service (CoS)-based features such as:
    - MPLS EXP classification and rewrites
    - Fixed-CoS value for a label-switched path (LSP) and RSVP bypass LSPs
    - CoS-based forwarding support for MPLS
  - LDP-signaled LSPs, LSP accounting, LSP policers
  - LSP ping and traceroute, which includes LSP traceroute for LDP LSPs with equal-cost multipath (ECMP) support
  - RSVP-signaled LSPs

- RSVP-signaled point-to-multipoint LSPs, which includes link protection for the LSPs, and maximum transmission unit (MTU) signaling in RSVP
- MPLS fast reroute, node protection, and link protection
- Time to live (TTL) propagation and explicit NULL label support (ultimate-hop popping) for IPv4 and IPv6
- MPLS load balancing based on IP header and MPLS labels
- Static and explicit-path LSP, including support for **push** label and **swap-push** label operations
- MPLS over GRE tunnels and IPv6 tunnels over MPLS
- MPLS firewall filters
- Generalized MPLS (GMPLS)
- Source class usage (SCU) on label-switched interfaces (LSIs)
- Diffserv-aware traffic engineering

All the MPLS features that are currently supported on existing T Series Core Routers are also supported on the T4000 routers.

[*MPLS*]

Multicast

- **Bidirectional PIM (RFC 5015) (M120, M320, MX Series, and T Series routers)**—Provides an alternative to other PIM modes, such as PIM sparse mode (PIM-SM), PIM dense mode (PIM-DM), and PIM source-specific multicast (SSM). In bidirectional PIM, multicast groups are carried across the network over bidirectional shared trees. This type of tree minimizes the amount of PIM routing state information that must be maintained, which is especially important in networks with numerous and dispersed senders and receivers.

  To configure designated forwarder election parameters, include the **bidirectional** statement and child statements at the **[edit protocols pim interface *interface-name* | all]** hierarchy level. To configure the PIM mode, include the **bidirectional-sparse** or **bidirectional-sparse-dense** statement at the **[edit protocols pim interface (*interface-name* | all) mode]** hierarchy level. To configure tracing operations, include the **bidirectional-df-election** statement at the **[edit protocols pim traceoptions flag]** hierarchy level. To configure an RP address, include an IP address at the **[edit protocols pim rp bidirectional address]** hierarchy level.

  Useful monitoring and troubleshooting commands include all of the existing **show pim...**, **show route...**, and **show multicast...** commands, plus the new **show pim bidirectional df-election** command.

  [*Multicast Protocols*]

- **Support for unicast RPF loose mode (T Series routers)**—Extends support for unicast reverse path forwarding (unicast RPF) loose mode with the ability to discard packets with the source address pointing to the discard interface, on the Type 1 FPC, Type 2 FPC, and Type 3 FPC on T Series routers. This feature, in conjunction with Remote Triggered Black Hole (RTBH) filtering, provides a mechanism to discard packets from untrusted sources. BGP policies in edge routers ensure that packets with untrusted source addresses have their next hop set to a discard route. When a packet arrives at the router with an untrusted source address, unicast RPF performs a route lookup of the source address. Because the source address route points to a discard next hop, the packet is dropped. This feature is supported only on the IPv4 (**inet**) address family.

  To configure unicast RPF loose mode with the ability to discard packets, you can use the **rpf-loose-mode-discard inet** statement at the **[edit forwarding options]** hierarchy level. Use the **show interfaces extensive** operational mode command to view the packet drops.

  [*Interfaces Fundamentals Configuration Guide*]

- **Point-to-multipoint support for RIP**—This feature introduces point-to-multipoint support for RIP. The point-to-multipoint feature enables all interfaces configured with RIP to have multiple peers. The following changes are introduced:

  - The **interface-type p2mp** statement is introduced at the **[edit protocols rip group *group-name* neighbor *neighbor-name*]** hierarchy level and enables an interface to have multiple peers.
  - The **dynamic-peers** statement is introduced at the **[edit protocols rip group *group-name* neighbor *neighbor-name*]** hierarchy level and enables dynamic neighbor discovery on an interface.
  - The **peer *address*** statement is introduced at the **[edit protocols rip group *group-name* neighbor *neighbor-name*]** hierarchy level and configures a peer on an interface.
  - Change in the output of the **show rip neighbors** command. The term local is prefixed to the state column.
  - Additional commands are introduced to view the statistics of all peers or a given peer: **show rip statistics peer all** and **show rip statistics peer *address***.
  - Additional commands are introduced to clear statistics of all peers or a given peer: **clear rip statistics peer all** and **clear rip statistics peer *address***.

Network Management

- **Updated enterprise-specific MIB and support for existing system log messages and operational commands for T4000 routers**—Starting with Junos OS Release 12.1, the following features are supported on T4000 Core Routers:

  - Updated MIB—The Juniper Networks enterprise-specific Chassis MIB provides information about the router and its components. The enterprise-specific Chassis Definitions for Router Model MIB—**jnx-chas-defines.mib**—is updated for T4000 routers with object identifiers (OIDs) that are used by the Chassis MIB to identify platform and chassis components.

- Support for existing system log messages—The following system log messages apply to T4000 routers:
  - CHASSISD_UNSUPPORTED_FPC
  - CHASSISD_UNSUPPORTED_SIB

  The other alarms related to T4000 routers can be viewed by executing the **show chassis alarms** operational command.

On Type 5 FPC on T4000 routers, there are no **top temperature sensor** or **bottom temperature sensor** parameters. Instead, **fan intake temperature sensor** and **fan exhaust temperature sensors** parameters are displayed.

[*System Log Messages Reference*, *SNMP MIBs and Traps Reference*, *Interface Command References*]

- **SNMP MIB support for OSPFv3**—Starting with Release 12.1, Junos OS supports RFC 5643, Management Information Base for OSPFv3, and thus extends the SNMP support to OSPFv3. Junos OS support for RFC 5643 is read-only, and does not include ospfv3HostTable and ospfv3CfgNbrTable.

  [*SNMP MIBs and Traps Reference*]

Routing Protocols

- **New option propagate-ttl for IP traceroute**—The **traceroute** command has a new option **propagate-ttl** that can be used on a PE router to view locally generated Routing Engine transit traffic. This is applicable for MPLS L3VPN traffic only.

  [*Routing Protocols Command Reference*]

- **Support for RFC 4861**—In Junos OS Release 12.1 and later, Junos OS supports Neighbor Discovery features as described in RFC 4861, *Neighbor Discovery for IP version 6 (IPv6)*, along with RFC 5095, *Deprecation of Type 0 Routing Headers in IPv6*, and RFC 4862, *IPv6 Stateless Address Auto Configuration for IPv6*. A new configuration statement, **donot-disable-ip6-op**, introduced at the **[edit system]** hierarchy level, prevents IPv6 operation on an interface from being disabled when the duplicate address detection process fails on link-local addresses that are based on hardware addresses.

  [*System Basics*]

- **Support for Layer 3 features on T4000 routers**—Support for Layer 3 protocols and Layer 3 forwarding is now extended to T4000 routers. Table 10 on page 158 lists the protocols, features, and services supported on T4000 routers.

Table 10: Protocols, Features, and Services Supported on T4000 Routers

Protocols	Features	Services
BGP	Equal-cost multipath (ECMP)	Layer 3 virtual private network (Layer 3 VPN)
OSPF	Loop-free Alternate	Layer 2 virtual private network (Layer 2 VPN)

Table 10: Protocols, Features, and Services Supported on T4000 Routers *(continued)*

Protocols	Features	Services
IS-IS	Unicast reverse path forwarding (unicast RPF)	Layer 2 circuit
RIP		
Bidirectional Forwarding Detection (BFD)		
SNMP		
Address Resolution Protocol (ARP)		
Neighbor Discovery Protocol (NDP)		
RSVP		

[*Routing Protocols*]

- **IEEE 802.3ah OAM functionality extended to 10-Gigabit Ethernet LAN/WAN PIC with SFP+ (T640, T1600, and TX Matrix routers with T640-FPC4-ES, T1600-FPC4-ES, and T640-FPC4-1P-ES)**—Enables you to perform Operation, Administration, and Maintenance (OAM)-related operations such as link fault management and link discovery.

  Support for the following OAM operations on the T Series routers is extended to the 10-Gigabit Ethernet LAN/WAN PIC with SFP+:

  - Link fault management
  - Link discovery
  - Graceful Routing Engine Switchover
  - Layer 2 and Layer 3 control protocol packets (OSPF, OSPF3, VRRP, IGMP, RSVP, PIM, BGP, BFD, LDP, IS-IS, RIP, RIPV6, LACP, ARP, IPv6 NDP, CFM, and LFM) are mapped to the control queue. In the control queue, these packets are not dropped even if there is oversubscription or congestion on a port group.

  NOTE: The following OAM features are not supported on the 10-Gigabit Ethernet LAN/WAN PIC with SFP+:

  - Remote Loopback
  - Unified in-service software upgrade (unified ISSU)

[*Channelized Interfaces*, *Routing Protocols*]

- **IEEE 802.3ag OAM functionality extended to 10-Gigabit Ethernet LAN/WAN PIC with SFP+ (T640, T1600, and TX Matrix routers with T640-FPC4-ES,**

T1600-FPC4-ES, and T640-FPC4-1P-ES)—Enables you to perform Operation, Administration, and Maintenance (OAM)-related operations. Support for the following OAM operations on the T Series routers is extended to the 10-Gigabit Ethernet LAN/WAN PIC with SFP+:

- Connectivity-fault management (CFM)
- Linktrace
- Loopback
- Graceful Routing Engine switchover (GRES)
- Layer 2 and Layer 3 control protocol packets (OSPF, OSPF3, VRRP, IGMP, RSVP, PIM, BGP, BFD, LDP, IS-IS, RIP, RIPV6, LACP, ARP, IPv6 NDP, CFM, and LFM) are mapped to the control queue. In the control queue, these packets are not dropped even if there is oversubscription or congestion on a port group.

NOTE: OAM unified in-service software upgrade (unified ISSU) is not supported on the 10-Gigabit Ethernet LAN/WAN PIC with SFP+.

[*Channelized Interfaces*, *Routing Protocols*]

- **Accumulated IGP Attribute for BGP**—Enables deployment in which a single administration can run several contiguous BGP autonomous systems. Such deployments allow BGP to make routing decisions based on the IGP metric. In such networks, it becomes possible for BGP to select paths based on metrics as is done by IGPs. In this case, BGP chooses the shortest path between two nodes, even though the nodes might be in two different autonomous systems. To enable accumulated IGP processing, include the **aigp** statement in the BGP configuration on a protocol family basis. Junos OS supports accumulated IGP for **family inet labeled-unicast** and f**amily inet6 labeled-unicast**. The **aigp** statement can be configured for a given family at the global BGP, group, or neighbor level. By default, the value of the AIGP attribute for a local prefix is zero. An AIGP-enabled neighbor can originate an AIGP attribute for a given prefix by export policy, using the **aigp-originate** policy action. The value of the AIGP attribute reflects the IGP distance to the prefix. Alternatively, you can specify a value, by using the **aigp-originate distance *distance*** policy action.

  [*Routing Protocols*]

- **Point-to-multipoint support for RIP**—The demand circuit (DC) feature implementation in RIP required the use of a single RIP peer. The point-to-multipoint feature enables a RIP device to have multiple peers on an interface irrespective of whether it uses demand circuits. To enable this feature, include:
  - The **interface-type p2mp** statement at the **[edit protocols rip group *group-name* neighbor *interface-name*]** hierarchy level to enable the neighbor to function as a point-to-multipoint endpoint.
  - The **dynamic-peers** statement at the **[edit protocols rip group *group-name* neighbor *interface-name*]** hierarchy level to enable or disable dynamic peer discovery at the neighbor level.

- The **peer *address*** statement at the **[edit protocols rip group *group-name* neighbor *interface-name*]** hierarchy level to manually configure peers.

As a result of this feature, the following **show** commands have been introduced to view the statistics of all peers or a given peer.

- **show rip statistics peer all**
- **show rip statistics peer *address***

As a result of this feature, the following clear commands have been introduced to clear the statistics of all peers or a given peer.

- **clear rip statistics peer all**
- **clear rip statistics peer *address***

[*Routing Protocols*]

Subscriber Access Management

- **Junos OS subscriber management scaling values (M120, M320, and MX Series routers)**—A spreadsheet is available online that lists scaling values supported for Junos OS subscriber management beginning with Junos OS Release 10.1. Access the *Subscriber Management Scaling Values (XLS)* spreadsheet from the Downloads box at http://www.juniper.net/techpubs/en_US/junos*release-number*/information-products/pathway-pages/subscriber-access/index.html. Substitute the number of the latest Junos OS release for the *release-number*. For example, **...en_us/junos11.1/...**.

  [*Subscriber Management Scaling*]

- **Delay in removing subscriber routes after graceful Routing Engine switchover (M120, M320, and MX Series routers)**—For a subscriber network in which either nonstop active routing (NSR) or graceful restart has been configured, you can configure the router to wait for 180 seconds (3 minutes) before removing access routes and access-internal routes after a graceful Routing Engine switchover (GRES) takes place.

  This 3-minute delay provides sufficient time for the appropriate client process (jpppd or jdhcpd) or routing protocol process to reinstall the access routes and access-internal routes before the router removes the stale routes from the forwarding table. As a result, the risk of traffic loss is minimized because the router always has available subscriber routes.

  To configure the router to wait for 180 seconds before removing (flushing) access-routes and access-internal routes after a graceful Routing Engine switchover, include the **gres-route-flush-delay** statement at the **[edit system services subscriber-management]** hierarchy level.

  Using the **gres-route-flush-delay** statement in your subscriber management configuration offers the following benefits:

  - Provides sufficient time to reinstall subscriber routes from the previously active Routing Engine

In subscriber networks with graceful restart and routing protocols such as BGP and OSPF configured, the router purges any remaining stale routes as soon as the graceful restart operation completes, which can occur very soon after completion of the graceful Routing Engine switchover. Using the **gres-route-flush-delay** statement causes the router to retain the stale routes for a full 180 seconds, which provides sufficient time for the jpppd or jdhcpd client process to reinstall all of the subscriber routes.

- Prevents loss of subscriber traffic due to unavailable routes

  In subscriber networks with nonstop active routing and routing protocols such as BGP and OSPF configured, the routing protocol process immediately purges the stale routes that correspond to subscriber routes. This removal results in a loss of subscriber traffic. Using the **gres-route-flush-delay** statement causes the router to retain the stale routes for a full 180 seconds, which prevents potential traffic loss due to unavailable routes.

[*Junos OS Subscriber Access Configuration Guide*]

- **Configuring retransmission of L2TP control messages (MX Series 3D Universal Edge Routers)**—L2TP peers maintain a queue of control messages that must be sent to the peer device. After a message is sent, the local peer waits for a response from the remote peer. If a response is not received, the local peer retransmits the message. You can configure how many times an unacknowledged message is retransmitted by the LAC or the LNS. For tunnels that have been established, include the **retransmission-count-established** statement at the **[edit services l2tp tunnel]** hierarchy level. For tunnels that are not yet established, include the **retransmission-count-not-established** statement.

  You can specify a maximum count in the range 0 through 30. The default count for established tunnels is 7; for not-established tunnels, the default is 5. The local peer waits one second for the first response to a control message. The retransmit timer then doubles the interval between each successive retransmission, up to a maximum interval of 16 seconds. This behavior allows the remote peer more time to respond. If the maximum retransmission count is reached and no response has been received, the tunnel and all its sessions are cleared.

  BEST PRACTICE: Before you downgrade to a Junos OS release that does not support these statements, we recommend that you explicitly unconfigure the feature by including the **no retransmission-count-established** statement and the **no retransmission-count-non-established** statement at the **[edit services l2tp tunnel]** hierarchy level.

  BEST PRACTICE: During a unified in-service software upgrade (ISSU) on an MX Series router configured as the LAC, the LAC might not respond to control messages from the LNS. This can result in dropping LAC L2TP sessions. You can avoid this situation by ensuring that the maximum retransmission count on the LNS is set to 16 or higher.

[*Subscriber Access*]

- **Configuring the idle timeout for L2TP tunnels without sessions (MX Series 3D Universal Edge Routers)**—You can configure the LAC or the LNS to specify how long a tunnel without any sessions remains active. The idle timer starts when the last session on the tunnel is terminated. When the timer expires the tunnel is disconnected. This idle timeout frees up resources otherwise consumed by inactive tunnels.

  To configure how long the tunnel remains active, include the **idle-timeout** statement at the **[edit services l2tp tunnel]** hierarchy level. You can set the timer in the range 0 through 86,400 seconds; the default value is 80 seconds. If you set the idle-timeout value to 0, the tunnel is forced to remain active indefinitely after the last session is terminated until one of the following occurs:

  - You issue the **clear services l2tp tunnel** command.
  - The remote peer disconnects the tunnel.

  BEST PRACTICE: **Before you downgrade to a Junos OS release that does not support this statement, we recommend that you explicitly unconfigure the feature by including the no idle-timeout statement at the [edit services l2tp tunnel] hierarchy level.**

[*Subscriber Access*]

- **Configuring how long L2TP maintains dynamic information (MX Series 3D Universal Edge Routers)**—You can configure the LAC or the LNS to specify how long the router attempts to maintain dynamic destinations, tunnels, and sessions after they have been torn down. This *destruct* timeout aids debugging and other analysis by saving underlying memory structures of those destinations, tunnels, or sessions. Any specific dynamic destination, tunnel, or session may not be maintained for this entire time period if the resources must be reclaimed early to allow new tunnels to be established. To set the destruct timeout, include the **destruct-timeout** statement at the **[edit services l2tp** hierarchy level. You can set the timer in the range 10 through 3600 seconds; the default value is 300 seconds.

  BEST PRACTICE: **Before you downgrade to a Junos OS release that does not support this statement, we recommend that you explicitly unconfigure the feature by including the no destruct-timeout statement at the [edit services l2tp] hierarchy level.**

[*Subscriber Access*]

- **Support for shaping rate and overhead accounting on dynamic subscriber interfaces based on access line parameters in PPPoE discovery packets (MX Series routers)**—Enables you to configure access line parameters in PPPoE discovery packets to set the shaping rate and overhead accounting attributes on dynamic subscriber interfaces in a broadband access network. This feature is supported on MPC/MIC interfaces on MX Series routers.

When you enable this feature, the values supplied by the PPPoE vendor-specific tags override the parameters that you have configured for **shaping-rate** and **overhead-accounting** statements at the **[edit dynamic-profiles profile-name class-of-service traffic-control-profile]** hierarchy level.

The shaping rate is based on the actual data rate downstream attribute, and is only overridden if the vendor specific-tag value is less than the configured value. The overhead accounting value is based on the access loop encapsulation attribute and specifies whether the access loop uses Ethernet (frame mode) or ATM (cell mode).

You can mix ANCP and PPPoE vendor-specific tags for dynamically instantiated static and interface sets so that the shaping rate is first using PPPoE vendor-specific tags and is later adjusted by ANCP. In this case, the shaping rate value overrides the PPPoE value.

To enable this feature, include the **actual-data-rate-downstream** or **access-loop-encapsulation** option with the **vendor-specific-tags** statement at the **[edit dynamic-profiles *profile-name* class-of-service dynamic-class-of-service-options]** hierarchy level.

[*Subscriber Access*, *Class of Service*]

- **Support for processing subscriber-initiated PPP fast keepalive requests (MX Series routers with MPCs/MICs)**—Enables the Packet Forwarding Engine on an MPC/MIC in an MX Series router to process and respond to Link Control Protocol (LCP) Echo-Request packets that the PPP subscriber (client) initiates and sends to the router. LCP Echo-Request packets and LCP Echo-Reply packets are part of the PPP keepalive mechanism that helps determine whether a link is functioning properly.

  In earlier Junos OS releases, processing of LCP Echo-Request packets and LCP Echo-Reply packets was handled by the Routing Engine. In the current release, the Packet Forwarding Engine on the MPC/MIC receives LCP Echo-Request packets from the PPP subscriber and transmits LCP Echo-Reply packets in response, without having to send the LCP packets to the Routing Engine for processing. The mechanism by which LCP Echo-Request packets are processed by the Packet Forwarding Engine instead of by the Routing Engine is referred to as *PPP fast keepalive*. Transmission of keepalive requests from the Packet Forwarding Engine on the router is not enabled in the current release.

  Relieving the Routing Engine of having to process LCP Echo-Request packets provides increased bandwidth on the router to support a larger number of subscribers with improved performance.

  No special configuration is required on an MX Series router with MPCs/MICs to enable processing of PPP fast keepalive requests on the Packet Forwarding Engine. The feature is enabled by default, and cannot be disabled.

  When you issue the **show interfaces pp0.*logical* statistics** operational command to display interface statistics, the display does not include the number of keepalive packets processed or the amount of time since the router processed the last keepalive packet.

  [*Junos OS Subscriber Access Configuration Guide*]

- **Support for DHCP Subscriber IP Session BFD Liveness Detection**—Liveness detection for DHCP subscriber IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

  You can configure DHCP liveness detection either globally or per DHCPv4 or DHCPv6 group. To configure liveness detection, include the **liveness-detection** statement at the following hierarchy levels:

  [edit system services dhcp-local-server],
  [edit system services dhcp-local-server dhcpv6],
  [edit forwarding-options dhcp-relay],
  [edit forwarding-options dhcp-relay dhcpv6]
  [edit system services dhcp-local-server group *group-name*],
  [edit system services dhcp-local-server dhcpv6 group *group-name*],
  [edit forwarding-options dhcp-relay group *group-name*],
  [edit forwarding-options dhcp-relay dhcpv6 group *group-name*]

  In Junos OS Release 12.1, the only method supported for liveness detection is Bidirectional Forwarding Detection (BFD). To configure BFD as the liveness detection method, include the **bfd** statement at the following hierarchy levels:

  [edit system services dhcp-local-server liveness-detection method],
  [edit system services dhcp-local-server dhcpv6 liveness-detection method],
  [edit forwarding-options dhcp-relay liveness-detection method],
  [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method],
  [edit system services dhcp-local-server group *group-name* liveness-detection method],
  [edit system services dhcp-local-server dhcpv6 group *group-name* liveness-detection method],
  [edit forwarding-options dhcp-relay group *group-name* liveness-detection method],
  [edit forwarding-options dhcp-relay dhcpv6 group *group-name* liveness-detection method]

  At the **bfd** hierarchy level, you can configure any of the following BFD-related statements:

  - **detection-time**
  - **holddown-interval**
  - **minimum-interval**
  - **minimum-receive-interval**
  - **multiplier**
  - **no-adaptation**
  - **session-mode**
  - **transmit-interval**
  - **version**

  After configuring the liveness detection method, configure the action the router takes when a liveness detection failure occurs by including the **failure-action** statement at the following hierarchy levels:

  [edit system services dhcp-local-server liveness-detection],
  [edit system services dhcp-local-server dhcpv6 liveness-detection],
  [edit system services dhcp-relay liveness-detection],
  [edit system services dhcp-relay dhcpv6 liveness-detection],
  [edit system services dhcp-local-server group *group-name* liveness-detection],

[edit system services dhcp-local-server dhcpv6 group *group-name* liveness-detection],
[edit system services dhcp-relay group *group-name* liveness-detection],
[edit system services dhcp-relay dhcpv6 group *group-name* liveness-detection]

You can choose from the following three options when configuring a liveness detection failure option:

- **clear-binding**—The client session is cleared when a liveness detection failure occurs.
- **clear-binding-if-interface-up**—The client session is cleared only when a liveness detection failure occurs and the local interface is detected as being up.
- **log-only**—A message is logged to indicate the event; no action is taken and DHCP is left to manage the failure.

[*Subscriber Access*]

- **DHCPv6 Rapid Commit (M120, M320, and MX Series routers)**—The extended DHCPv6 local server supports the DHCPv6 Rapid Commit option (DHCPv6 option 14). When rapid commit is enabled on the extended DHCPv6 local server, the server supports a two-message exchange (Solicit and Reply) to configure clients , rather than the traditional four-method exchange (Solicit, Advertise, Request, and Reply). The two-message exchange provides faster client configuration, which is useful in environments in which client attachment points frequently change, such as mobile networks.

  You can configure the DHCPv6 local server to support the Rapid Commit option globally, for a specific group, or for a specific interface. The DHCP client must also be configured to include the DHCPv6 Rapid Commit option in the Solicit messages sent to the DHCP local server.

  To configure DHCP local server to support rapid commit, use the **rapid-commit** statement at the [**edit dhcp-local-server dhcpv6 overrides**] hierarchy level for global configuration, at the [**edit dhcp-local-server dhcpv6 group *group-name* overrides**] hierarchy level for group configurations, or at the [**edit dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides**] hierarchy level for interface-specific configurations.

  [*Subscriber Access*]

- **Support for interface-style services for PPPoE subscribers**—Starting with Junos OS Release 12.1, all interface-style services are supported for dynamic Point-to-Point Protocol over Ethernet (PPPoE) subscribers on all MX Series routers with modular Modular Port Concentrators (MPCs).

  [*Services Interfaces*]

- **Support for rewrite rules and classifiers on Ethernet pseudowires (MX Series routers)**—Enables you to configure rewrite rules and classifiers on Ethernet pseudowires that are configured on logical tunnel interfaces. This feature is supported on MPC/MIC modules on MX Series routers.

  Logical interfaces such as **lt-*fpc/pic/port***, which are required to configure this feature, are created while configuring tunnel services for the router (using the **set chassis** command). For example, the **set chassis fpc 4 pic 0 tunnel-services** command creates

a tunnel interface lt-4/0/0. You must then specify the Ethernet encapsulation type and **inet** as the family on the lt interface to configure this feature.

To configure the CoS parameters, include the **rewrite-rules** and **classifier** statements at the **[edit class-of-service]** hierarchy level. You can specify **inet-precedence** or **dscp** as the rewrite rule or the classification type.

You can use logical tunnel interfaces to create pseudowires by connecting two virtual routing forwarding (VRF) instances. A pseudowire can be used to represent a single subscriber (for example, a business subscriber).

[*Class of Service*, *Subscriber Access*]

- **Support for RADIUS attribute Local-Loopback-Interface for L2TP**—With Junos OS Release 12.1, the RADIUS attribute Local-Loopback-Interface [26-3] is now supported for an L2TP LAC configured on an MX Series router.

  You can configure the Local-Loopback-Interface attribute on a RADIUS server to manage multiple LAC devices. This attribute is used as the LAC source address on an LNS tunnel for PPPoE subscribers tunneled over L2TP.

  When you use the Tunnel-Client-Endpoint attribute as the LAC source address, you must configure the Tunnel-Client-Endpoint attribute for each MX Series router that uses the same RADIUS server. Starting with Junos OS Release 12.1, you can use the Local-Loopback-Interface attribute, which needs to be configured only once.

  When the LAC initiates an Access-Request message to RADIUS for authentication, RADIUS returns the Local-Loopback-Interface attribute in the Access-Accept message. This attribute contains the name of the loopback interface, either as a generic interface name such as “lo0” or as a specific name like “lo0.0” The MX Series router then uses the configured loopback interface IP address as the source address during tunnel negotiation with the LNS.

  [*Broadband Subscriber Management Solutions*]

- **Support for removing inactive dynamic subscriber VLANs (MX Series routers)**—Junos OS Release 12.1 supports the removal of dynamic subscriber VLANs when an inactivity threshold has been reached. To define the threshold at which a subscriber VLAN is removed, include the **client-idle-timeout** statement, along with the timeout value (from 10 through 1440 minutes), at the **[edit access profile *profile-name* session-options]** hierarchy level. The **client-idle-timeout** value specifies a maximum period of time that the subscriber can be idle. By default, no timeout is present.

  In addition to removing inactive dynamic subscriber VLANS, the **client-idle-timeout** statement removes dynamic VLANs if no client sessions are ever created (for example, due to inactivity or error during creation or authentication).

  When configuring dynamic VLAN removal upon inactivity timeout, keep the following in mind:

  - The idle timeout period begins after a dynamic subscriber VLAN interface is created or traffic activity stops on a dynamic subscriber VLAN interface.
  - If a new connection is created or a client session is reactivated successfully, the client idle timeout resets.

- The removal of inactive subscriber VLANs functions only with VLANs that have been authenticated.

[*Subscriber Access*, *Network Interfaces*]

- **Support for PTSP application on aggregated and redundant service PICs**—You can configure packet-triggered subscribers and policy control (PTSP) feature on aggregated multiservices (ams) and redundant multiservices (rms) interfaces. For the PTSP functionality, you can use a 1:1 redundancy model to pair two services PICs in high availability mode using a virtual redundant Multiservices PIC (rms) interface. You can also employ an N:1 redundancy mechanism to cluster together N number of ms- interfaces in an ams group that supports load sharing for PTSP subscribers.

  With service PICs configured as rms interfaces, if a failover of a service PIC occurs, the subscribers on the failed service PIC are logged out, and the traffic is switched over to the redundant service PIC that initiates the subscribers to log in again.

  With multiservices interfaces configured in an ams group and traffic distributed over the service PICs in the ams group, the traffic of subscribers that are logged in to PTSP partitions on a particular service PIC is redistributed to other service PICs in the ams group. Such a replication of subscriber traffic for PTSP partitions enables the same subscriber detail to be present on different service PICs. In such a scenario, when one of the service PIC fails, the subscribers that are logged in over that PIC remain connected; the sessions are terminated only when the subscriber logs out or the idle timeout period is exceeded.

  [*Subscriber Access*]

- **Enhanced show binding and clear binding commands for DHCP local server and DHCP relay agent (MX Series routers)**—The **show binding** and **clear binding** commands for extended DHCP local server and extended DHCP relay agent (including DHCPv6) have been enhanced to include additional options, which enable you to display or clear DHCP binding information by FPC, PIC, port, VLAN, and S-VLAN. The new options are supported on all underlying interfaces that support DHCP bindings.

  The enhancement includes the following two new options:

  - *<interfaces-vlan>*—The interface VLAN ID and S-VLAN ID on which to show or clear bindings.
  - *<interfaces-wildcard>*—The set of interfaces on which to show or clear bindings. This option supports the use of the wildcard character (*), which enables you to identify interfaces based on FPC, PIC, and port.

  The new options are supported by the operational commands shown in Table 11 on page 168.

Table 11: Supported show and clear Commands

show dhcp server binding	show dhcp relay binding
show dhcpv6 server binding	show dhcpv6 relay binding
clear dhcp server binding	clear dhcp relay binding

Table 11: Supported show and clear Commands *(continued)*

clear dhcpv6 server binding	**clear dhcpv6 relay binding**

The following examples show sample commands that use the new options.

NOTE: IP demux interfaces are not supported by the show and clear DHCP bindings commands for DHCP local server and DHCP relay agent.

[*Subscriber Access*]

- **DHCPv6 relay agent support for DHCP snooping (M120, M320, and MX Series routers)**—Extends support for DHCP snooping to the DHCPv6 relay agent configured on the router. In multi-relay topologies where more than one DHCPv6 relay agent is between the IPv6 client and the DHCPv6 server, snooping enables intervening DHCPv6 relay agents between the client and the server to correctly receive and process the unicast traffic from the client and forward it to the DHCPv6 server.

  The DHCPv6 relay agent snoops incoming unicast DHCPv6 packets by setting up a filter with UDP port 547 (the DHCPv6 UDP server port) on a per-forwarding table basis. The DHCPv6 relay agent then processes the packets intercepted by the filter and forwards the packets to the DHCPv6 server.

  DHCPv6 relay agent snooping is disabled on the router by default. You can override the default DHCPv6 snooping configuration to explicitly enable or disable DHCPv6 snooping.

  To enable snooping for the DHCPv6 relay agent, do one of the following:

  - To enable DHCPv6 snooping support globally, include the **allow-snooped-clients** statement at the **[edit forwarding-options dhcp-relay dhcpv6 overrides]** hierarchy level.
  - To enable DHCPv6 snooping support for a named group of interfaces, include the **allow-snooped-clients** statement at the **[edit forwarding-options dhcp-relay dhcpv6 group *group-name* overrides]** hierarchy level.
  - To enable DHCPv6 snooping support for a specific interface within a named group of interfaces, include the **allow-snooped-clients** statement at the **[edit forwarding-options dhcp-relay dhcpv6 group *group-name* interface *interface-name* overrides]** hierarchy level.

  To disable snooping for the DHCPv6 relay agent after you have enabled it, do one of the following:

  - To disable DHCPv6 snooping support globally, include the **no-allow-snooped-clients** statement at the **[edit forwarding-options dhcp-relay dhcpv6 overrides]** hierarchy level.
  - To disable DHCPv6 snooping support for a named group of interfaces, include the **no-allow-snooped-clients** statement at the **[edit forwarding-options dhcp-relay dhcpv6 group *group-name* overrides]** hierarchy level.

- To disable DHCPv6 snooping support for a specific interface within a named group of interfaces, include the **no-allow-snooped-clients** statement at the **[edit forwarding-options dhcp-relay dhcpv6 group *group-name* interface *interface-name* overrides]** hierarchy level.

[*Junos OS Subscriber Access Configuration Guide*]

- **Offload status for PTSP and local L-PDF flows**—Starting with Junos OS Release 12.1, the **show services application-aware-access-list flows subscriber *subscriber-name*** and **show services subscriber flows client-id *client-id*** commands display flow offload status for each flow. Offloading is supported only on MX Series routers with Modular Port Concentrators (MPCs) by the packet-triggered subscribers and policy control (PTSP) and local L-PDF plug-ins. No configuration is necessary to enable offloading.

  [*Services Interfaces*]

- **EX Series switches support the CLI edit mode wildcard range command**—The **wildcard range** command allows you to specify ranges in **activate**, **deactivate**, **delete**, **protect**, **set**, **show**, and **unprotect** commands. You can use ranges to specify a range of interfaces, logical units, VLANs, and other numbered elements. The **wildcard range** command expands the command you entered into multiple commands, each of which corresponds to one item in the range. For example, **wildcard range interfaces deactivate ge-0/0/[1-3]** expands to deactivate interfaces **ge-0/0/1**, **ge-0/0/2**, and **ge-0/0/3**.

- **Extended DHCPv4 local server and extended DHCPv4 relay agent and relay proxy support on M120 and M320 routers**—The extended DHCPv4 local server and extended DHCPv4 relay agent and relay proxy features used for subscriber management are supported and qualified on M120 and M320 routers. In addition to the configuration and command support for extended DHCPv4, M120 and M320 routers now support the subscriber management features listed in Table 12 on page 170.

Table 12: Additional Supported Features on M120 and M320 Routers

Ethernet interfaces on the following PICs: • 8-port Gigabit Ethernet IQ2 PIC (Type 3) • 2-port Gigabit Ethernet IQ PIC • 10-Gigabit Ethernet PIC with XENPAK • 10-Gigabit Ethernet IQ2 PIC with XFP	Aggregated Ethernet interfaces
MAC address validation	Service accounting (on FPCs that support bulk statistics)
Change of Authorization (CoA)	Filters (one input and one output filter per VLAN)
Class of Service (CoS), single-shaper per VLAN on IQ2 PICs	Non-default routing instances

Table 13 on page 171 lists subscriber management features that are not supported on M120 and M320 routers.

Table 13: Unsupported Features on M120 and M320 Routers

IP and VLAN demux logical interfaces	Extended DHCPv6 local server and DHCPv6 relay agent
Layer 2 and Layer 3 wholesale	Subscriber secure policy traffic mirroring
Bi-directional Forwarding Detection (BFD)	Autosensed VLANs
NWay active link aggregation (LAG)	–

[*Subscriber Access*]

- **Support for link redundancy for CoS configured on an L2TP**—You can now configure multiple ports on the same IQ2 and IQ2E PICs to support link redundancy for CoS on L2TP tunnels configured on an Ethernet interface.

  Link redundancy is useful when the active port is unavailable due to events such as:

  - Disconnection of a cable
  - Rebooting of a remote end system
  - Re-routing the traffic through a different port due to network conditions

  When link redundancy is enabled, the traffic to the LAC devices is re-routed through another Ethernet interface configured on the same IQ2 or IQ2E PIC and the L2TP sessions are maintained.

  [*Subscriber Access*]

- **Support to display CoS statistics for L2TP session**—In Junos OS Release 12.1, a new command, **show services l2tp cos-policier**, has been introduced to display CoS statistics for a policed or shaped L2TP session configured on an IQ2 or IQ2E PIC.

  [*Subscriber Access*]

- **Support to display disconnect cause summary for L2TP sessions on M Series routers**—In Junos OS releases earlier than Release 12.1, there was no mechanism to view the statistics for the disconnect cause summary of L2TP sessions. The following new commands are now supported on M Series routers to view the disconnect cause summary statistics for an L2TP session:

  - **show services l2tp disconnect-cause-summary**
  - **clear services l2tp disconnect-cause-summary**

  [*Subscriber Access*]

- **Support to display LCP statistics for an L2TP session**—You can now view LCP statistics among other statistics for an L2TP session. The output of the following commands has been modified to include LCP statistics information:

  - **show services l2tp session**
  - **show services l2tp summary**

- **Support to display MLPPP statistics for an L2TP session**—You can now view MLPPP (Multilink Point-to-Point Protocol) statistics along with other L2TP statistics for an L2TP session. The **show services l2tp multilink** command has been modified to display the MLPPP statistics for an L2TP session.
- **Default subscriber service (MX Series routers)**—Subscriber management enables you to specify a default subscriber service for DHCP subscribers. The default service (dynamic profile) is applied to subscribers who are not assigned a service by a remote server, such as RADIUS or a provisioning server (for example, a JSRC server or Gx-Plus server) when the subscriber logs in.

  When a subscriber logs in, subscriber management examines the subscriber's access profile and uses a predetermined sequence to activate the subscriber's service.

  To provide support for default subscriber services, use the following statements at the **[edit system services dhcp-local-server...]** and **[edit forwarding-options dhcp-relay...]** hierarchy levels:

  - **service-profile** ***dynamic-profile-name***—Specifies that the service (dynamic profile) is used as the default subscriber service.
  - **dynamic-profile** ***dynamic-profile-name***—Specifies that the default service is used globally, for a group of interfaces or for a specific interface.

  [*Subscriber Access*]

User Interface and Configuration

- **Support for CLI edit mode wildcard range command**—The wildcard range command enables you to specify ranges in activate, deactivate, delete, protect, set, show and unprotect commands. You can use ranges to specify a range of interfaces, logical units, VLANs, and other numbered elements. The wildcard range command expands the command you entered into multiple commands, each of which corresponds to one item in the range. For example, wildcard range interfaces deactivate ge-0/0/[1-3] expands to deactivate interfaces ge-0/0/1, deactivate interfaces ge-0/0/2, and deactivate interfaces ge-0/0/3.

  [*CLI User Guide*]
- **Support for batch commits**—The batch commit feature aggregates or merges multiple configuration edits from different CLI sessions or users and adds them to a batch commit queue. A commit server running on the device takes one or more jobs from the batch commit queue, applies the configuration changes to the shared configuration database, and then commits the configuration changes in a single commit operation. When compared to the regular commit operation where all commits are independently committed sequentially, batch commits save time and system resources by committing multiple small configuration edits in a single commit operation.

  Batch commits are performed from the **[edit batch]** configuration mode. The commit server properties can be configured at the **[edit system commit server]** hierarchy level.

  [*CLI User Guide*]

VPNs

- **Support for Layer 3 VPN composite next hop (T4000 routers)**—Layer 3 VPN composite next hop is supported on T4000 Type 5 FPCs. Next-hop chaining (also known as composite next hop) is a composition function that concatenates the partial rewrite strings associated with individual next hops to form a larger rewrite string that is added to a packet.

  A chained next hop contains the inner label and the downstream indirect next-hop destination information. The outer labels and Layer 2 rewrite bytes are associated with the unicast next hop. The T4000 Type 5 FPC Packet Forwarding Engine supports full chaining—that is, the ingress Packet Forwarding Engine adds the inner VPN label to the packet and sends the modified packet, along with a token that corresponds to the unicast next hop, to the egress Packet Forwarding Engine. The egress Packet Forwarding Engine adds the transport label and Layer 2 encapsulation information based on the token to the packet.

  For Layer 3 VPNs configured on Juniper Networks routers, Junos OS normally allocates one inner VPN label for each VPN network on the customer edge (CE)-facing interfaces of a provider edge (PE) router. However, other vendors allocate one VPN label for each BGP route on the CE-facing interfaces of a PE router. This practice increases the number of VPN labels exponentially, which leads to slow system processing and slow convergence time. To account for this difference, configure the **l3vpn-composite-nexthop** statement at the **[edit routing-options]** hierarchy level on the Juniper Networks routers participating in a mixed vendor network. The **l3vpn-composite-nexthop** statement is disabled by default.

  [*VPNs*]

- **eBGP and iBGP load-balancing support for MVPN and PIM**—The multipath PIM join load balancing feature enables customer PIM (C-PIM) join messages to be load-balanced across unequal EBGP and IBGP paths in a draft-rosen MVPN, and across all available IBGP paths in a next-generation MVPN that does not have any EBGP upstream path toward the source or RP.

- **Load balancing and IP header filtering for Layer 3 VPNs**—You can now simultaneously enable load balancing and IP header filtering for traffic in a network with both internal and external BGP paths. To enable these features, include the**equal-external-internal** statement at the **[edit routing-instances *routing-instance-name* routing-options multipath vpn-unequal-cost]** hierarchy level and the **vrf-table-label** statement at the **[edit routing-instances *routing-instance-name*]** hierarchy level.

  [*VPNs*]

- **Inter-AS multicast Layer 3 VPNs**—You can now configure multicast Layer 3 VPNs (also known as mulitprotocol BGP (MBGP)-based multicast VPNs) across autonomous systems (ASs). Previously, you could only configure unicast Layer 3 VPNs across ASs. Although there are a number of different network configurations that can be used to enable inter-AS support for multicast VPN traffic, Junos OS Release 12.1 supports only next generation VPN option A and option C. For both option A and option C, the customer service provider depends on the VPN service provider to deliver a VPN transport service between the customer service provider's points of presence (POPs)

or regional networks. This functionality might be used by a VPN customer who has connections to several different Internet service providers (ISPs), or different connections to the same ISP in different geographic regions, each of which has a different AS number.

- Option A—In this implementation, the VPN routing and forwarding (VRF) table in the ASBR of one AS is linked to the VRF table in the ASBR in the other AS. Each ASBR must contain a VRF instance for every VPN configured in both service provider networks. In addition, PIM needs to be configured between the VRF instances and IGP or BGP must be configured between the ASBRs. Option A is a relatively simple interprovider VPN solution. However, it is less scalable relative to option C.
- Option C—In this implementation, only routes internal to the service provider networks are announced between ASBRs. This is achieved by using the **family inet labeled-unicast** statements in the IBGP and EBGP configuration on the PE routers. Labeled IPv4 (not VPN-IPv4) routes are exchanged by the ASBRs to support MPLS. An MP-EBGP session between the end PE routers is used for the announcement of VPN-IPv4 routes. In this manner, VPN connectivity is provided while keeping VPN-IPv4 routes out of the core network.

The existing configuration statements and documented procedures for the implementation of interprovider Layer 3 VPNs option A and option C can be applied to interprovider multicast Layer 3 VPNs. Of course, interprovider multicast Layer 3 VPNs requires the configuration of the multicast features in addition to the interprovider features.

[*VPNs*]

Related Documentation

- Changes in Default Behavior and Syntax, and for Future Releases in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 174
- Issues in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers
- Errata and Changes in Documentation for Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 185
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 191

Changes in Default Behavior and Syntax, and for Future Releases in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers

Changes in Default Behavior and Syntax

The following are changes made to Junos OS default behavior and syntax.

High Availability

- **Updates to command forwarding support for MX Series Virtual Chassis (MX240, MX480, and MX960 routers with MPC/MIC interfaces)**—The following operational commands now support command forwarding in an MX Series Virtual Chassis configuration:
  - **show chassis craft-interface**
  - **show chassis fan**
  - **show chassis pic**
  - **show chassis power**

  Command forwarding enables you to monitor and manage an MX Series Virtual Chassis as a single network element by running operational commands on a specific member router in the Virtual Chassis, on both member routers, or on the local member router from which you issue the command. With command forwarding, the router sends the command to the specified member router or routers and displays the results as if the command were processed on the local router.

  To forward operational commands to one or both member routers in an MX Series Virtual Chassis, use one of the following options when you issue these commands:

  - To forward the command to a specifed member router, use the **member** ***member-id*** option, where *member-id* can be 0 or 1.
  - To run the command on the local member router on which the command was issued, use the **local** option.
  - To forward the command to both member routers, use the **all-members** option. This is the default command forwarding option for the **show chassis craft-interface**, **show chassis fan**, **show chassis pic**, and **show chassis power** commands.

  [*Junos OS System Basics and Services Command Reference*, *Junos OS High Availability Configuration Guide*]

Interfaces and Chassis

- The **allow-sram-parity-errors** statement is made visible at the **[edit chassis fpc** ***slot-number***] hierarchy level (for T Series routers only).

  [*System Basics Configuration Guide*]

Routing Protocols

- When a route with an improved metric is added to the IS-IS internal routing table, IS-IS flushes all next-hop information (including LSP next-hop information) for a route. To override this default behavior for load balancing, the **lsp-equal-cost** statement is added at the **[edit protocols isis traffic-engineering multipath]** hierarchy level to retain the equal cost path information in the routing table.

  [*Routing Protocols*]

- **Enhancements to DDoS Protection (MX Series routers)**—The configuration of DDoS Protection has changed slightly. You can now include the **disable-fpc** statement at the **[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]** hierarchy level to disable policers on all line cards for a particular packet type or aggregate within a protocol group. The ability to configure this statement globally or for a particular line card remains unchanged.

  You can also now include the **disable-logging** statement at the **[edit system ddos-protection protocols *protocol-group* (aggregate | *packet-type*)]** hierarchy level to disable router-wide logging of DDoS violation events for a particular packet type or aggregate within a protocol group. The **disable-logging** statement has been moved from the **[edit system ddos-protection violation]** hierarchy level, and that hierarchy level has been removed from the CLI.

  The **show ddos-protection protocols** command now displays **Partial** in the **Enabled** field to indicate when some of the instances of the policer are disabled. The **Routing Engine Information** section of the output now includes fields for bandwidth, burst, and state.

  The **show ddos-protection protocols parameters** command and the **show ddos-protection protocols statistics** command now include a **terse** option to display information only for active protocol groups—that is, groups that show traffic in the **Received (packets)** column. The **show ddos-protection protocols parameters** command also displays **part.** for policers that have some disabled instances.

  [*DDoS Protection*]

Subscriber Access Management

- **Enhanced Subscriber Service Accounting Information**—Subscriber access accounting has been enhanced in Junos OS Release 11.4R2 and later, and Release 12.1R1 and later. RADIUS VSA 26-83 (Service-Session), which is included in RADIUS service accounting start and stop packets, now includes the parameter values used to activate a subscriber service, in addition to the service name. In earlier releases, only the service name was included. When VSA 26-83 is not available from the RADIUS server, subscriber management sends the service name in the accounting message (as was the case in earlier releases).

  [*Subscriber Acess*]

- **Keepalive statistics display for PPP fast keepalive (MX Series routers with MPCs/MICs)**—PPP fast keepalive, which is enabled by default on MX Series routers with MPCs/MICs, is the mechanism by which LCP Echo-Request packets are processed by the Packet Forwarding Engine instead of by the Routing Engine. When the router is using PPP fast keepalive for a PPP link, the output of the **show interfaces pp0.*logical*** operational command does not include the number of keepalive packets received or sent, or the amount of time since the router received or sent the last keepalive packet.

  With PPP fast keepalive and **no-keepalives** configured, the **show interfaces pp0.*logical*** command does not display output statistics for keepalive packets sent, as expected, or input statistics for keepalive packets received from PPP subscribers (clients). Even if **no-keepalives** is configured to prevent the router from sending PPP keepalive messages, the router is still able to respond to PPP keepalive messages that it receives from clients.

When PPP fast keepalive is *not* in use on MX Series routers without MPCs/MICs, or on routers other than MX Series routers, you can view input statistics for received PPP keepalive packets with the **show interfaces pp0.*logical*** command, even if you have issued the **no-keepalives** statement to disable sending keepalive messages on the PPP interface.

[*Junos OS Subscriber Access Configuration Guide*]

- **Configuring a AAA local access profile for L2TP clients on the LNS (MX240, MX480, MX960 3D Universal Edge Routers)**—You can now configure a local access profile that specifies a particular RADIUS server configuration to override the global access profile and the tunnel group AAA access profile for a LAC client. The AAA access profile for the client takes precedence over the tunnel group profile, which in turn takes precedence over the global access profile for the routing instance.

  Include the **aaa-access-profile** statement at the **[edit access profile *access-profile-name* client *client-name*]** hierarchy level. In earlier releases, you included this statement only at the **[edit services l2tp tunnel-group *name*]** hierarchy level to configure a profile for an L2TP tunnel group. The global access profile is configured at the routing instance that hosts the L2TP tunnel with the **profile *access-profile-name* statement** at the **[edit access]** hierarchy level.

  [*Subscriber Access*]

- **Enhanced monitoring of RADIUS server status and information (MX Series routers)**—RADIUS server monitoring is updated to include a new operational command for displaying RADIUS server information, and an enhanced system log message for RADIUS server events. The new **show network-access aaa radius-servers** command enables you to display status and information related to RADIUS servers. The command also supports the **detail** option, which displays additional information. The AUTHD_AUTH_SERVER_STATUS_CHANGE system log (syslog) message is reported at the **warning** Severity level when a RADIUS server state changes from **up** to **down**, or vice versa.

  [*Subscriber Access*]

- **Session-ID added to output of show network-access aaa subscribers username command (MX Series routers)**—The output of the **show network-access aaa subscribers username *username*** command now includes a column showing the Session-ID for the specified username.

  [*Subscriber Access*]

- **Managing CoA requests that include unapplied changes to client profile dynamic variables**—You can manage the way that subscriber management processes CoA requests that include changes to a client profile dynamic variable that cannot be applied. For example, a CoA request might include several changes to client profile dynamic variables, one of which contains updates to a firewall filter that does not exist and so cannot be applied.

  In the default behavior, subscriber management does not apply the incorrect firewall filter update but makes the other changes to the client profile dynamic variables, and then responds with an ACK message. Subscriber management now supports an optional configuration, which replaces the default behavior. The optional configuration specifies

that when a CoA operation is unable to apply a requested change to a client profile dynamic variable, subscriber management does not apply any changes to client profile dynamic variables in the request and then responds with a NACK message.

To configure subscriber management to override the default behavior, use the **coa-dynamic-variable-validation** statement at the **[edit access profile *profile-name* radius options]** hierarchy level.

[*Subscriber Access*]

- **Enhanced output for show network-access aaa statistics authentication command (MX Series routers)**—The **show network-access aaa statistics authentication** command now supports the **detail** option, which displays additional authentication information. The following example shows the output for the enhanced command. The new fields are described in the table after the example.

```
user@host> show network-access aaa statistics authentication detail

Authentication module statistics
  Requests received: 2118
  Multistack requests: 0
  Accepts: 261
  Rejects: 975
    RADIUS authentication failures: 975
      Queue request deleted: 0
      Malformed reply: 0
      No server configured: 0
      Access Profile configuration not found: 0
      Unable to create client record: 0
      Unable to create client request: 0
      Unable to build authentication request: 0
      No server found: 975
      Unable to create handle: 0
      Unable to queue request: 0
      Invalid credentials: 0
      Malformed request: 0
      License unavailable: 0
      Redirect requested: 0
      Internal failure: 0
    Local authentication failures: 0
    LDAP lookup failures: 0
  Challenges: 0
  Requests timed out: 882
```

Table 14: New show network-access aaa statistics authentication Output Fields

Field Name	Field Description
Multistack requests	Number of authentication requests for dual stack subscribers.
RADIUS authentication failures	Number of RADIUS authentication requests that have failed
Queue request deleted	Number of queue requests that have been deleted
Malformed reply	Number of malformed replies received from the RADIUS authentication server

Table 14: New show network-access aaa statistics authentication Output Fields *(continued)*

Field Name	Field Description
No server configured	Number of authentication requests that failed because no authentication server is configured
Access Profile configuration not found	Number of authentication requests that failed because no access profile is configured
Unable to create client record	Number of times that the router is unable to create the client record for the authentication request
Unable to create client request	Number of times that the router is unable to create the client request for the authentication request
Unable to build authentication request	Number of times that the router is unable to build the authentication request
No server found	Number of requests to the authentication server that have timed out; the server is then considered to be down
Unable to create handle	Number of authentication requests that have failed because of an internal allocation failure
Unable to queue request	Number of times the router was unable to queue the request to the authentication server
Invalid credentials	Number of times the router did not have proper authorization to access the authentication server
Malformed request	Number of times the router request to the authentication server is malformed.
License unavailable	Number of times the router did not have a license to access the authentication server
Redirect requested	Number of authentication requests that have been redirected based on routing instance
Internal failure	Number of internal failures
Local authentication failures	Number of times local authentication failed
LDAP lookup failures	Number of times the LDAP lookup operation failed

[*Subscriber Access*]

Related Documentation

- New Features in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 135
- Issues in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers

Issues in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers

The current software release is Release 12.1B2. For information about obtaining the software packages, see "Upgrade and Downgrade Instructions for Junos OS Release 12.1 for M Series, MX Series, and T Series Routers" on page 191.

Current Software Release

Outstanding Issues in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers

Class of Service

- The **show class-of-service classifier name "classifier name with spaces"** command does not work for classifiers which has spaces in their name. [PR/535967]

Infrastructure

- The /mfs partition has only 64MB when only compact flash is available as the storage media, and hence large configuration files cannot be stored. So, when the HDD is broken and /mfs partition is not large enough to store the configuration files, the Routing Engine does not boot. [PR/720540]

Interfaces and Chassis

- The password recovery process does not work on some MX80 routers. [PR/585092]
- When input both IPv6 multicast and unicast traffic, changing the MTU for output interface might cause incorrect counter for "Output packets". [PR/700018]
- Source Address Filtering is not supported on aggregated Ethernet interfaces. [PR/710262]

- Due to a bug in the kernel, the **lc** interfaces or old child links show up as member links of AE interface. This is caused due to a clean up issue in the kernel. For example, the interface extensive for a ae bundle configuration with xe-8/1/0 and xe-4/3/3 as member links:

```
LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
     xe-8/1/0.0            223171      223707            0            0
     xe-4/3/3.0            223171      223716            0            0
     lc-3/1/0.32769             0           0            0            0
<<
```

  or, xe-7/1/3 and xe-7/2/0 are not configured to be member links of ae1:

```
Physical interface: ae1, Enabled, Physical link is Up
 <trimmed for brevity>
   LACP Statistics:       LACP Rx     LACP Tx   Unknown Rx   Illegal Rx
     xe-7/1/3.0                 0           0            0            0
 <<
     xe-7/2/0.0                 0           0            0            0
 <<
     xe-4/2/0.0           3164683     3165879            0            0
     xe-5/2/0.0           3164369     3165539            0            0
```

  In case of LC intf showing up as part of AE bundle SNMP walk fails with "Request failed: General error" for OID .1.2.840.10006.300.43.1.2.1.1 due to incorrect member links in AE Bundle.

  As a workaround, delete the AE bundle configurations and reconfigure it. [PR/712148]

Multicast

- When Rosen MVPN is configured with SSM option, PIM neighbors may not establish. There is no workaround at this time. [PR/708685]

Platform and Infrastructure

- The SFC management interface **em0** is often displayed as **fxp0** in several warning messages. [PR/454074]
- Discrepancies exist in MAC and filter statistics between Trio MPC and Enhanced DPCs. [PR/517926]
- M10i routers installed with Service PICs and chipset ecfeb will not work with Junos OS Release 12.1B2 because of PR 739209. [PR/576830]
- On a TX Matrix Plus router, when an **em0** interface is disabled, the **em1** interface is also disabled. This causes a loss of communication to the LCCs. [PR/596113]
- The time stamp of the messages in the firewall log shows incorrect values. The system time and time stamp in the log messages are not affected. However, this issue does not occur if the NTP server is configured. [PR/661768]
- During certain configuration corner cases when the source address or destination address associated with one of the listed Packet Forwarding Engine firewall filter logs is of a certain length, it causes the system log module in the Packet Forwarding Engine to crash. [PR/718485]

Routing Protocols

- When IGMP is enabled on an **fxp0** interface, a discard next hop might get installed for 224/4 routes. [PR/601619]
- A BGP family configuration expects that if any more specific configuration, for example a neighbor vs. group, group vs. global, is present, then no family configuration from a lesser specific configuration is used. When family **route-target advertise-default** is configured at BGP peer group scope and the BGP neighbor scope configuration contains family statements, the **advertise-default** should not be propagated. [PR/706925]
- When MSDP SA message received from MSDP peer is rejected by MSDP import policy, that reject action does not prevent MSDP from passing that SA to MVPN and/or PIM modules. A resolution to the issue no longer imports a rejected SA to the bgp.mvpn.0 table. [PR/711333]
- In the NG-MVN scenario, the **maximum-prefixes** option configured under *routing_instance*.mvpn.0 rib does not take effect. For example:

```
user@router# show routing-instances vrf routing-options

rib vrf.mvpn.0 {
    maximum-prefixes 5 threshold 3;
}
```

  [PR/712060]
- Under scaled situations, BGP may core in bgp_rtarget_tsi_update when running family route-target. This may happen when all viable RT-Constrain routes to a destination have been deleted but the route has not been withdrawn from BGP peers. [PR/725196]
- In a situation where "prefix-export-limit", and NSR is configured together, when there is a Routing Engine mastership switchover, the IS-IS overload bit may be set after the NSR switchover. This issue is triggered due to inconsistent state between the master Routing Engine and the backup Routing Engine. [PR/725478]

Services Applications

- When a standard application is specified under the **[edit security idp idp-policy *policy-name* rulebase-ips rule *rule-name* match application]** hierarchy level, IDP does not detect the attack on the nonstandard port (for example, junos:ftp on port 85). [PR/477748]
- Multiservices PICs on M Series routers and Multiservices DPCs on MX Series routers currently have the limitation that after a hot-standby redundant Multiservices PIC or DPC (RMS) switchover, all the existing flows are dropped and it takes a while for new flows to appear with the state. Because the states are not replicated, all existing traffic is dropped. The Remote Procedure Call (RPC) ALG is most affected because it has a long retry timer and takes a long time to recover. [PR/535597]
- When unit **0** of the Multiservices PIC interface is not specified, the **monitor interface traffic** command does not display the input packet's number properly for that particular ms-I/F interface. [PR/544318]

- The default Junos OS configuration contains an application definition for matching UDP-based traceroute. It does not include port 33434 which is also used by the unix traceroute implementation. [PR/727825]
- On MX Series routers with subscriber management feature enabled, upon very frequent execution of the **show services l2tp** commandschild processes of jl2tpd process does not exit cleanly resulting in defunct process to be left behind. If these said commands are executed repeatedly over time, ultimately the maxproc limit of jl2tpd is reached and the process would core, and in situations with graceful Routing Engine switchover enabled, it can finally lead to kernel crash due to Process Table overflow. Typical error messages when jl2tpd nears the limit of maxproc:

```
/kernel: nearing maxproc limit by uid 0, please see tuning(7) and
login.conf(5).
/kernel: Process with Most Children- 2231:jl2tpd - Children - 399

upon jl2tpd exceeding the maxproc limit:

/kernel: maxproc limit exceeded by uid 0, please see tuning(7) and
login.conf(5).
/kernel: Process with Most Children- 2231:jl2tpd - Children - 400
...
/kernel: pid 1437 (jl2tpd), uid 0: exited on signal 10 (core dumped)

- from bsd shell, ps -aux command would show defunct processes upon this
 issue occurrence

root 40840  0.0  0.0     0     0  ??  Z     2:13AM   0:00.01 <defunct>
root 40843  0.0  0.0     0     0  ??  Z     2:13AM   0:00.01 <defunct>
```

  [PR/729509]

Subscriber Access Management

- Although the si interface type is not supported for the **clear services l2tp tunnel interface** *interface-name*, **show services l2tp tunnel interface** *interface-name*, and **show services l2tp summary interface** *interface-name* commands, the CLI allows you to enter this interface type. [PR/699151]
- The **client-idle-timeout** under access profile statement does not work when RADIUS accounting is not configured. [PR/717870]

User Interface and Configuration

- The pop-up window for logging out of the J-Web interface is hidden when the log out button is used from the Diagnose> CLI terminal page on both Internet Explorer and Mozilla Firefox browsers. [PR/401772]
- In the J-Web interface , the “Generate Report” option under Monitor Event and Alarms opens the report on the same web page. [PR/433883]
- Selecting the monitor port for any port on the Chassis Viewer page displays the common Port Monitoring page instead of the corresponding Monitoring page of the selected port. [PR/446890]

- The link up/down hold time cannot be configured on a **coc12** interface. However, the configuration can be inherited by means of an apply group. When a router is reloaded, the **coc12** interface does not come back up because the link up/down hold time configuration is inherited with the help of the apply group. [PR/468598]
- In the J-Web interface, the options **Access Concentrator**, **Idle Timeout**, and **Service Name** for PPPoE logical interfaces are not supported on MX Series routers. [PR/493451]
- While accessing the J-Web pages, the httpd process dumps core at irregular intervals. [PR/535768]
- When an HTTPS connection is used for the J-Web interface in Internet Explorer to save a report from the View Events page (Monitor>Events and Alarms>View events), the following error message is displayed “Internet Explorer was not able to open the Internet site.”

  This issue also appears in the following places on the J-Web interface:

  - maintain>config management>history
  - maintain>customer support>support information>Generate Reports
  - Troubleshoot port>Generate Reports
  - maintain>files
  - Monitor>Routing>Route Information>Generate Reports

  [PR/542887]
- When a J-Web session is opened and the login credentials are provided, the J-Web interface takes 20 seconds longer to load the Dashboard page on an HTTPS connection than it does when an HTTP connection is used. [PR/549934]
- The time displayed on the Monitor>Events And Alarms> View Events page does not match the switch's time when the J-Web interface is launched through an HTTPS connection. As a workaround, reset the correct time after the J-Web interface is launched through the HTTPS connection. [PR/558556]
- The javascript error, "Object Expected" occurs when J-Web pages are navigated before the page loads completely. [PR/567756]
- The J-Web application allows duplicate term names to be created on the Configure> Security> Filters> IPV4 Firewall Filters page. However, these duplicate entries are not displayed in the grid and there is no impact on the functionality. [PR/574525]
- In the J-Web interface, when a user is deleted on the Configure> System Properties> User Management> Users page using the Internet Explorer version 7 Web browser, no warning messages are displayed. However, the warning message appears when the Firefox Web browser is used. [PR/595932]
- When the J-Web interface is accessed using the Microsoft Internet Explorer web browser Version 7, all flags on the BGP Configuration page (Configure> Routing> BGP) might be shown in the Configured Flags list (in the Edit Global Settings window, on the Trace Options tab) even when the flags are not configured. As a workaround, use the Mozilla Firefox Web browser. [PR/603669]

- Multiple entries are listed for a few processes on the Process details page (Monitor> System View> Process details) of the J-Web interface. This issue does not have any functionality impact. [PR/661704]
- Using the **# load** command to replace policy configuration could lead to a configuration corruption which causes the routing protocol process to crash upon commit. [PR/704294]

VPNs

- The BGP community 0xFF04 (65284) is incorrectly displayed as "mvpn-mcast-rpt" in the output of the **show route** command. [PR/479156]
- Under certain circumstances, a vrf-import policy's term with the "accept" action that matches the BGP VPN route based on the criteria different than the target community can reject the matching route. [PR/706064]
- The different endianness of an MX80's PowerPC was not considered in mpls-internet-multicast functions, causing routing failures. [PR/732563]

Related Documentation

- New Features in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 135
- Changes in Default Behavior and Syntax, and for Future Releases in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 174
- Errata and Changes in Documentation for Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 185
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 191

Errata and Changes in Documentation for Junos OS Release 12.1 for M Series, MX Series, and T Series Routers

Errata

High Availability

- The *Virtual Chassis Components Overview* topic and the *Guidelines for Configuring Virtual Chassis Ports* topic in the *Junos OS High Availability Configuration Guide* incorrectly state that an MX Series Virtual Chassis configuration supports up to 24 Virtual Chassis ports per trunk. An MX Series Virtual Chassis configuration actually supports up to 16 Virtual Chassis ports per trunk.

  [*Junos OS High Availability Configuration Guide*]

- TX Matrix Plus routers and T1600 routers that are configured as part of a routing matrix do not currently support nonstop active routing.

  [*High Availability*]

Interfaces and Chassis

- With Junos OS Release 10.1 and later, you need not include the **tunnel** option or the **clear-dont-fragment-bit** statement when configuring **allow-fragmentation** on a tunnel.

  [*Services Interfaces*]

J-Web Interface

- To access the J-Web interface, your management device requires the following software:
  - Supported browsers—Microsoft Internet Explorer version 7.0 or Mozilla Firefox version 3.0
  - Language support—English-version browsers
  - Supported OS—Microsoft Windows XP Service Pack 3

Layer 2 Ethernet Services

- In the *Layer 2 Configuration Guide*, the examples provided in the sections, *Configuring Layer 2 Protocol Tunneling*, *Configuring BPDU Protection on Individual Interfaces*, and *Configuring BPDU Protection on All Edge Ports* are incorrect for configuring layer 2 tunneling with routing instances.

Multicast

- The listings for the following RFCs incorrectly state that Junos OS supports only SSM include mode. Both include mode and exclude mode are supported in Junos OS Release 9.3 and later.
  - RFC 3376, *Internet Group Management Protocol, Version 3*
  - RFC 3590, *Source Address Selection for the Multicast Listener Discovery (MLD) Protocol*

[*Hierarchy and Standards Reference*]

Services Applications

- The **rate** statement for packet sampling is now configured at the **[edit forwarding options sampling input family *family*]** hierarchy level.

  [*Services Interfaces*]

Subscriber Access Management

- The *Configuring Per-Subscriber Session Accounting* topic in the *Subscriber Access Configuration Guide*, incorrectly states that the **update-interval** statement rounds up an interval of 10 through 15 minutes to 15. The actual behavior is that all configured values are rounded up to the next higher multiple of 10. For example, the values 811 through 819 are all accepted by the CLI, but are all rounded up to 820.

  [*Subscriber Access*]

- The *DHCP in Broadband Networks* topic erroneously states that the Junos OS subscriber management solution currently supports only DHCP as a multiple-client configuration protocol. However, subscriber management solutions support DHCP and PPPoE as multiple-client configuration protocols.

  [*Broadband Subscriber Management Solutions*]

- The *Configuring Service Packet Counting* topic in the *Junos OS Subscriber Access Configuration Guide* does not include the following configuration guideline. When you specify the **service-accounting** action for the term, you cannot additionally configure the **count** action in the same term.

  [*Subscriber Access*]

- The table titled *Supported Juniper Networks VSAs* in the *Juniper Networks VSAs Supported by the AAA Service Framework* topic lists RADIUS VSA 26-157 (IPv6-NdRa-Pool-Name). This VSA is not supported and should not appear in the table.

  [*Subscriber Access*]

- The *Configuring a Dynamic Profile for Client Access* topic erroneously uses the **$junos-underlying-interface** variable when an IGMP interface is configured in the client access dynamic profile. The following example provides the appropriate use of the **$junos-interface-name** variable:

  ```
  [edit dynamic-profiles access-profile]
  user@host# set protocols igmp interface $junos-interface-name
  ```

- Table 25 in the *Dynamic Variables Overview* topic does not define the **$junos-igmp-version** predefined dynamic variable. This variable is defined as follows:

  $junos-igmp-version—IGMP version configured in a client access profile. Junos OS obtains this information from the RADIUS server when a subscriber accesses the router. The version is applied to the accessing subscriber when the profile is instantiated. You specify this variable at the **[dynamic-profiles *profile-name* protocols igmp]** hierarchy level for the **interface** statement.

In addition, the *Subscriber Access Configuration Guide* erroneously specifies the use of a colon (:) when you configure the dynamic profile to define the IGMP version for client interfaces. The following example provides the appropriate syntax for setting the IGMP interface to obtain the IGMP version from RADIUS:

```
[edit dynamic-profiles access-profile protocols igmp interface $junos-interface-name]
user@host# set version $junos-igmp-version
```

- The *Subscriber Access Configuration Guide* and the *System Basics Configuration Guide* contain information about the **override-nas-information** statement. This statement does not appear in the CLI and is not supported.

  [*Subscriber Access*, *System Basics*]

- When you modify dynamic CoS parameters with a RADIUS change of authorization (CoA) message, Junos OS accepts invalid configurations. For example, if you specify a transmit rate that exceeds the allowed 100 percent, the system does not reject the configuration and returns unexpected shaping behavior.

  [*Subscriber Access*]

- Juniper Networks does not support multicast RIF mapping and ANCP when configured simultaneously on the same logical interface. For example, configuring a multicast VLAN and ANCP on the same logical interface is not supported, and the subscriber VLANs are the same for both ANCP and multicast.

  [*Subscriber Access*]

- The *Subscriber Access Configuration Guide* incorrectly describes the **authentication-order** statement as it is used for subscriber access management. When configuring the **authentication-order** statement for subscriber access management, you must always specify the **radius** method. Subscriber access management does not support the **password** keyword (the default), and authentication fails when you do not specify an authentication method.

  [*Subscriber Access*]

- In the *Subscriber Access Configuration Guide*, the *Juniper Networks VSAs Supported by the AAA Service Framework* table and the *RADIUS-Based Mirroring Attributes* table incorrectly describe VSA 26-59. The correct description is as follows:

Attribute Number	Attribute Name	Description
26-59	Med-Dev-Handle	Identifier that associates mirrored traffic to a specific subscriber.

  [*Subscriber Access*]

- In the *Subscriber Access Configuration Guide*, the table titled "Supported Juniper Networks VSAs" in the "Juniper Networks VSAs Supported by the AAA Service Framework" topic lists RADIUS VSA 26-42 (Input-Gigapackets) and VSA 26-43 (Output-Gigapackets). These two VSAs are not supported.

[*Subscriber Access*]

- In the *Junos OS Subscriber Access Configuration Guide*, the "Qualifications for Change of Authorization" section in the topic titled “RADIUS-initiated Change of Authorization (CoA) Overview”, has been rewritten as follows to clarify how CoA uses the RADIUS attributes and VSAs.

  Qualifications for Change of Authorization

  To complete the change of authorization for a user, you specify identification attributes and session attributes. The identification attributes identify the subscriber. Session attributes specify the operation (activation or deactivation) to perform on the subscriber’s session and also include any client attributes for the session (for example, QoS attributes). The AAA Service Framework handles the actual request.

  Table 15 on page 189 shows the identification attributes for CoA operations.

  NOTE: Using the Acct-Session-ID attribute to identify the subscriber session is more explicit than using the User-Name attribute. When you use the Acct-Session-ID, the attribute identifies the specific subscriber and session. When you use the User-Name as the identifier, the CoA operation is applied to the first session that was logged in with the specified username. However, because a subscriber might have multiple sessions associated with the same username, the first session might not be the correct session for the CoA operation.

Table 15: Identification Attributes

Attribute	Description
User-Name [RADIUS attribute 1]	Subscriber username.
Acct-Session-ID [RADIUS attribute 44]	Specific subscriber and session.

Table 16 on page 189 shows the session attributes for CoA operations. Any additional client attributes that you include depend on your particular session requirements.

Table 16: Session Attributes

Attribute	Description
Activate-Service [Juniper Networks VSA 26–65]	Service to activate for the subscriber.
Deactivate-Service [Juniper Networks VSA 26–66]	Service to deactivate for the subscriber.

[*Subscriber Access*]

User Interface and Configuration

- The **show system statistics bridge** command displays system statistics on MX Series routers.

  [*System Basics Command Reference*]

VPNs

- In *Chapter 19, Configuring VPLS* of the *VPNs Configuration Guide*, an incorrect statement that caused contradictory information about which platforms support LDP BGP interworking has been removed. The M7i router was also omitted from the list of supported platforms. The M7i router does support LDP BGP interworking.

  [*VPNs*]

Changes to the Junos OS Documentation Set

The following are the changes made to the Junos OS documentation set:

- Stateless firewall filter and traffic policer documentation is no longer included in the *Junos OS Policy Framework Configuration Guide*. This material is now available in the *Junos OS Firewall Filter and Policer Configuration Guide* only.
- Routing policy, traffic sampling, forwarding, and monitoring documentation is no longer included in the *Junos OS Policy Framework Configuration Guide*. This material is now available in the *Junos OS Policy Framework Configuration Guide*.
- The material that was formerly covered in the *Junos OS Policy Framework Configuration Guide* Web pages is now available as three subject-based Web pages. You can locate the links to the new Web pages at the following URLs:
  - *Routing Policy, Traffic Sampling, Forwarding, and Monitoring Configuration*—http://www.juniper.net/techpubs/en_US/junos11.2/information-products/pathway-pages/config-guide-policy/config-guide-policy.html
  - *Stateless Firewall Filter Configuration*—http://www.juniper.net/techpubs/en_US/junos11.2/information-products/pathway-pages/config-guide-firewall-filter/config-guide-firewall-filter.html
  - *Traffic Policer Configuration*—http://www.juniper.net/techpubs/en_US/junos11.2/information-products/pathway-pages/config-guide-firewall-filter/config-guide-policer.html
- The *Junos OS Hierarchy and Standards Reference* is now available as three subject-based Web pages. You can locate the links to the new Web pages for the guides at the following URLs:
  - *Junos OS Configuration Statements and Commands*—http://www.juniper.net/techpubs/en_US/junos11.1/information-products/pathway-pages/reference-hierarchy/junos-configuration-hierarchies.html
  - *Junos OS Product and Feature Descriptions*—http://www.juniper.net/techpubs/en_US/junos11.1/information-products

/pathway-pages/reference-hierarchy/junos-product-features.html

- *Standards Supported by the Junos OS*—http://www.juniper.net/techpubs/en_US/junos11.1/information-products/pathway-pages/reference-hierarchy/junos-supported-standards.html

- In addition, individual HTML pages have a **Print** link in the upper left corner of the text area on the page.

Related Documentation

- New Features in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 135
- Changes in Default Behavior and Syntax, and for Future Releases in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 174
- Issues in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 191

Upgrade and Downgrade Instructions for Junos OS Release 12.1 for M Series, MX Series, and T Series Routers

This section discusses the following topics:

Basic Procedure for Upgrading to Release 12.1

In order to upgrade to Junos OS 10.0 or later, you must be running Junos OS 9.0S2, 9.1S1, 9.2R4, 9.3R3, 9.4R3, 9.5R1, or later minor versions, or you must specify the **no-validate** option on the **request system software install** command.

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 *Junos OS Installation and Upgrade Guide*.

NOTE: With Junos OS Release 9.0 and later, the compact flash disk memory requirement for Junos OS is 1 GB. For M7i and M10i routers with only 256 MB memory, see the Customer Support Center JTAC Technical Bulletin PSN-2007-10-001 at **https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2007-10-001&actionBtn=Search**.

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

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

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

The download and installation process for Junos OS Release 12.1 is the same as for previous Junos OS releases.

If you are not familiar with the download and installation process, follow these steps:

1. Using a Web browser, follow the links to the download URL on the Juniper Networks Web page. Choose either **Canada and U.S. Version** or **Worldwide Version**:
   - https://www.juniper.net/support/csc/swdist-domestic/ (customers in the United States and Canada)
   - https://www.juniper.net/support/csc/swdist-ww/ (all other customers)
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. Download the software to a local host.
4. Copy the software to the routing platform or to your internal software distribution site.
5. 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.**

   Customers in the United States and Canada use the following command:

   ```
   user@host> request system software add validate reboot
   source/jinstall-12.1B25-domestic-signed.tgz
   ```

   All other customers use the following command:

   ```
   user@host> request system software add validate reboot
   source/jinstall-12.1B25-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 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 can take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 12.1 **jinstall** package, you cannot issue the **request system software rollback** command to return to the previously installed software. Instead you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

NOTE: Before you upgrade a router that you are using for voice traffic, you should monitor call traffic on each virtual BGF. Confirm that no emergency calls are active. When you have determined that no emergency calls are active, you can wait for nonemergency call traffic to drain as a result of graceful shutdown, or you can force a shutdown. For detailed information on how to monitor call traffic before upgrading, see the *Junos OS Multiplay Solutions 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 10.0, 10.4, and 11.4 are EEOL releases. You can upgrade from Junos OS Release 10.0 to Release 10.4 or even from Junos OS Release 10.0 to Release 11.4. However, you cannot upgrade directly from a non-EEOL release that is more than three releases ahead or behind. For example, you cannot directly upgrade from Junos OS Release 10.3 (a non-EEOL release) to Junos OS Release 11.4 or directly downgrade from Junos OS Release 11.4 to Junos OS Release 10.3.

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 http://www.juniper.net/support/eol/junos.html.

Upgrading a Router with Redundant Routing Engines

If the router has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation as follows:

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

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

Upgrading Juniper Network Routers Running Draft-Rosen Multicast VPN to Junos OS Release 10.1

In releases prior to Junos OS Release 10.1, the draft-rosen multicast VPN feature implements the unicast **lo0.x** address configured within that instance as the source address used to establish PIM neighbors and create the multicast tunnel. In this mode, the multicast VPN loopback address is used for reverse path forwarding (RPF) route resolution to create the reverse path tree (RPT), or multicast tunnel. The multicast VPN loopback address is also used as the source address in outgoing PIM control messages.

In Junos OS Release 10.1 and later, you can use the router's main instance loopback (**lo0.0**) address (rather than the multicast VPN loopback address) to establish the PIM state for the multicast VPN. We strongly recommend that you perform the following procedure when upgrading to Junos OS Release 10.1 if your draft-rosen multicast VPN network includes both Juniper Network routers and other vendors' routers functioning as provider edge (PE) routers. Doing so preserves multicast VPN connectivity throughout the upgrade process.

Because Junos OS Release 10.1 supports using the router's main instance loopback (**lo0.0**) address, it is no longer necessary for the multicast VPN loopback address to match the main instance loopback adddress **lo0.0** to maintain interoperability.

NOTE: **You might want to maintain a multicast VPN instance lo0.x address to use for protocol peering (such as IBGP sessions), or as a stable router identifier, or to support the PIM bootstrap server function within the VPN instance.**

Complete the following steps when upgrading routers in your draft-rosen multicast VPN network to Junos OS Release 10.1 if you want to configure the routers's main instance loopback address for draft-rosen multicast VPN:

1. Upgrade all M7i and M10i routers to Junos OS Release 10.1 before you configure the loopback address for draft-rosen Multicast VPN.

NOTE: **Do not configure the new feature until all the M7i and M10i routers in the network have been upgraded to Junos OS Release 10.1.**

2. After you have upgraded all routers, configure each router's main instance loopback address as the source address for multicast interfaces. Include the **default-vpn-source interface-name *loopback-interface-name*]** statement at the **[edit protocols pim]** hierarchy level.
3. After you have configured the router's main loopback address on each PE router, delete the multicast VPN loopback address (**lo0.x**) from all routers.

   We also recommend that you remove the multicast VPN loopback address from all PE routers from other vendors. In Junos OS releases prior to 10.1, to ensure interoperability with other vendors' routers in a draft-rosen multicast VPN network, you had to perform additional configuration. Remove that configuration from both the Juniper Networks routers and the other vendors' routers. This configuration should be on Juniper Networks routers and on the other vendors' routers where you configured the lo0.mvpn address in each VRF instance as the same address as the main loopback (lo0.0) address.

   This configuration is not required when you upgrade to Junos OS Release 10.1 and use the main loopback address as the source address for multicast interfaces.

NOTE: **To maintain a loopback address for a specific instance, configure a loopback address value that does not match the main instance address (lo0.0).**

For more information about configuring the draft-rosen Multicast VPN feature, see the *Junos OS Multicast Configuration Guide*.

Upgrading the Software for a Routing Matrix

A routing matrix can use either a TX Matrix router as the switch-card chassis (SCC) or a TX Matrix Plus router as the switch-fabric chassis (SFC). By default, when you upgrade software for a TX Matrix router or a TX Matrix Plus router, the new image is loaded onto the TX Matrix or TX Matrix Plus router (specified in the Junos OS CLI by using the **scc** or **sfc** option) and distributed to all T640 routers or T1600 routers in the routing matrix (specified in the Junos OS CLI by using the **lcc** option). To avoid network disruption during the upgrade, ensure the following conditions before beginning the upgrade process:

- A minimum of free disk space and DRAM on each Routing Engine. The software upgrade will fail on any Routing Engine without the required amount of free disk space and DRAM. To determine the amount of disk space currently available on all Routing Engines of the routing matrix, use the CLI **show system storage** command. To determine the amount of DRAM currently available on all the Routing Engines in the routing matrix, use the CLI **show chassis routing-engine** command.
- The master Routing Engines of the TX Matrix or TX Matrix Plus router (SCC or SFC) and T640 routers or T1600 routers (LCC) are all re0 or are all re1.
- The backup Routing Engines of the TX Matrix or TX Matrix Plus router (SCC or SFC) and T640 routers or T1600 routers (LCC) are all re1 or are all re0.

- All master Routing Engines in all routers run the same version of software. This is necessary for the routing matrix to operate.
- All master and backup Routing Engines run the same version of software before beginning the upgrade procedure. Different versions of the Junos OS can have incompatible message formats especially if you turn on GRES. Because the steps in the process include changing mastership, running the same version of software is recommended.
- For a routing matrix with a TX Matrix router, the same Routing Engine model is used within a TX Matrix router (SCC) and within a T640 router (LCC) of a routing matrix. For example, a routing matrix with an SCC using two RE-A-2000s and an LCC using two RE-1600s is supported. However, an SCC or an LCC with two different Routing Engine models is not supported. We suggest that all Routing Engines be the same model throughout all routers in the routing matrix. To determine the Routing Engine type, use the CLI **show chassis hardware | match routing command**.
- For a routing matrix with a TX Matrix Plus router, the SFC contains two model RE-DUO-C2600-16G Routing Engines, and each LCC contains two model RE-DUO-C1800-8G Routing Engines.

NOTE: It is considered best practice to make sure that all master Routing Engines are re0 and all backup Routing Engines are re1 (or vice versa). For the purposes of this document, the master Routing Engine is re0 and the backup Routing Engine is re1.

To upgrade the software for a routing matrix, perform the following steps:

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine (re0) and save the configuration change to both Routing Engines.
2. Install the new Junos OS release on the backup Routing Engine (re1) while keeping the currently running software version on the master Routing Engine (re0).
3. Load the new Junos OS on the backup Routing Engine. After making sure that the new software version is running correctly on the backup Routing Engine (re1), switch mastership back to the original master Routing Engine (re0) to activate the new software.
4. Install the new software on the new backup Routing Engine (re0).

For the detailed procedure, see the Routing Matrix with a TX Matrix Feature Guide or the Routing Matrix with a TX Matrix Plus Feature Guide.

Upgrading Using ISSU

Unified in-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic. Unified in-service software upgrade is only supported by dual Routing Engine platforms. In addition, graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) must be enabled. For additional information about using unified in-service software upgrade, see the *Junos High Availability Configuration Guide*.

Upgrading from Junos OS Release 9.2 or Earlier on a Router Enabled for Both PIM and NSR

Junos OS Release 9.3 introduced NSR support for PIM for IPv4 traffic. However, the following PIM features are not currently supported with NSR. The commit operation fails if the configuration includes both NSR and one or more of these features:

- Anycast RP
- Draft-Rosen multicast VPNs (MVPNs)
- Local RP
- Next-generation MVPNs with PIM provider tunnels
- PIM join load balancing

Junos OS 9.3 Release introduced a new configuration statement that disables NSR for PIM only, so that you can activate incompatible PIM features and continue to use NSR for the other protocols on the router: the **nonstop-routing disable** statement at the **[edit protocols pim]** hierarchy level. (Note that this statement disables NSR for all PIM features, not only incompatible features.)

If neither NSR nor PIM is enabled on the router to be upgraded or if one of the unsupported PIM features is enabled but NSR is not enabled, no additional steps are necessary and you can use the standard upgrade procedure described in other sections of these instructions. If NSR is enabled and no NSR-incompatible PIM features are enabled, use the standard reboot or ISSU procedures described in the other sections of these instructions.

Because the **nonstop-routing disable** statement was not available in Junos OS Release 9.2 and earlier, if both NSR and an incompatible PIM feature are enabled on a router to be upgraded from Junos OS Release 9.2 or earlier to a later release, you must disable PIM before the upgrade and reenable it after the router is running the upgraded Junos OS and you have entered the **nonstop-routing disable** statement. If your router is running Junos OS Release 9.3 or later, you can upgrade to a later release without disabling NSR or PIM—simply use the standard reboot or ISSU procedures described in the other sections of these instructions.

To disable and reenable PIM:

1. On the router running Junos OS Release 9.2 or earlier, enter configuration mode and disable PIM:

   ```
   [edit]
   user@host# deactivate protocols pim
   user@host# commit
   ```

2. Upgrade to Junos OS Release 9.3 or later software using the instructions appropriate for the router type. You can either use the standard procedure with reboot or use ISSU.

3. After the router reboots and is running the upgraded Junos OS, enter configuration mode, disable PIM NSR with the **nonstop-routing disable** statement, and then reenable PIM:

```
[edit]
user@host# set protocols pim nonstop-routing disable
user@host# activate protocols pim
user@host# commit
```

Downgrade from Release 12.1

To downgrade from Release 12.1 to another supported release, follow the procedure for upgrading, but replace the 12.1 **jinstall** package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases. For example, if your routing platform is running Junos OS Release 11.4, you can downgrade the software to Release 10.4 directly, but not to Release 10.3 or earlier; as a workaround, you can first downgrade to Release 10.4 and then downgrade to Release 10.3.

For more information, see the *Junos OS Installation and Upgrade Guide*.

Related Documentation

- New Features in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 135
- Changes in Default Behavior and Syntax, and for Future Releases in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 174
- Issues in Junos OS Release 12.1 for M Series, MX Series, and T Series Routers
- Errata and Changes in Documentation for Junos OS Release 12.1 for M Series, MX Series, and T Series Routers on page 185

Junos OS Documentation and Release Notes

For a list of related Junos OS documentation, see http://www.juniper.net/techpubs/software/junos/ .

If the information in the latest release notes differs from the information in the documentation, follow the *Junos OS Release Notes.*

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/ .

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at http://www.juniper.net/books .

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/customers/support/downloads/710059.pdf.
- Product warranties—For product warranty information, visit http://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: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

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

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html.

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

`user@host>` **request support information** | **save** *filename*

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net:pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to **support@juniper.net**. For documentation issues, fill out the bug report form located at https://www.juniper.net/cgi-bin/docbugreport/.

Revision History

23 February 2012—Revision 5, Junos OS 12.1 B2 – High End SRX Series, Branch SRX Series, J Series, EX Series, M Series, MX Series, and T Series.

31 January 2012—Revision 4, Junos OS 12.1 B1 – High End SRX Series, Branch SRX Series, J Series, EX Series, M Series, MX Series, and T Series.

27 December 2011—Revision 3, Junos OS 12.1 B1 – High End SRX Series, Branch SRX Series, J Series, EX Series, M Series, MX Series, and T Series.

16 December 2011—Revision 2, Junos OS 12.1 B1 – High End SRX Series, Branch SRX Series, J Series and EX Series

5 December 2011—Revision 1, Junos OS 12.1 B1 – High End SRX Series, Branch SRX Series, and J Series