

JUNOS 7.2 Internet Software Release Notes

Release 7.2R4
15 August 2006
Part No: 530-013082-01
Revision 4

These release notes accompany Release 7.2R4 of the JUNOS Internet software. They describe the documentation for the routing platforms and known problems with the software. JUNOS software runs on all Juniper Networks J-series, M-series, and T-series platforms.

You can also find these release notes on the Juniper Networks Technical Publications Web page, which is located at <http://www.juniper.net/techpubs/>.

Contents

Release 7.2 Features	3
Current Software Release	10
Resolved Issues	10
Outstanding Issues	15
Previous Releases	26
Release 7.2R3	26
Release 7.2R2	28
Release 7.2R1	39
Errata	45
M-series and T-series Upgrade and Downgrade Instructions	46
Upgrade to Release 7.2	46
Downgrade from Release 7.2	48
J-series Upgrade and Downgrade Instructions	48
Upgrade Instructions	48
Before You Begin	49
About the junos-jservice Package	49
Installing Software Upgrades with the J-Web Interface	50
Installing Software Upgrades from a Remote Server	50
Installing Software Upgrades by Uploading Files	51

Installing Software Upgrades with the CLI	51
Downgrade Instructions	52
Downgrading the Software with the J-Web Interface	53
Downgrading the Software with the CLI	53
List of Technical Publications	53
Requesting Support	57
Revision History	58

Release 7.2 Features

The following features have been added to JUNOS Release 7.2. The identifier following the description is the short title of the manual or manuals to consult for further information. For a complete list of manuals, see Table 4.

Changes in Default Behavior and Syntax

- Combinations of PICs—On Juniper Networks routing platforms, you can typically install any combination of Physical Interface Cards (PICs) on a single Enhanced Flexible PIC Concentrator (FPC). On M5, M10, M20, M40, M40e, M160, and J20 routers, there are some combinations of PICs that cannot be installed together on the same Enhanced FPC. For more information, please consult Technical Bulletin PSN-2005-03-009 on the Juniper Networks Support Web site at <http://www.juniper.net/support/>. M20 and M40e routers with an Enhanced Plus FPC do not have these constraints.
- JUNOS-FIPS—JUNOS-FIPS is a version of the JUNOS operating system that meets the requirements of Federal Information Processing Standard (FIPS) PUB 140-2. The installation procedure for JUNOS-FIPS is different from the one you normally perform for JUNOS. [*JUNOS-FIPS Configuration Guide*]
- Adaptive Services PIC—For the Adaptive Services PIC, the Compressed Real-Time Transport Protocol (CRTP) is currently included in both the Layer 2 and Layer 3 services packages. Starting in JUNOS Release 7.5, CRTP will be included in the Layer 2 service package only. To enable a service package, include the `service-package` statement at the `[edit chassis fpc slot-number pic pic-number adaptive-services]` hierarchy level, and specify `layer-2` or `layer-3`. [*Services Interfaces, Network Interfaces*]
- Ethernet VLAN-tagged network-control packets—By default, starting in JUNOS Release 6.4R3 and 7.0R1, Ethernet virtual LAN (VLAN)-tagged network-control packets have IEEE 802.1p bits set to 110. Previously, these bits were set to 000 by default. [*Network Interfaces*]
- Starting in JUNOS Release 7.2, IP precedence rewrite rules by default alter the first three bits on the type-of-service (ToS) byte while leaving the last three bits unchanged. Previously, all six bits in the ToS byte were altered by IP precedence rewrite rules. This new default behavior is not configurable, which means the previous implementation cannot be used for Release 7.2 and above. The new default behavior applies to rules you configure by including the `inet-precedence` statement at the `[edit class-of-service rewrite-rules]` hierarchy level. The new default behavior also applies to rewrite rules you configure for Multiprotocol Label Switching (MPLS) packets with IP version 4 (IPv4) payloads. You configure these types of rewrite rules by including the `mpls-inet-both` or `mpls-inet-both-non-vpn` option at the `[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules exp rewrite-rule-name protocol]` hierarchy level. [*Network Interfaces*]
- Default MTU modification for E3 IQ and Channelized DS3 IQ PICs (M40e and M160 routers)—The default physical interface MTU on E3 IQ and Channelized

DS3 IQ PICs installed in M40e and M160 routers has changed to 9192.
[*Network Interfaces*]

- Previously, the JUNOS software dropped Neighbor Discovery Protocol (NDP) packets if the source addresses of the packets were not reachable through the interface that received the packets. In order to comply with RFC 2461, starting in JUNOS Release 7.2R1, the software enters the packets into the routing platform's cache, even if there is no known route to the source. [*Routing*]
- Modifications to MLPPP processing on link services IQ interfaces (Adaptive Services PICs)—Provides RFC 1990-compliant Multilink Point-to-Point Protocol (MLPPP) interoperability with other vendors' equipment. The routing platform now compares the local family maximum transmission unit (MTU) with the maximum received reconstructed unit MRRU of the remote peer. If the MRRU of the peer is lower than the local family MTU, the routing platform adjusts the family MTU by lowering the bundle link MTU. In addition, the MRRU or MTU values of the remote peer do not overwrite the family MTU value unless the new value is smaller than the current one. The new functionality is available by default when you configure MLPPP on link services intelligent queuing (IQ) interfaces. Previously, the MRRU of the remote peer was compared with the local MRRU, and the MRRU or MTU values of the remote peer might have overwritten the family MTU value incorrectly. [*Services Interfaces*]
- Revised backup router requirement for graceful Routing Engine switchover and routing matrix topologies—Requires you to configure a routing platform destination when you specify a backup router for graceful Routing Engine switchover or for a T640 routing node in a routing matrix. To specify a destination for an IPv4 network, include the `destination` statement at the [edit system backup-router] hierarchy level. To specify a destination for an IP version 6 (IPv6) network, include the `destination` statement at the [edit system inet6-backup-router] hierarchy level. [*System Basics*]
- The `include` statement configured at the [edit protocols mpls label-switched-path *lsp-name* admin-group] hierarchy level has been deprecated and replaced with the `include-any` statement. If you upgrade to the current JUNOS software release, any `include` statements in your configuration are changed to `include-any` statements. If you then downgrade to a previous release, you need to change the `include-any` statements back to `include` statements before committing the configuration; otherwise the commit operation will fail. For more information, see also the `include-any` statement feature description in the *MPLS Applications* section. [*MPLS Applications*]

Interfaces and Chassis

- IDS flow limitation—Enables you to specify thresholds for limiting the number of open intrusion detection services (IDS) sessions. To configure, include the `session-limit` statement at the [edit services ids rule *term* then] hierarchy level. You can limit stateful firewall and network address translation (NAT) flows by destination, by source, or by pair. You can also specify thresholds for maximum number of sessions, number of sessions per second, and packets per second, as well as a hold time during which the flows are stopped. The

`show services ids` command supports new anomaly types that describe this behavior. [*Services Interfaces, Command Reference: Interfaces*]

- Enhancement to `show services` command output—Supports improved displays for multiple service sets in the output of the `show services` family of commands. A new `count` keyword is added for the `show services stateful-firewall conversations` command. [*Command Reference: Interfaces*]
- AS PIC service packages (AS PICs on all platforms and the ASM in the M7i platform)—Enables you to configure the PIC to support the Layer 2 or Layer 3 service package. In general, the Layer 2 service package includes link services and tunnel services. The Layer 3 service package includes security, accounting, tunnel, Layer 2 Tunneling Protocol (L2TP) network server (LNS), and voice services. The specific services supported in each package differ by PIC and platform type. To configure a service package on an Adaptive Services (AS) PIC or Adaptive Services Module (ASM), include the `service-package` statement at the `[edit chassis fpc slot-number pic pic-number adaptive-services]` hierarchy level. [*Network Interfaces, Services Interfaces, Command Reference: Interfaces*]
- LSQ interfaces (AS PICs on all platforms and the ASM in the M7i platform)—Once you configure an AS PIC or ASM to support the Layer 2 service package, you can also configure link services intelligent queuing (LSQ) interfaces on the PIC. LSQ interfaces support JUNOS software class-of-service (CoS) components, link fragment interleaving (LFI) (FRF.12), Multilink Frame Relay user-to-network interface network-to-network interface (MLFR UNI NNI) (FRF.16), and MLPPP (defined in RFC 1990, *The PPP Multilink Protocol (MP)*). To configure, include the `service-package` statement at the `[edit chassis fpc slot-number pic pic-number adaptive-services]` hierarchy level, and specify `layer-2`; for MLPPP, include the `bundle lsq-fpc / pic / port .logical-unit-number` statement at the `[edit interfaces interface-name unit logical-unit-number encapsulation ppp family mlppp]` hierarchy level; for FRF.16, include the `mlfr-uni-nni-bundles` statement at the `[edit chassis fpc slot-number pic slot-number]` hierarchy level and the `bundle lsq-fpc / pic / port :channel` statement at the `[edit interfaces interface-name unit logical-unit-number family mlfr-uni-nni]` hierarchy level. For LSQ interfaces, JUNOS CoS components are fully supported and are handled normally. Additionally, you can configure the percentage of total bundle bandwidth to be set aside for link-layer overhead by including the `link-layer-overhead` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level; and you can define fragmentation properties for individual forwarding classes by including the `fragmentation-maps` statement at the `[edit class-of-service]` hierarchy level. [*Network Interfaces, Services Interfaces, Command Reference: Interfaces*]
- CRTP for LSQ interfaces (AS PICs on all platforms and the ASM in the M7i platform)—Provides expanded support for CRTP to LSQ interfaces on the AS PIC and the ASM in the M7i platform. To configure, include the `rtp` statement at the `[edit interfaces lsq-fpc / pic / port unit logical-unit-number compression]` hierarchy level. [*Services Interfaces, Network Interfaces*]
- MCML for LSQ (`lsq`) interfaces (AS PICs on all platforms and the ASM in the M7i platform)—Provides support for Multiclass Multilink (MCML) PPP, as defined in RFC 2686, *The Multi-Class Extension to Multi-Link PPP*. MCML is an extension to Multilink PPP that makes it possible to carry multiple classes of

latency-sensitive traffic over a single multilink bundle along with bulk traffic. To configure, include the `multilink-class` statement at the `[edit class-of-service fragmentation-map map-name forwarding-class class-name]` hierarchy level. [*Network Interfaces, Services Interfaces*]

- Eight egress CoS queues on ATM2 IQ interfaces (T-series and M320 platforms)—Enables you to configure eight egress queues on Asynchronous Transfer Mode 2 (ATM2) IQ interfaces. There is a restriction on random early drop (RED) profile selection for these queues. The ATM2 cookie can only accommodate four RED profile indices and the field-programmable gate array (FPGA) selects the RED profile based on just two Q bits. Q0 and Q4 share the same RED profile index, as do Q1 and Q5, Q2 and Q6, and Q3 and Q7. To configure, include the `max-queues-per-interface` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level, and specify the 8 option; include the `linear-red-profiles` and `scheduler-maps` statements at the `[edit interfaces at-fpc / pic / port atm-options]` hierarchy level; and include the `classifiers` statement at the `[edit class-of-service]` hierarchy level. [*Network Interfaces*]
- Unrestricted proxy ARP (Ethernet interfaces on all platforms)—Enables the router to respond to any Address Resolution Protocol (ARP) request, on condition that the router has an active route to the ARP request's target address. This is especially useful for routers that are acting as provider edge (PE) devices in Ethernet Layer 2 LAN switching domains. To configure, include the `proxy-arp` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level. To track the number of unrestricted proxy ARP requests processed by the router, issue the `show system statistics arp operational-mode` command. [*Network Interfaces, Command Reference: Interfaces*]
- You can configure J-series routers to execute a `show system alarms` command whenever a user who belongs to the `admin` login class logs on to the router. [*System Basics*]
- Two new system alarms are available. A configuration alarm appears when no rescue configuration is set. A license alarm appears when a software feature is configured on the router and no valid license is configured for that feature. [*System Basics*]
- Flexible allocation of DLCIs to ports in 4-port E3 IQ PIC—Increases the number of configurable data-link connection identifiers (DLCIs) per E3 IQ interface from 160 to 1022. The number of queued DLCIs you can configure per E3 IQ PIC remains 752. You can configure the 752 queued DLCIs on a single E3 IQ interface, or you can divide them among the four E3 IQ interfaces. To configure DLCIs, include the `dci` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level. To configure queued DLCIs, include the `per-unit-scheduler` statement at the `[edit interfaces interface-name]` hierarchy level and include the `scheduler-map` the `shaping-rate` statements at the `[edit class-of-service interfaces interface-name unit logical-unit-number]` hierarchy level. [*Network Interfaces*]
- Passive ARP learning for backup Virtual Router Redundancy Protocol (VRRP) routers—Enables the backup router to learn the IP-to-media access control (MAC) address mapping for the hosts sending ARP requests. This causes the

backup ARP cache to hold approximately the same contents as the ARP cache in the primary router, thus preventing the problem of learning ARP entries in a burst, when the backup router becomes the primary router. To enable passive ARP learning, include the `passive-learning` statement at the `[edit system arp]` hierarchy level. [*Network Interfaces, System Basics*]

- Adjustable ARP aging timer—Allows you to configure the ARP aging timer explicitly. To configure, include the `aging-timer` statement at the `[edit system arp]` hierarchy level. The configurable range is 20 through 240 minutes. [*Network Interfaces, System Basics*]
- FPC settings—The `show chassis hardware` command now displays new FPC settings on M20 and M40e routers. The new Enhanced Plus FPC on the M20 router is listed as `FPC-EP` and the new Enhanced Plus FPC on the M40e router is listed as `M40E-FPC1 EP`. [*System Basics*]
- Graceful switchover for adaptive services—You can configure graceful switchover for routers in which AS PICs are installed. When a Routing Engine switchover occurs, features using adaptive services are interrupted momentarily, much as when a PIC or process is restarted on a single Routing Engine. Features that do not use adaptive services continue uninterrupted. After switchover, all features are restored and packet forwarding continues. Note, however, that L2TP does not come up after a graceful switchover. [*System Basics*]
- Modification to the operation of flow collection services—When you configure a flow collector interface on a Monitoring Services PIC, the following functionality is now the default behavior:
 - You must configure a default flow collector interface. To do so, include the `collector cp-fpc / pic / port` statement at the `[edit services flow-collector interface-map]` hierarchy level.
 - If you do not map an input interface to a specific flow collector interface, the input interface uses the default flow collector interface. To reference a specific flow collector interface for an input interface, include the `collector cp-fpc / pic / port` statement at the `[edit services flow-collector interface-map interface-name]` hierarchy level.
 - If a flow collector interface is mapped to a specific input interface and the flow collector interface stops operating, the flows created for the input interface are discarded and not rerouted to the default flow collector interface.

[*Feature Guide, Services Interfaces*]

- LNS support on the Adaptive Services PIC for the M10i router—Adds support for LNS on the Adaptive Services PIC for M10i routers. [*Network Interfaces*]
- It is now possible to display output for a single interface when you issue the `show rsvp interface interface-name` command. [*Protocols Command Reference*]

Routing Protocols

- MSDP in virtual private network (VPN) routing and forwarding (VRF) routing instances—Specifies the Multicast Source Discovery Protocol (MSDP) for a routing instance. For more information about configuring MSDP, see the *JUNOS Multicast Protocols Configuration Guide*. To configure, include the `msdp` statement at the `[edit routing-instances protocols]` hierarchy level. [*Routing Protocols*]
- OSPF active backbone detection—The JUNOS software now supports active backbone detection. There are two changes in Open Shortest Path First (OSPF) default behavior associated with active backbone detection, but there are no new configuration statements. First, if an area border router (ABR) loses its OSPF adjacency to backbone area 0, then the router no longer announces the default into connected stub areas or not-so-stubby areas (NSSAs) via the configuration under the `nssa` or `stub default-metric` statements at the `[edit protocols ospf]` hierarchy level. This makes it possible to reroute traffic through another ABR that has an active adjacency to backbone area 0. Second, an ABR with no active backbone area 0 adjacency now considers inter-area traffic destined to areas that are not directly connected to that ABR. This change does not obviate the need for virtual links in the case of a partitioned area. [*Routing Protocols*]
- IP Security (IPSec) authentication for OSPFv3—Provides a method for protecting and securing the OSPF traffic through the router. OSPF version 3 (OSPFv3) uses authentication header (AH) and the IP Encapsulating Security Payload (ESP) protocols to authenticate routing information. To configure, include the `ipsec-sa` statement at the `[edit protocols ospf area area-id interface interface-name]` hierarchy level. [*Routing Protocols*]
- Routing table path selection—For each prefix in the routing table, the routing protocol process selects a single best path, called the active route. For paths that include an autonomous system (AS) path, by default only the multiple exit discriminators (MEDs) of routes that have the same peer ASs are compared. However, you can modify this behavior by configuring one of the routing table path selection options for the `path-selection` statement included at the `[edit protocols bgp]` hierarchy level. The original options are `cisco-non-deterministic` (which mimics the behavior of Cisco IOS software) and `always-compare-med` (which compares MEDs whether or not the ASs of the compared routes are the same). The new `external-router-id` option allows you to compare the router ID between external Border Gateway Protocol (BGP) paths to determine the active path. By default, router ID comparison is not performed if one of the external paths is active. [*Routing Protocols*]

MPLS Applications

- Enhanced load balancing for MPLS—Per-packet load balancing for MPLS over IP enables you to load balance traffic based on the information in the IP header, as well as on the MPLS header. This enables you to better distribute network traffic to next hops. [*MPLS Applications*]
- You can now include the `include-any` statement at the `[edit protocols mpls label-switched-path lsp-name admin-group]` hierarchy level. A label switched path

(LSP) configured with the `include-all` statement can traverse only links that have all the administration groups specified in the `include-all` statement. For more information, see the `include-any` statement description in the *Changes in Default Behavior and Syntax* section. [*MPLS Applications*]

Multicast

- MSDP statement enhancement—MSDP statements are now configurable for the following routing instance types: `forwarding`, `no-forwarding`, `virtual-router`, `vpls`, and `vrf`. MSDP configuration statements are not configurable at the same hierarchy levels as are Protocol Independent Multicast (PIM) configuration statements. [*Multicast*]

Routing Policy and Firewall Filters

- DHCP server—You can configure a J-series router or interface to act as a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server can allocate network IP addresses and deliver configuration settings to clients on a Transmission Control Protocol (TCP)/IP network. [*System Basics*]
- Allow lists for tag match—You can specify multiple tags under one match condition by including the tags within a bracketed list, for example: `from tag [tag1 tag2 tag3]`. To configure, include the tag list at the `[edit policy-options policy-statement term from]` hierarchy level. [*Policy Framework*]

System Basics

- Software upgrade enhancements—Adds new options to assist with software upgrades:
 - Use the new `request system storage cleanup` command to free system storage space before performing a software upgrade. With confirmation, this command rotates log files, deletes log files in `/var/log` that are not currently being written to. This command also deletes temporary files in `/var/tmp` that have not been touched in two days, and deletes all crash files in `/var/crash`.
 - On J-series Services routers, when you upgrade to a new software package from a remote location using the `request system software add validate package-name` command, the package is removed at the earliest opportunity in order to make room for the installation to be completed. If you copy the software to a local directory on the router and then install the new package, use the new `unlink` option with the `request system software add validate package-name` command to achieve the same effect and allow the installation to complete.
 - On M-series and T-series routers, use the `unlink` option with the `request system software add validate package-name` command to remove the software package after a successful upgrade is completed.

[*System Basics, Command Reference: System Basics and Services*]

VPNs

- You can filter traffic based on the IP header by including the `vrf-table-label` statement at the `[edit routing-instance routing-instance-name]` hierarchy level. This statement is now supported for aggregated and VLAN interfaces on M-series routers equipped with enhanced FPCs. [VPNs]

JUNOScript and other APIs

- JUNOScript support for private configuration—Enables JUNOScript client applications to create a private copy of the configuration (equivalent to the `configure private` command-line interface [CLI] command). The client application emits the following tag sequence: `<open-configuration> <private/> </open-configuration>`. The interaction between operations on the locked regular candidate configuration and a private copy is the same as in the CLI (described in the *JUNOS System Basics Configuration Guide*). The client application can perform the same operations on a private copy as on the regular candidate configuration. [JUNOScript API Guide]
- Table 1 lists the new JUNOScript tags and their corresponding CLI commands. [JUNOScript Reference]

Table 1: JUNOS 7.2 JUNOScript Tags and Equivalent CLI Commands

Request Tag	Response Tag	CLI Command
<code><get-fips-pic-status-information></code>	<code><fips-pic-status-information></code>	<code>show services fips pic status</code>
<code><get-interface-optics-diagnostics-information></code>	<code><interface-optics-diagnostics-information></code>	<code>show interfaces diagnostics optics</code>
<code><get-rtflow-dep-information></code>	<code><rtflow-dep-information></code>	<code>show route flow validation</code>
<code><get-service-deployment-service-information></code>	<code><service-deployment-service-information></code>	<code>show system services service-deployment</code>
<code><get-system-alarm-information></code>	<code><alarm-information></code>	<code>show system alarms</code>

Current Software Release

The current software release is Release 7.2R4. For information about obtaining the software packages, see “Upgrade to Release 7.2” on page 46.

Resolved Issues

The following issues have been resolved since JUNOS Release 7.2R3. The identifier following the description is the tracking number in our bug database.

Platform and Infrastructure

- When you configure the last octet of a Network Time Protocol (NTP) source address in the range of 224 to 239 with the `source-address` statement at the `[edit system ntp source-address]` hierarchy level, an “attempt to configure invalid address” system log error message might be generated. [PR/60200: This issue has been resolved.]
- On T-series platforms, Address Resolution Protocol (ARP) next-hop resolution might not work as expected. [PR/61488: This issue has been resolved.]
- On E1 and T1 interface links, you might observe very low BGP and TCP throughput. A workaround is to increase the physical interface MTU value to 9K. In addition, TCP retransmissions in general may stall the TCP connections. As a workaround, contact JTAC for instructions on how to disable RFC 1323 for all TCP connections. [PR/64682: This issue has been resolved.]
- When you include the `on-disk-failure` statement at the `[edit chassis redundancy failover]` hierarchy level and the `graceful-switchover enable` statement at the `[edit chassis redundancy]` hierarchy level, the commit fails. As a workaround, also include the `on-loss-of-keepalives` statement at the `[edit chassis redundancy failover]` hierarchy level. [PR/64817: This issue has been resolved.]
- When the `daemon` statement is included at the `[edit system syslog console]` hierarchy level, some daemons might not start after a graceful restart operation. [PR/65413: This issue has been resolved.]
- On an M320 or T-series routing platform, if you install a Tunnel Services PIC in the same FPC as a PIC used as an outbound interface for port mirrored traffic, then port mirror and loop traffic from an inbound interface through a virtual loopback tunnel (vt) interface to the outbound interface, output filters might not work. As a workaround, install the Tunnel Services PIC and the PIC containing the outbound interface in different FPCs. [PR/65444: This issue has been resolved.]
- Lchip configuration was not cleaned up properly after failed to bring up lchip-pic link. [PR/66083: This issue has been resolved.]
- If you configure an output filter on a discard interface, the filter might not work, traffic might not be forwarded, and the firewall filter counters might not increment in the output of the `show firewall filter` command. [PR/67663: This issue has been resolved.]

User Interface and Configuration

- JUNOS Release 6.4R4 does not recognize trailing spaces included in secret passwords generated by encryption algorithms. Previous releases handled this occurrence differently, causing a disparity in behavior. [PR/63967: This issue has been resolved.]
- Setting of discontinuous prefixes are not recorded properly. [PR/64857: This issue has been resolved.]

- If you configure a user login class with the `class` statement at the `[edit groups group-name system login]` hierarchy level, the user might not be assigned a valid login class. As a workaround, configure login classes for users at the `[edit system login]` hierarchy level. [PR/65146: This issue has been resolved.]
- With some `apply-group` configurations, the command-line parser might hang when executing a `commit` or `commit check` function. [PR/65365: This issue has been resolved.]

Interfaces and Chassis

- On ATM interfaces configured with Automatic Protection Switching (APS), if the working and protect circuits are forced to switch back and forth every five seconds for more than an hour, both circuits might be enabled at the same time in error. [PR/55493: This issue has been resolved.]
- If the `show interfaces` command is issued during a configuration operation, such as the creation or deletion of an interface, the CLI stops operating. This happens rarely, and there is no operational impact. As a workaround, terminate the CLI session and run the same command in another CLI session. [PR/59707: This issue has been resolved.]
- For IQ PICs on M160 and M40e platforms, the physical interface traffic statistics for input packets and bytes are sometimes displayed incorrectly as all zeroes. [PR/61864: This issue has been resolved.]
- If a Routing Engine switchover occurs due to graceful Routing Engine switchover (GRES), and Automatic Protection Switching (APS) is used in a multirouter configuration, traffic on the APS-protected circuit might be lost for up to five seconds. [PR/64211: This issue has been resolved.]
- Corruption in `chassisd` causes the router to report temperature sensor failure alarms for T-series routing platform PEMs [PR/64551: This issue has been resolved.]
- The output from the `show aps detail` and `show aps extensive` operational-mode commands provides correct information, but the data is not well formatted. [PR/64662: This issue has been resolved.]
- If you issue the `show interfaces controller interface-name` command, the routing platform might stop operating and dump core. [PR/65284: This issue has been resolved.]
- When you install a 10-port Gigabit Ethernet PIC into an FPC and insert copper small form-factor pluggable transceivers (SFPs) into the PIC, then issue the `ping` command, the response time of the ping might be delayed by several hundred milliseconds. [PR/65315: This issue has been resolved.]

- On adaptive services interfaces, when the PIC or the routing platform reboots, the MTU configured for the protocol family might be overwritten by the device MTU. [PR/65331: This issue has been resolved.]
- On Channelized IQ PICs connected to J-series Services Routers, when you configure time slots for E1 or T1 channels and commit the configuration, the T1 and E1 interfaces might go down and up. [PR/65838: This issue has been resolved.]

Services Applications

- If you issue the `show services l2tp session` command, the following options might be missing and unavailable: `interface`, `local-gateway`, `local-gateway-name`, `local-tunnel-id`, `peer-gateway`, `peer-gateway-name`, and `tunnel-group`. [PR/65135: This issue has been resolved.]
- When no traffic is received from a PPP client, the Layer 2 Tunneling Protocol (L2TP) network server (LNS) might not send a PPP keepalive. [PR/65855: This issue has been resolved.]

General Routing

- When you change the BGP path selection method with the `path-selection` statement at the `[edit protocols bgp]` hierarchy level, the routing protocol process (`rpd`) might stop operating. [PR/65323: This issue has been resolved.]

Routing Protocols

- When an existing source active (SA) route to the rendezvous point (RP) changes, the Multicast Source Discovery Protocol (MSDP) active-source limit might not work correctly. [PR/61754: This issue has been resolved.]
- If a BGP peer flaps while a routing instance is added to the configuration, the routing protocol process (`rpd`) might restart. [PR/64625: This issue has been resolved.]
- A provider edge (PE) router acting as a rendezvous point (RP) for a PIM routing instance might not send a register-stop message if the designated router (DR) of the multicast source is sending PIM registers in version 1 format. This situation results in redundant traffic on the network, in the form of data-encapsulated PIM register packets. The workaround is to configure the source DR as PIM version 2. [PR/65101: This issue has been resolved.]
- If the router receives an (S,G,rpt) join message for an (S,G) that has an (S,G,rpt) prune state, and no data packets have been sent by the source, the router might stop operating. [PR/65571: This issue has been resolved.]
- For multicast virtual private networks (VPNs), if the forwarding cache downstream interface list excludes a customer edge (CE) router interface containing local receivers, the local receivers do not receive traffic. As a workaround, deactivate and reactivate IGMP. [PR/65875: This issue has been resolved.]

- If a PIM multicast router has a local source, local receiver, and remote receiver for the same group, and the local source stops sending traffic, the PIM state might not be removed from the router. Additionally, Multicast Source Discovery Protocol (MSDP) might continue to advertise source active (SA) messages for the local source, even after the source has stopped sending traffic. As a result, incorrect PIM state and forwarding state information might remain on other routers in the network. [PR/65919: This issue has been resolved.]
- After an OSPF graceful restart, the restarted router becomes the designated router (DR) or the backup designated router (BDR), even though it was not a DR or BDR before the restart. [PR/65940: This issue has been resolved.]
- If BGP is configured with a rib-group and damping is enabled, the command `clear bgp damping` might cause internal data structures to be corrupted. That might lead to a subsequent RPD restart. [PR/67189: This issue has been resolved.]
- If you configure the BGP path-selection statement at the [edit protocols bgp] hierarchy level when an aggregate or generated route that references a more specific static route is present, then you restart the routing platform, the routing protocol process (rpd) might stop operating. [PR/67567: This issue has been resolved.]

MPLS Applications

- If you enable fast reroute on an LSP and you configure a reoptimization timer, there might be packet loss for traffic passing through the affected LSP. [PR/64426: This issue has been resolved.]
- When you change the RSVP LSP bandwidth configuration and the new bandwidth requirement cannot be met, it is not apparent that the new bandwidth setting fails, sometimes the number of retries are insufficient, and RSVP might retain the old bandwidth state indefinitely. [PR/64870: This issue has been resolved.]
- RSVP might accept incoming hello packets and establish neighbor relationships arriving from any source address, even if the routing platform originated a hello packet from one of its own interfaces. This is a cosmetic issue and there is no operational impact. [PR/65172: This issue has been resolved.]
- After an RSVP signaling failure, MPLS might not accurately enforce bandwidth changes. The `show mpls lsp` command displays the bandwidth that you configure, but it does not show the bandwidth that is actually reserved; this is shown in the output of the `show rsvp session` command. [PR/65608: This issue has been resolved.]

Class of Service

- When you remove an IEEE 802.1p classifier from a logical interface, IEEE 802.1p classification does not function correctly on other logical interfaces that are still configured with IEEE 802.1p classifiers. [PR/63381: This issue has been resolved.]

- On Enhanced FPCs installed in TX Matrix platforms, when the line rate is greater than 40 percent on high-priority fabric queues, packet tail drops might occur. [PR/64178: This issue has been resolved.]
- If you configure a class of service (CoS) attribute for a logical interface, the CoS process (cosd) might leak memory and cause high levels of CPU utilization. [PR/65047: This issue has been resolved.]

Forwarding and Sampling

- On a routing platform configured to send cflowd records, if there is a mismatch of metadata information between the sampling process (sampled) and the routing protocol process (rpd), the sampling process log might continuously receive the system log message “rr DELETE: pref < address > len 24 doesn’t exist.” [PR/66620: This issue has been resolved.]

Network Management

- If the software performs an snmpget operation on jnxPingCtlTable objects with nonexistent indices, the remote operations process (rmopd) might dump core. [PR/65106: This issue has been resolved.]

Outstanding Issues

Software Installation

- For hard disks that were originally formatted by JUNOS Release 4.4 or earlier, after you issue the `request system snapshot partition` command, the router cannot boot from the hard disk. As a workaround, issue the `request system snapshot` command before upgrading. [PR/36742]

Platform and Infrastructure

- When you configure a Challenge Handshake Access Protocol (CHAP) local name with more than 128 characters, characters beyond 128 are truncated and the authentication does not succeed because the `access-profile` client names of sending and receiving interfaces do not match. As a workaround, configure the local name to have no more than 128 characters. [PR/20532]
- When the Monitoring Services PIC is overloaded, the output from the `show services accounting flow-detail` command might freeze. [PR/32896]
- On T-series platforms, a Layer 2 maximum transmission unit (MTU) check is not supported for MPLS packets exiting the routing platform. [PR/46238]
- If you upgrade the routing platform from JUNOS Release 6.2R2.4 to JUNOS Release 6.2R2.5 by issuing the `request system software add` command, the Routing Engine might restart. [PR/49194]

- When you configure the source-class usage (SCU) name as an integer (for example, `source-class 100`), the class ID is the same as the integer value (100). [PR/50247]
- On a T640 routing platform, you can exceed the hardware limit of the platform if you configure link protection by including the `link-protection` statement at the `[edit protocols mpls label-switched-path isp-name]` hierarchy level, or if you configure a triple-push operation by including the `exp-push-push-push` statement at the `[edit class-of-service interfaces interface-name unit logical-unit-number rewrite-rules]` hierarchy level in conjunction with VLAN tagging and Ethernet-based Layer 2 circuit configuration. In the case of link protection, the problem is transitory while the platform changes to link-protection mode. [PR/51688]
- When you configure destination class usage along with the `port-mirroring` statement, port mirroring might stop working. [PR/51916]
- On J-series Services Routers, when you include the `vrf-table-label` statement at the `[edit routing-instances routing-instance-name]` hierarchy level, the incoming traffic is considered to come from the internal label-switched interface (LSI) associated with the VRF instance. The original incoming logical interface is unknown, so the traffic is not accounted for by the original incoming logical unit. Furthermore, the LSI is an internal interface and has no accounting support. [PR/53148]
- When a Monitoring Services PIC is overloaded with traffic, the FPC might take the PIC offline and repeatedly send the same error message. The error message does not seem to affect normal operation of the FPC and PICs. As a workaround, restart the FPC and bring the PIC online. [PR/55981]
- On a J-series Services Router, if you configure a Dynamic Host Control Protocol (DHCP) server and DHCP request traffic arrives at a rate of 100 packets per second or more, the DHCP process (`dhcpd`) might drop some of the requests. [PR/58250]
- On a 2-port OC3 ATM2 Intelligent Queuing (IQ) PIC installed in an M-series router, if both ports use a single input stream and you deactivate one of the two ATM physical interfaces, the VPN routing and forwarding (VRF) table label feature is not supported. [PR/58814]

User Interface and Configuration

- When using `S/Key` with an SSH connection, the challenge might not get displayed. [PR/38715]
- If you use the `netconf` command to modify a configuration data store that has been locked by another `netconf` session, or if you try to delete a configuration statement, that does not exist, you see both `<rpc-error>` and `<ok/>` at the same time in the `<rpc-reply>` tag. [PR/62664]
- When you modify the date on the router, the time at which an event should be generated might be changed from its original configuration at the `[edit event-options generate-event event-name time-of-day hh:mm:ss]` hierarchy level. As a

workaround, issue the `commit full` command after modifying the date on the router. [PR/66801]

Interfaces and Chassis

- On aggregated SONET/SDH interfaces, the counter for drops and errors in the `show interfaces` command output does not display the correct value, because the counter does not collect data from the constituent interfaces within the aggregate. [PR/23577]
- On ATM interfaces, when the IP address of a remote device is changed, the output of the `show ilmi interface` command on the local routing platform might continue to display the old IP address for the remote device. [PR/24126]
- On channelized E1 interfaces, you might be able to configure clocking on `ds-fpc/pic/port:n` interfaces, where *n* is not unit 0. This is an invalid configuration and might cause a clocking selection problem on the other channels. [PR/24722]
- If virtual channel identifiers (VCIs) for a large number (approximately 400) of virtual connections (VCs) on an ATM DS3 interface are changed frequently, the interface might mishandle the ATM cells. As a result, OSPF and IS-IS neighbor adjacencies might not remain stable. [PR/25639]
- On a 2-port OC12 ATM2 IQ interface, the total virtual path (VP) downtime might not display correctly in the `show interfaces` command output. [PR/27128]
- On a 2-port OC12 ATM2 IQ interface, if you configure and then change the virtual path (VP) setting, the SNMP `jnxAtmVpTotalDownTime` counter might be reset. [PR/27131]
- When you configure a shaping rate greater than the speed of an OC3 link on an OC3 ATM2 IQ interface, the configuration might commit but the actual shaping rate is less than the interface speed. [PR/27459]
- On ATM2 IQ interfaces, when you include the `atm-l2circuit-mode` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level, the control word with the sequence number 0 is not treated as a non-sequenced packet. [PR/31392]
- On ATM2 IQ interfaces, when you configure the `atm-l2circuit-mode` statement, the control-word sequence number is not reset to 1 after the transmit sequence number reaches 65,535. [PR/31669]
- On ATM2 IQ interfaces, when you include the `atm-l2circuit-mode aal5` statement at the `[edit chassis fpc slot-number pic pic-number]` hierarchy level, the initial control word sequence number is not set to 1. [PR/31974]
- On M20 and M40 routers, when a physical layer problem affects a SONET/SDH interface, carrier transition statistics might not increment correctly in the output of the `show interfaces extensive` command. [PR/33325]

- When you configure both the bundle link and constituent links at the [edit logical-routers *logical-router-name* interfaces] hierarchy level, the constituent links do not come up. As a workaround, configure the constituent links at the [edit interfaces] hierarchy level. [PR/35578]
- On DS3 and E3 ATM2 IQ interfaces, when you configure ATM point-to-multipoint permanent virtual circuits (PVCs), the following error messages might appear in the system log: “/kernel: RT_COS: COS IPC op 4 (CLASS TO IFL) failed, err 1 (Unknown),” “ssb BCHIP 0: invalid entry type 127 at stream 8 channel 0 for ifl 83,” and “ssb COSMAN: mapping table bind to ifl 83 failed.” There is no operational impact. [PR/36524]
- On logical tunnel (lt) interfaces, if you configure IPv6 addresses and an interior gateway protocol (IGP) between peering lt logical interfaces, the peer interfaces might not be able to establish an adjacency. As a workaround, configure different IPv6 link-local addresses on each of the peers. [PR/37537]
- When an ATM interface configured for CCC encapsulation receives MPLS packets that exceed 484 bytes, the packets can overflow the buffer and cause the ATM PIC to hang. As a workaround, take the PIC offline and bring it back online. [PR/39918]
- When an IPsec firewall filter is applied to match traffic sent across a generic routing encapsulation (GRE) tunnel and originating from the local routing platform, the local traffic is dropped. Transient traffic is not affected. [PR/44871]
- On channelized T3 interfaces, the T1 loopback state does not reflect the loopback set by facilities data link requests using the `remote-loopback-respond` statement at the [edit interfaces *interface-name* t1-options] hierarchy level. [PR/45837]
- When the data-link connection identifier (DLCI) is greater than 335 on a Link Services PIC with Multilink Frame Relay (MLFR) configured, the ping command might fail. [PR/49567]
- On a Link Services PIC, the CLI might incorrectly allow you to configure a logical tunnel interface (interface identifier lt); however, the resulting interface might not work correctly. [PR/49818]
- On ATM2 IQ interfaces, if you configure OAM F4 on the physical interface by including the `oam-liveness` and `oam-period` statements at the [edit interfaces *at-fpc / pic / port atm-options vpi identifier*] hierarchy level, and the remote interface goes down and comes up again, the VP might not come up again. As a workaround, deactivate and reactivate the interface. To avoid this problem, configure OAM on the logical interface by including the `oam-liveness` and `oam-period` statements at the [edit interfaces *interface-name* unit *logical-unit-number*] hierarchy level. [PR/51435]
- Changes to DS0 timeslots on a channelized interface do not synchronize with the parent Multilink Frame Relay (MLFR) bundles on the Link Services II PIC. The new interface speed is updated on the channelized interface but

the link speed tracked on the MLFR bundle displays the original value. As a workaround, deactivate and reactivate the channelized interface. [PR/53030]

- When you deactivate and reactivate a remote LSQ interface, the `show interface lsq-fpc / pic / port extensive` command might display erroneous counter values for the LSQ bundle. [PR/54855]
- On Channelized STM1 PICs, a tributary unit alarm indication signal (TU-AIS) alarm enabled for one channel might cause another channel to shut down. [PR/55357]
- If an MLPPP LSQ bundle carries a large volume of link fragmentation and interleaving (LFI) traffic and a small proportion of multilink traffic, packets might be dropped on the egress constituent links. [PR/56664]
- On 1-port 10-Gigabit Ethernet PICs with XENPAK installed in an M320 or T-series routing platform, when you bring the PIC online, the following error message might be logged: “XGE(x/y): runaway interrupt count (1000001).” [PR/57376]
- If you disable an adaptive services interface by including the `disable` statement at the `[edit interfaces sp-fpc / pic / port]` hierarchy level and then delete the `disable` statement from the configuration, IPsec service is not reset correctly. As a workaround, either issue the `deactivate services` command followed by the `activate services` command, or issue the `request chassis pic offline fpc-slot slot-number pic-slot pic-number` command followed by the `request chassis pic online fpc-slot slot-number pic-slot pic-number` command. [PR/58522]
- If you try to convert a Gigabit Ethernet interface into an aggregated Ethernet interface by using a single commit, the routing platform might write the `DCD_CONFIG_WRITE` message to the system log and perform a core dump. As a workaround, issue separate configuration commits: one to rename the interface and a second to add the interface into the bundle. [PR/59185]
- When you take an ISDN interface offline on a J-series Services Router, the LEDs on the ISDN interface card might not turn off. [PR/59536]
- On ISDN interfaces in a J-series Services Router, if you configure the `vrf-table-label` statement at the `[edit routing-instances instance-name]` hierarchy level, packets might be dropped from the connection. [PR/59718]
- On ISDN dialer interfaces in a J-series Services Router, if you configure the `minimum-links` statement at the `[edit interfaces d10 unit logical-unit-number]` hierarchy level and then deactivate the BRI interface associated with the dialer interface, the output packets counter displayed in the output of the `show interfaces d10` command might continue to increment. [PR/59986]
- On ISDN dialer interfaces in a J-series Services Router, when you configure the `load-threshold 100` statement at the `[edit interfaces d10 unit logical-unit-number dialer-options]` hierarchy level and the 56 Kbps bandwidth threshold is exceeded, the interface does not support additional network traffic and might not activate another BRI interface. [PR/60045]

- On a Channelized E1 Intelligent Queuing (IQ) PIC, when you configure Frame Relay encapsulation on a point-to-multipoint interface and issue the `ping` command, the ping might fail. As a workaround, reconfigure the interface as a point-to-point interface. [PR/61074]
- On Adaptive Services PICs installed in M10i routers, if you add more peers to an existing IPSec services configuration, all services might stop functioning and the Single Board Router (SBR) might dump core. [PR/61692]
- On J-series Services Routers with a G.SHDSL PIM, at a line rate of 320 Kbps the `ping` command fails to work with an AdTran DSLAM. [PR/62177]
- On J-series Services Routers with a G.SHDSL PIM, at a line rate of 448 Kbps the line flaps and the `ping` command fails to work with an AdTran DSLAM. [PR/62179]
- On J-series Services Routers with a G.SHDSL PIM, for the 320 kbps and 256 kbps line rates only, when the software is bringing up the G.SHDSL line with an AdTran DSLAM, it can take more than one minute to negotiate the line successfully. [PR/62462]
- On J-series Services Routers with a G.SHDSL PIM, at a line rate of 320 kbps, the `ping` command fails to work with an AdTran DSLAM. [PR/64727]
- On J-series Services Routers with a G.SHDSL PIM, at a line rate of 448 kbps, the line flaps with an AdTran DSLAM. [PR/64729]
- For Automatic Protection Switching (APS) on SONET/SDH interfaces, there are no operational mode commands that display the presence of APS mode mismatches. An APS mode mismatch occurs when one side is configured to use bidirectional mode, and the other side is configured to use unidirectional mode. [PR/65800]
- On J-series Services Routers, when an ISDN dialer interface is configured as a watch list and is then deactivated, connected as a backup interface, and a `commit` command is issued, the dialer interface does not dial out even if the primary interface is down. As a workaround, disable the primary interface, issue a `commit` command, and then renable the primary interface and issue another `commit` command. [PR/67355]
- When a router with a Gigabit Ethernet IQ PIC comes online, the Packet Forwarding Engine might dump core and reset. The system log shows the following message: "SGE(0/2): link 0 timeout waiting CAM search complete, sge_cam_data_search." There is no workaround. [PR/67446]

Services Applications

- The output of the `show services nat pool` command displays duplicate entries for a single Network Address Translation (NAT) pool. [PR/34678]

- When you configure intrusion detection services (IDS) on J-series platforms, including the threshold statement at the [edit services ids rule *rule-name* term *term-name* then logging] hierarchy level has no effect. [PR/46577]
- On Adaptive Services PICs configured for IPsec tunnel redundancy, if there are a large number of tunnels, some of them might switch over to the backup tunnel. [PR/46733]
- The local-id fqdn statement at the [edit services ipsec-vpn ike policy *policy-name*] hierarchy level has no effect. [PR/46908]
- On routing platforms configured for Internet Key Exchange (IKE)-based IPsec, if a remote peer using other vendor's equipment does not renegotiate the IKE security association (SA) when it is about to expire and continues to send dead peer detection (DPD) requests on the same SA, the routing platform might not be able to reply to these messages. [PR/47004]
- If the socket buffer becomes full on a remote router, you cannot clear all the IPsec security associations (SAs) from the router. [PR/55189]
- For flow collection services interfaces, if you include a description for ifalias statement in the format option at the [edit services flow-collector file-specification *file-specification-name* name-format] hierarchy level, the interface might generate files with nonexistent SNMP indices in the filename. [PR/57382]
- When a routing platform is configured for graceful Routing Engine switchover and Adaptive Services (AS) PIC redundancy, and a switchover to the backup Routing Engine occurs, the redundant services interface (rsp-) only uses the primary services interface (sp-) if the primary interface is operational. [PR/59070]
- On Monitoring Services I and II PICs, if the export channel to the external cflowd collector is closed, cflowd records might be lost. As a workaround, restart the PIC. [PR/59432]
- On Monitoring Services II PICs configured for flow collection services, during memory overload conditions, the flow collector interface might create files lacking cflowd records and these files might not be sent to the external FTP server. [PR/62599]
- When you modify a flow collection services configuration and commit the changes, the system log might contain error messages regarding the commit. There is no operational impact and these messages can be ignored. [PR/64201]
- On Monitoring Services II PICs configured for flow collection services, when the flow collector interface exports files to an FTP server, the start time of a given flow might change, even though flow identifier stays the same. [PR/64714]
- On Monitoring and Adaptive Services PICs, the cflowd records generated for 20-byte IP packets with the IP protocol set to UDP, TCP, or ICMP might contain nonzero values for source port, destination port, and ICMP type/code. [PR/67344]

General Routing

- A T1 interface might continue flapping with flooding network control messages. This can cause excessive tail drop on the network-control queue. The workaround is to increase the capacity of the network-control queue. [PR/55898]
- If you delete or deactivate the `rib inet.0` statement at the `[edit routing-options]` hierarchy level, this action might not remove the static routes configured under the statement. [PR/61533]
- If you issue the `show ldp traffic-statistics` command, the following system log message might be generated for all forwarding equivalence classes (FECs) with an ingress counter set to zero: “send rnhstats GET: error: ENOENT -- Item not found.” [PR/67647]

Routing Protocols

- When you include the `as-path atomic-aggregate` statement at the `[edit routing-options aggregate defaults as-path]` hierarchy level to manually add the `ATOMIC_AGGREGATE` attribute on a BGP AS path, the attribute is not added. [PR/2527]
- When you issue the `show pim statistics` command to view traced PIM protocol traffic, messages sent to the rendezvous point (RP) might not increment the Register counter. [PR/13887]
- When you issue the `mtrace` command from a UNIX client, the router does not respond to a query that requires multicast response, but responds correctly to any query that requires unicast response. As a result, the first two probes time out. The third probe is the unicast response probe, which usually succeeds. [PR/17237]
- If you issue the `ospfNbrAddressLessIndex` SNMP query for an interface configured with an IP address, you might receive output containing the value of the SNMP interface index instead of the value 0 suggested by RFC 1850. [PR/20104]
- It is possible to specify an invalid value for the `metric` statement included at the `[edit protocols dvmrp interfaces interface-name]` hierarchy level. Values larger than 32 are invalid. [PR/33429]
- When virtual links are configured on a router, OSPF graceful restart might not work as expected. [PR/36947]
- If you configure Bidirectional Forwarding Detection (BFD) and graceful restart for OSPF or IS-IS, graceful restart might not work as expected. [PR/37106]
- If a router receives a Pragmatic General Multicast (PGM) Source Path Message (SPM), it does not create a forwarding cache, nor does it forward the message to other routers as a heartbeat, as specified in RFC 3208. Also, the router’s multicast cache might time out if it does not receive actual PGM data (ODATA) for more than 6 minutes. As a workaround, configure the PGM source

application to send PGM ODATA at least once every 6 minutes. The ODATA acts as the heartbeat message in lieu of the SPM messages and ensures the multicast and forwarding caches are created and updated. [PR/37504]

- Bidirectional Forwarding Detection (BFD) might not work as expected within a logical router. [PR/38332]
- If secondary addresses are configured on an interface, Bidirectional Forwarding Detection (BFD) might establish a session for only one address at a time on a random basis. [PR/38498]
- If you configure the sham-link statement at the [edit routing-instances *instance-name* protocols ospf area] or [edit routing-instances *instance-name* protocols ospf] hierarchy level on a provider edge (PE) router, extraneous OSPF link-state advertisements (LSAs) might be added. In some cases, this can result in a routing loop between the customer edge (CE) and PE routers. [PR/40000]
- On a provider edge (PE) router configured for multicast over Layer 3 VPNs, if you enable PIM in a routing instance and on a GRE tunnel through the provider core network, the router might not be able to establish PIM neighbor relationships over the GRE tunnel and the routing protocol process might restart. As a workaround, use an interface other than a GRE interface when connecting to the provider core network. [PR/40124]
- The address fields in the BGP MIB are not compatible with IPv6 address lengths. [PR/51150]
- If you include the vpn-group-address statement at the [edit routing-instance *routing-instance-name* protocols pim] hierarchy level in a routing instance of type VRF, and you change the router ID or loopback address value in a master routing instance, the router might lose connectivity with other provider edge (PE) routers for the VPN. As a workaround, deactivate the vpn-group-address statement at the [edit routing-instance *instance-name* protocols pim] hierarchy level, commit the configuration, reactivate the statement, and commit the configuration again. [PR/51839]
- When you configure damping globally and use the import policy to not damp specific routes, and a new route is received from a peer with the local interface address as the next hop, the route is added to the routing table with default damping parameters, even though the import policy has a non-default setting. As a result, damping settings do not change appropriately when the route attributes change. [PR/51975]
- If you configure IS-IS to run IPv6 between two logical routers in the same physical router by including a logical-router configuration, IS-IS routes might not get installed into the inet6.0 routing table. The workaround is to manually configure unique IPv6 link-local addresses on the interfaces that connect the two logical routers. [PR/61530]
- When the IGMP/MLD SSM-Map feature is enabled on a LAN interface with multiple receiving hosts, the router might continue to forward traffic for the

group until the IGMP group membership timeout interval, even though all receivers might have already left the group. [PR/61538]

- When the `clear bgp neighbor soft` command or a received BGP REFRESH request coincides with generating the initial advertisement set for a peer that is not the first peer to become established in a group, the routing protocol process (rpd) might restart. [PR/64938]
- The `no-holddown` statement does not completely bypass the adjacency holddown mechanism. As a result, IS-IS might quench BGP for a short time even though the `no-holddown` statement is configured. [PR/65471]
- When you configure OSPF graceful restart and the routing platform restarts, the output of the `show ospf neighbor detail` command might not display correct information for the designated router (DR) and backup DR (BDR). [PR/67902]

MPLS Applications

- If you configure a label-switched path (LSP) with the `no-cspf` statement at the `[edit protocols mpls]` hierarchy level, the LSP might cycle up and down several times before stabilizing. [PR/10415]
- The local bandwidth log for a Constrained Shortest Path First computation might show an incorrect value. [PR/21369]
- Per-prefix forwarding does not support multiple-weight next hops. If you forward traffic over a transit router on which the `fast-reroute` statement is configured at the `[edit protocols mpls label-switched-path lsp-name]` hierarchy level, the backup information is not passed to the Packet Forwarding Engine. [PR/22755]
- After a label-switched path (LSP) is established, increasing the LSP bandwidth beyond what is available does not bring down the LSP. The `show mpls lsp` command displays the configured bandwidth value rather than the actual bandwidth used. [PR/40164]
- If you include the `explicit-null` statement at the `[edit protocols bgp family inet labeled-unicast]` hierarchy level, the `traceroute` command might not work properly. [PR/44814]
- If a vendor's equipment employs proprietary TLV information, the `ping mpls` command might have interoperability issues because the JUNOS software cannot understand the content of that vendor's proprietary TLV information. [PR/51084]
- If you issue the `show mpls lsp statistics` command on an ingress router with the slower Routing Engine (RE2) and there are many label-stacked VPNs, the Packet Forwarding Engine might restart. [PR/51305]
- If a cross-connected circuit (CCC) traverses a forwarding-adjacency label-switched path (LSP), traffic forwarding might be affected. [PR/60088]

- RSVP graceful restart does not function for LSPs that have a forwarding adjacency (FA) label-switched path (LSP) as a next hop. [PR/60256]
- When you modify the primary path for an MPLS LSP by using the `delete protocols mpls label-switched-path lsp-path-name primary path-name` command in configuration mode, followed by the `set protocols mpls label-switched-path lsp-path-name primary path-name` command, and then issue the `commit` command, the entire LSP (both primary and secondary) is torn down and then rebuilt from scratch. As a workaround, issue the `delete protocols mpls label-switched-path lsp-path-name primary path-name` command in configuration mode followed by the `commit` command. Then issue the `set protocols mpls label-switched-path lsp-path-name primary path-name` command followed by the `commit` command. [PR/62365]
- Rarely, during a point-to-multipoint make-before-break procedure, the branches for a point-to-multipoint LSP that have the same downstream link are assigned a different outgoing label. This might cause packet drops for some of the branches. As a workaround, clear the RSVP session. [PR/66354]
- If you configure a point-to-multipoint label-switched path (LSP) and a point-to-multipoint transmit switch and commit the configuration, the routing protocol process (rpd) might stop operating and dump core. [PR/67488]

VPNs

- For IPv6 VPNs running on Gigabit Ethernet and Fast Ethernet interfaces, `ping` and `traceroute` operations do not work from local provider edge (PE) routers to remote PE and customer edge (CE) routers. [PR/28502]
- When you modify the `frame-relay-tcc` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level of a Layer 2 VPN, the connection for the second logical interface might not come up. As a workaround, restart the chassis process (chassisd) or reboot the router. [PR/32763]

Class of Service

- When you configure an ES PIC, a log message similar to “fpc0 LCHIP(3): Unable to fathom what channel used by IFD 432” might be displayed. There is no operational impact. [PR/36184]
- When you apply a class-of-service (CoS) scheduler map to an interface, the CoS daemon (cosd) might develop a memory leak. [PR/42465]
- When you remove or omit the `shaping-rate` statement from a scheduled VLAN configuration, the routing platform might drop large numbers of packets. [PR/47057]
- On ATM2 IQ PICs configured to use alternate VC CoS mode, when the traffic pattern on low-priority queues is changed, the high-priority queue can send less traffic than it should be able to send. As a workaround, you can raise the high-priority queue weight. [PR/50178]

- The error message indicating that an IEEE 802.1 rewrite rule cannot be applied on a nontagged interface references a classifier instead of a rewrite rule. There is no operational impact. [PR/50980]
- The JUNOS software does not support the IEEE-802.1p rewrite rule when an interface is the outbound interface. [PR/55903]
- If you try to configure a scheduler map containing two forwarding classes that are mapped to the same queue, the class-of-service scheduler is not applied to the Packet Forwarding Engine. As a workaround, configure a single forwarding class for each of the available queues. [PR/57907]
- If you configure a scheduler map and a random early detection (RED) drop profile that uses a fill level of 100 percent, and the routing platform receives traffic that oversubscribes the queue scheduler, the **Resource errors** counter in the output of the **show interfaces extensive** command increases and packets going to other queues and interfaces might be impacted. [PR/60215]
- On J-series Services Routers, if you oversubscribe an E1 interface, latency on the high priority queue might be higher than expected. As a workaround, configure a shaping rate on the E1 interface that is equal to the line rate minus the E1 framing overhead. [PR/60595]

Forwarding and Sampling

- On a T640 routing node, the sampling process (sampled) might write to a sampling output file inconsistently or might fail to export cflowd records as expected. As a workaround, restart the sampling process. [PR/31021]

Routing Policy and Firewall Filters

- If the software cannot find a referenced policy, the routing protocol process (rpd) might dump core. [PR/67098]

Network Management

- The following groups of MIB objects do not segregate the data they return according to the routing instance specified in an SMMP request: **vrpMIB**, **jnxCosIfqStatsTable**, and **jnxCosQstatTable** [PR/63045]
- Sometimes, the default routing instance (configured at the default logical router level) does not report the physical interface associated with the logical interface. [PR/66793]

Previous Releases

Release 7.2R3

The following issues have been resolved since JUNOS Release 7.2R2. The identifier following the description is the tracking number in our bug database.

Software Installation

- While installing a PC card, you might see these change-owner error messages: “chown: wheel: illegal group name” and “pkg_add: couldn't change owner/group of '*file*' to 'root.wheel'.” [PR/50755: This issue has been resolved.]

Platform and Infrastructure

- If a routing platform is configured with a VPN routing and forwarding (VRF) table label and you include the `explicit-null` statement at the `[edit protocols ldp]` hierarchy level (for LDP) or at the `[edit protocols mpls]` hierarchy level (for RSVP), and a neighbor that uses equipment from another vendor replies with an explicit null label as the outer label and a VRF table label as the VPN label, the VPN might stop operating. As a workaround, remove the `explicit-null` statement. [PR/49544: This issue has been resolved.]
- In a multiport SONET/SDH interface, connecting an unconfigured port to a configured port can cause the configured port to come down. The workaround is either to remove the configuration from the remote port or to disconnect the unconfigured port from the configured port. [PR/57922: This issue has been resolved.]

Interfaces and Chassis

- On TX Matrix platforms, when you take a 10 Gigabit Ethernet PIC offline and bring it online again, the `show chassis hardware` command output displays inconsistent small form-factor pluggable transceiver (SFP) information. [PR/51389: This issue has been resolved.]
- On J-series Services Routers, the `pseudo-2e20-o153`, `2e7-1`, and `pseudo-2e9-o153` T1 BERT algorithms return zero after a test run. [PR/51890: This issue has been resolved.]
- When OAM loopback cells are not received on an ATM interface, the router marks the interface down and logs a message. But when the interface is marked up as a result of receiving the loopback cells, the router does not log an interface up message. [PR/51942: This issue has been resolved.]
- PPP over Ethernet (PPPoE) interfaces do not support the `idle-timeout` statement at the `[edit interfaces pp-fpc / pic / port unit logical-unit-number pppoe-options]` hierarchy level. [PR/52150: This issue has been resolved.]
- When you delete an address on a logical interface and set the same address on another logical interface, for a short time the software might behave as though there are duplicate addresses on the two logical interfaces. This can cause the device control process (dcd) to dump core. [PR/53166: This issue has been resolved.]
- When you deactivate and reactivate a remote LSQ interface, the `show interface lsq-fpc / pic / port extensive` command might display erroneous counter values for the LSQ bundle. [PR/54855: This issue has been resolved.]

- RED drops might occur when E1 links in G704 framed mode are used as the constituent links of an LSQ interface. The workaround is to either configure the `e1-options framing unframed` statement at the `[edit interfaces interface-name]` hierarchy level on the affected E1 links or configure an extra 4 percent link-layer overhead on the LSQ interface. [PR/57080: This issue has been resolved.]
- For link services interfaces at close to full capacity, MRRU changes on a bundle can cause the bundle to be deleted. As a workaround, deactivate and reactivate the link services interface. [PR/58553: This issue has been resolved.]

General Routing

- Issuing a `show route advertising-protocol bgp` command can cause a core dump in the routing protocol process (rpd). [PR/58492: This issue has been resolved.]

Routing Protocols

- If you enable LDP tunneling for a label-switched path (LSP), wide metric changes are not reflected for the LSP. [PR/57320: This issue has been resolved.]
- If you have not configured a router ID and have also not configured an address on the loopback interface, OSPF does not form adjacencies. [PR/58870: This issue has been resolved.]

VPNs

- On a single-tagged Gigabit Ethernet intelligent queuing (IQ) port, if you configure the `input-vlan-map pop` statement at the `[edit interfaces interface-name unit logical-unit-number]` hierarchy level, Internetwork Packet Exchange (IPX) traffic might be dropped across the cross-connect. [PR/56421: This issue has been resolved.]
- The `ping mpls` command does not work for VPNs configured with the `vrf-table-label` statement. [PR/57599: This issue has been resolved.]
- If you configure link protection for an LDP over RSVP LSP, and these VPN routes are readvertised over a VPN-EBGP session, the routing platform might attempt to install routes with a swap/triple push operation and the routing protocol process might dump core continuously. As a workaround, disable link protection. [PR/59908: This issue has been resolved.]

Release 7.2R2

The following issues have been resolved since JUNOS Release 7.2R1. The identifier following the description is the tracking number in our bug database.

Software Installation

- You might not have been able to upgrade to JUNOS Release 7.4 using the `request system software add package-name` command. [PR/61378: This issue has been resolved.]

Platform and Infrastructure

- When you include the `vrf-table-label` statement at the `[edit routing-instances]` hierarchy level, MPLS packets with label-switched interface (LSI) labels that arrive on core-facing ATM or Frame Relay interfaces are not counted. [PR/51733]
- When a file system read/write error occurs, the Routing Engine might enter a state in which it responds to local pings and interfaces remain up, but no other processes are responding. As a workaround, reboot the router. [PR/55650: This issue has been resolved.]
- For Ethernet-based interfaces in a Layer 2 circuit topology, if you apply the same circuit cross-connect (CCC) input filter on multiple logical interfaces in different VLANs, and the state of the associated physical interface changes from up to down to up, all Layer 2 circuit traffic might travel over only one of the logical interfaces. As a workaround, apply a unique CCC input filter to each logical interface. [PR/57276: This issue has been resolved.]
- On Adaptive Services PICs, if you configure a virtual loopback tunnel (vt-) interface and include the `service-package layer-2` statement at the `[edit chassis fpc fpc-slot pic pic-slot adaptive-services]` hierarchy level, the routing platform might reboot multiple times when it is restarted. [PR/59915: This issue has been resolved.]
- On an E3 IQ interface configured with PPP encapsulation, if you include the unsupported `per-unit-scheduler` statement at the `[edit interfaces interface-name]` hierarchy level, the routing platform might become unresponsive. [PR/60048: This issue has been resolved.]
- For M320 and T-series routing platforms configured with Ethernet interfaces and BGP, if you upgrade to JUNOS Releases 6.4R4, 7.0R3, or 7.1 and later, next-hop errors might be reported and an FPC might stop operating when Jtree memory is allocated. [PR/60081: This issue has been resolved.]
- Issuing the `set ntp system source address` command to set the last octet of the NTP source address to the range of 224 to 239 causes an “attempt to configure invalid address” syslog error message. [PR/60200: This issue has been resolved.]
- On M-series and T-series routing platforms with a backup Routing Engine, when graceful switchover is configured, convergence times are delayed. [PR/61216: This issue has been resolved.]
- On an M40e router containing an E3 Intelligent Queuing (IQ) PIC, if you configure graceful Routing Engine switchover and issue the `commit synchronize`

command, the backup Routing Engine might stop operating. [PR/61434: This issue has been resolved.]

- If an NCP Terminate Request is received on a PPP interface that does not have the `family` statement configured, the kernel might panic. [PR/61459: This issue has been resolved.]
- On J-series Services Routers, when you configure a firewall filter containing a prefix list, the list of optimized prefixes for the firewall compiler might not be handled correctly and the forwarding process (fwdd) might dump core. [PR/61741: This issue has been resolved.]
- On routing platforms containing a single hard drive and no compact flash drive, if you include the `reboot` statement at the `[edit chassis routing-engine on-disk-failure]` hierarchy level and the hard disk fails, the statement might not take effect and the routing platform might not reboot. [PR/61850: This issue has been resolved.]
- When the routing platform learns a route prefix through OSPF or a static route, and the prefix specifies an interface instead of a next-hop IP address, the prefix might not be reachable. [PR/62052: This issue has been resolved.]
- Interrupt handling was not disabled when the PIC was being detached. [PR/63175: This issue has been resolved.]
- If you configure a stateful firewall on a J-series Services Router and the router experiences heavy traffic, the forwarding process (fwdd) might dump core. [PR/63465: This issue has been resolved.]

User Interface and Configuration

- If the `/var/transfer/config` directory is not available, automatic configuration uploading might fail and the resulting system log message might not provide enough information to troubleshoot the problem. [PR/47341: This issue has been resolved.]
- If you edit the order of terms in a firewall configuration on the master Routing Engine and then issue the `commit synchronize` command, the revised term order might not be copied to the backup Routing Engine. [PR/58550: This issue has been resolved.]
- The `explicit-null` option at the `[edit protocols bgp group group-name family inet6 labeled-unicast]` hierarchy level might have been hidden in the command-line interface (CLI). [PR/59042: This issue has been resolved.]
- When you issue the `load update` command, it is possible that terms could be reordered, especially if you add a term in a hierarchy. [PR/59615: This issue has been resolved.]

- If you use a JUNOScript Perl client to connect to a Secure Shell (SSH) server, the following errors might be generated:
 - “login: LOGIN_FLAGS: Failed to clear flags for /dev/tty?: No such file or directory” [PR/60288: This issue has been resolved.]
 - “login: LOGIN_OWNER: Failed to change owner for /dev/tty?: No such file or directory”
 - “login: LOGIN_INFORMATION: User username logged in from host host-address on device tty?”
- If you issue the `deactivate groups group-name` command in configuration mode for an option that is currently inactive in the configuration, and then issue the `commit` command, the system might produce an error message, such as “error: could not add object.” However, the configuration change is still committed. [PR/61825: This issue has been resolved.]
- When you use the J-Web user interface to log on to a J-series or M-series routing platform, even if authentication succeeds, you might see error messages, such as “initauthconf: unable to open file: /etc/auth.conf.” There is no operational impact. [PR/62034: This issue has been resolved.]
- When you configure a long SSH DSA or SSH RSA key (approximately 1020 bytes or larger) and commit the configuration, several “buffer overflow” system log messages might be generated and the management process (mgd) might dump core. [PR/62141: This issue has been resolved.]
- When you configure forwarding class attributes at the [edit groups *group-name* class-of-service] hierarchy level and try to commit the configuration, the commit might fail. As a workaround, move the configuration statements to the [edit class-of-service] hierarchy level. [PR/62345: This issue has been resolved.]

Interfaces and Chassis

- On M320 and T-series routing platforms, if you quickly bring an FPC offline and online multiple times in a row by pressing the FPC button on the chassis or by issuing the `request chassis fpc slot slot-number (online | offline)` commands, the FPC might not come back online and you might see the following message in the system log: “fru restart waiting for FPC *fpc-number* to be clean.” To recover from this problem, remove the FPC from the slot and reinsert it. As a workaround, do not issue an offline request for an FPC until all the corresponding PICs are online. [PR/52098: This issue has been resolved.]
- On channelized interfaces, if you disable channel 0, commit the configuration, take the router offline, and then bring it back online, statistics are not updated for any of the enabled channels and a software object error message appears periodically in the system log directory. As a workaround, you can issue a `delete disable` command followed by a `set disable` command. [PR/55584: This issue has been resolved.]

- The PIC data structure should be cleared whenever an FPC is disabled using the external button or a CLI command issued from a console, otherwise chassisd displays the out-dated PIC information after the FPC goes back online in the same slot. [PR/56061: This issue has been resolved.]
- When a small form-factor pluggable transceiver (SFP) is absent on an SFP-based PIC, the chassis process (chassisd) might log the following message repeatedly in the system log: “pic_set_port_info:Got cable_type for FPC 0 Pic 3 port 1 cable num = 0, str = .” [PR/56274: This issue has been resolved.]
- After approximately 3 weeks and a few days of service, Monitoring Services PICs might stop exporting flows because a time counter overflows. As a workaround, restart the PIC. [PR/58333: This issue has been resolved.]
- On ATM2 intelligent queuing (IQ) interfaces, if a circuit cross-connect (CCC) ATM Adaptation Layer 5 (AAL5) virtual circuit (VC) receives alarm indication signal (AIS) cells while the interface is in the CCC_DOWN state, then the VC stops receiving the AIS cells, most of the Operation, Administration, and Maintenance (OAM) processing for all VCs might cease. [PR/59069: This issue has been resolved.]
- On ATM2 intelligent queuing (IQ) interfaces installed in M320 routers, if you configure Automatic Protection Switching (APS) and the APS-protected interface in the admin-down state receives packets, the protected interface might still process the packets. [PR/59152: This issue has been resolved.]
- On ATM2 intelligent queuing (IQ) interfaces, when a large number of VCs are configured with same value for the oam-period statement at the [edit interfaces *interface-name* unit *logical-unit-number*] hierarchy level, some of the Operation, Administration, and Maintenance (OAM) cells might be dropped and the VCs and logical interfaces might randomly be marked as down. [PR/59183]
- On M10 routers, when Internet Protocol Control Protocol (IPCP) negotiation appears to have completed, the router might restart the IPCP negotiation. [PR/59468: This issue has been resolved.]
- The AS PIC can crash when configured for active monitoring services while under a heavy load. [PR/59793: This issue has been resolved.]
- On Gigabit Ethernet intelligent queuing (IQ) interfaces, when you include the tag-protocol-id statement at the [edit interfaces *interface-name* *gigether-options* *ethernet-switch-profile*] hierarchy level with any value other than the default value of 0x8100, Virtual Router Redundancy Protocol (VRRP) interfaces start going down and up. If VRRP trace options are enabled, the log file includes the message: “vrrpd_rts_get_ifd_state VLAN information for ge-fpc/pic/port mismatch.” [PR/59909: This issue has been resolved.]
- On T-series and M320 routing platforms, if you configure unidirectional-mode Automatic Protection Switching (APS) and graceful Routing Engine switchover, another vendor’s router might not receive a line alarm indication signal (AIS) from the routing platform and the APS switchover might fail. [PR/60211: This issue has been resolved.]

- For link services intelligent queuing (IQ) interfaces configured for MLPPP on Adaptive Services PICs, if you manually configure a maximum received reconstructed unit (MRRU) value or deactivate and reactivate the interfaces in an MLPPP bundle, the `family inet` MTU might have the same value as the MRRU or there might be a `family inet` MTU mismatch between peer interfaces. As a workaround, deactivate and reactivate the interfaces in the MLPPP bundle on both sides of the connection. [PR/60407: This issue has been resolved.]
- Deleted or deactivated interface units are not being cleaned up properly, requiring a restart of the L2TP process. [PR/60710: This issue has been resolved.]
- On E1 interfaces installed in J-series Services Routers, if you include the `framing g704` statement at the `[edit interfaces e1-fpc / pic / port e1-options]` hierarchy level, random early detection (RED) might drop packets prematurely and might prevent the interface from sending traffic at line rate. [PR/60745: This issue has been resolved.]
- For multipoint ATM2 IQ logical interfaces, if you included the `plp-to-clp` statement at the `[edit interfaces at-fpc / pic / port unit logical-unit-number]` hierarchy level, the packet loss priority (PLP) setting might not have been copied to the cell loss priority (CLP) bit. The workaround was to configure the statement for the physical interface instead, at the `[edit at-fpc / pic / port atm-options]` hierarchy level. [PR/61167: This issue has been resolved.]
- On ATM2 intelligent queuing (IQ) interfaces, Operation, Administration, and Maintenance (OAM) cells might be placed into the second-highest priority trail termination point (TTP) queue instead of the highest as expected. [PR/61188: This issue has been resolved.]
- On M7i and M10i routers configured for L2TP, if the router receives a second Password Authentication Protocol (PAP) authentication request while the first PAP authentication request is being processed, the L2TP process (`l2tpd`) might dump core and stop operating. [PR/61207: This issue has been resolved.]
- If you configure T1 virtual tributaries on Channelized OC12 Intelligent Queuing (IQ), Channelized OC3 IQ, or Channelized DS3 IQ PICs, then issue the `show interfaces` command, the interfaces erroneously appear to be operational when in fact they are not. In some cases, the T1 channels might report loss of frame (LOF), alarm indication signal (AIS), and yellow (YLW) errors. Although these errors appear to increment the counters in the output of the `show interfaces` command, alarms are never generated by the router and the `DS1 alarms:` field displays `none`. [PR/61251: This issue has been resolved.]
- You might not be able to configure a VLAN identifier larger than 4025 at the `[edit interfaces interface-name-fpc / pic / port unit logical-unit-number vlan-tags (inner | outer) tag-protocol-id .vlan-id]` hierarchy level. [PR/61404: This issue has been resolved.]
- During a configuration change, a packet requesting an unknown service can cause the PIC to crash. The workaround is to drop any packets requesting unknown service types. [PR/61622: This issue has been resolved.]

- On ATM2 Intelligent Queuing (IQ) PICs installed in M-series and T-series platforms, ATM PVCs that have been idle longer than a few seconds might experience a start delay of approximately five to ten seconds, during which the output rate is slower than normal, followed by output at the nominal shaping rate. This situation occurs even when the ATM PVCs are not at their shaping limit and the ATM port is transferring less than the full line-rate potential. [PR/61746: This issue has been resolved.]
- On Adaptive Services PICs, if you configure a dynamic IKE-based IPsec tunnel, the tunnel might not become established with another vendor's router. [PR/61779: This issue has been resolved.]
- On T-series routing platforms, if the Switch Processor Mezzanine Board (SPMB) on the master Routing Engine fails, a switchover to the standby Routing Engine might not occur and the routing platform might stop forwarding packets. [PR/61910: This issue has been resolved.]
- On Adaptive Services PICs installed in a routing platform not configured for graceful Routing Engine switchover, if you use a next-hop-style service set to establish an IPsec tunnel in a VPN routing and forwarding (VRF) instance, then issue the `request chassis routing-engine master switch` command a few times, an attempt to ping across the IPsec tunnel might fail. [PR/62073: This issue has been resolved.]
- For Channelized IQ PICs installed in M40e and M160 routers, the default physical interface MTU might have been more restrictive than was necessary. To resolve this, the default physical interface MTU for these interfaces has been increased to 9192 bytes. [PR/62104: This issue has been resolved.]
- On an M-series router, when you issue the `commit` command on a large configuration (greater than 2 megabytes) that contains one or more ATM interfaces set to promiscuous mode, the `commit` operation might hang. As a workaround, remove the promiscuous mode option from the ATM interfaces and reissue the `commit` command. [PR/62610: This issue has been resolved.]
- On Gigabit Ethernet PICs with small form-factor pluggable transceivers (SFP), if the interface experiences link-down detection delays of up to 1 second, the operation of fast reroute might be affected. [PR/62682: This issue has been resolved.]
- When you configure a large number of ATM virtual circuits (VCs), Operation, Administration, and Maintenance (OAM) processing might become bursty. In rare cases, if very large bursts happen at the same time as an anomaly in alarm indication signal (AIS)/remote defect indication (RDI) cell reception, OAM processing might stop operating after several days. [PR/62719: This issue has been resolved.]
- If you configure flow monitoring and PIC sampling for Adaptive Services (AS) PICs installed in M10i routers, the AS PIC might stop operating when network traffic becomes heavy. [PR/63420: This issue has been resolved.]

- On Channelized DS3 Intelligent Queuing (IQ) PICs, if you connect the interfaces to another vendor's digital access cross-connect system (DACS), the output of the `show interfaces` command for the Channelized T3 controller interface might display the `Physical interfaces:` field as `Physical link is Down` and the `Active alarms:` field as `FERF`. In addition, T1 channels might appear to be down and not generate any T1 alarms. [PR/63666: This issue has been resolved.]
- On Gigabit Ethernet Intelligent Queuing (IQ) PICs and Gigabit Ethernet PICs with small form-factor pluggable transceivers (SFP), if you configure the interfaces with Virtual Router Redundancy Protocol (VRRP) and a tag protocol ID of 0x9100, VRRP might not work. [PR/63816: This issue has been resolved.]
- Under heavy load using multiple bundles, compression is disabled for some of the bundles. [PR/64268: This issue has been resolved.]

General Routing

- If you disable unicast reverse-path forwarding (RPF) on an interface, the routing protocol process (rpd) might restart. [PR/41964: This issue has been resolved.]
- Configuring 0/8 as an allowed martian and 0/8 as a static route causes the routing protocol process (rpd) to crash after a restart. [PR/60528: This issue has been resolved.]
- The addition or deletion of logical-routers causes the routing protocol process (rpd) not to be cleaned up properly, resulting in loss of routing protocol operation. [PR/60690: This issue has been resolved.]
- When you configure a BGP group that uses `allow` statements and a routing table group in any address family, then change the `rib-group` configuration, memory corruption might occur and the routing protocol process (rpd) might restart. [PR/61019: This issue has been resolved.]
- If the router ID is not explicitly configured on a J-series Services Router, the OSPF routing process might select an incorrect router ID. To configure the router ID, include the `router-id router-id` statement at the `[edit routing-options]` hierarchy level. [PR/61112: This issue has been resolved.]
- When a generated route has a contributing route with an indirect next hop, the routing protocol process (rpd) might restart unexpectedly. [PR/63208: This issue has been resolved.]

Routing Protocols

- When you remove an IP multicast scope definition by deleting either the interface `interface-names` or prefix `destination-prefix` statement at the `[edit routing-options multicast scope scope-name]` hierarchy level, and you commit the change, the scope definition might not be deleted from the configuration. As a workaround, issue the `restart routing` command to clear the multicast scope definition. [PR/45355: This issue has been resolved.]

- For PIM networks, if the routing platform receives an auto-RP packet containing new group ranges for an already known rendezvous point (RP), it immediately purges any previously learned group prefixes for that RP, which might cause a multicast group to transition up and down. [PR/59940: This issue has been resolved.]
- When you configure the routing platform as an automatic rendezvous point (auto-RP) mapping agent, it might fail to interoperate with other vendors' routers that follow a strict implementation of the auto-RP specification. [PR/60391: This issue has been resolved.]
- A route received over a LAN might flap constantly when the following occurs: the route is accepted from one neighboring router on a LAN; the same route is rejected from another neighboring router on the same LAN, but its next hop is set to the first neighboring router. [PR/60473: This issue has been resolved.]
- RIP tracing does not always include the sender information required for debugging. [PR/60579: This issue has been resolved.]
- When sending an IGMPv3 query message, the router might format the address of the source incorrectly. [PR/60590: This issue has been resolved.]
- On a broadcast link with a single neighbor, when the neighbor initiates an OSPFv3 graceful restart operation, the restart might be terminated at the point when the local router assumes the role of a helper. At this point, the subnet prefix on the broadcast link is moved from the link's transit intra-area-prefix link-state advertisement (LSA) to the local router's intra-area-prefix LSA. A change in the LSA is considered a topology change, which terminates the neighbor's restart operation. [PR/60629: This issue has been resolved.]
- If you configure RIPv2 on logical interfaces between a customer edge (CE) router and a provider edge (PE) router, some of the packets might be malformed. As a workaround, deactivate the neighbor and reactivate it. [PR/60759: This issue has been resolved.]
- If you configure a routing platform as a PE router and a BGP route reflector or AS boundary router, then configure a routing table group in a VPN routing and forwarding (VRF) instance to share unicast routes with the *instance.inet.2* routing table (used for multicast reverse path forwarding [RPF] information), and if you advertise these routes to the BGP inet-vpn multicast family, the routing protocol process (rpd) might restart. [PR/61005: This issue has been resolved.]
- When you deactivate an IP multicast scope policy with the `deactivate routing-options multicast scope-policy policy-name` configuration-mode command, the policy might still appear in the output of the `show multicast scope` operational-mode command. [PR/61063: This issue has been resolved.]
- If you configure a multicast scope policy in PIM sparse mode, the PIM encapsulation (pe) interface might not be added to the downstream interface list and the designated router (DR) might not be able to send register packets to the rendezvous point (RP). [PR/61287: This issue has been resolved.]

- You might not be able to configure BGP group and neighbor descriptions containing more than 126 characters. To resolve this issue, the maximum description length has been increased to 254 characters. [PR/62445: This issue has been resolved.]
- When a multicast router reboots and stops being the designated router (DR) on a LAN interface, a `<*,g>` PIM upstream state entry might not be updated and might cause traffic to be pruned incorrectly. [PR/62992: This issue has been resolved.]
- After an IS-IS adjacency goes down, even if both routing platforms use event-triggered generation of hello packets, it might take an additional hello interval before the adjacency is reestablished. [PR/63081: This issue has been resolved.]
- If a PIM multicast router does not succeed in an assert and receives an `<S,G>` Join message containing its own upstream interface address, the assert timer is not cleared. [PR/63150: This issue has been resolved.]
- If you issue the `show route advertising-protocol msdp` command, the routing protocol process (rpd) might restart. As a workaround, issue the more specific `show route table inet.4 advertising-protocol msdp` command. [PR/63375: This issue has been resolved.]
- If the routing platform receives an inet-flow route with a 0/0 prefix length, the routing protocol process (rpd) might stop operating. [PR/63520: This issue has been resolved.]
- If you disable Multicast Source Discovery Protocol (MSDP) in a configuration, then make routing-related changes to the configuration and issue two commits, the routing protocol process (rpd) might restart. As a workaround, deactivate or remove MSDP from the configuration. [PR/63576: This issue has been resolved.]

MPLS Applications

- The private address on the `fxp1` interface may confuse RSVP ERO processing. [PR/60689: This issue has been resolved.]
- If you configure traffic-engineering shortcuts for IS-IS, an IP hop-by-hop path might be preferred for a short time even though an RSVP LSP path is available. This temporary problem corrects itself within a few seconds. As a workaround, configure appropriate metrics on the MPLS LSPs. [PR/61894: This issue has been resolved.]
- If the routing platform reoptimizes the Constrained Shortest Path First (CSPF) algorithm after one of the current MPLS LSP transit links goes down, the value of the `CSPF metric:` field in the output of the `show mpls lsp name detail` command might be lower than expected and future CSPF recomputations might not find a shorter path. [PR/64059: This issue has been resolved.]

VPNs

- In an IPv6 over IPv4 tunnel network, when the routing platform rewrites a next hop to an interface address, it does not rewrite the associated BGP or VPN label. [PR/57930: This issue has been resolved.]
- Issuing the `show l2circuit connections` command causes the routing protocol process (rpd) to restart. [PR/59849: This issue has been resolved.]
- When adding a new CE interface to a VPLS routing instance, you might get the syslog error message “RT: Failed prefix change VPLS_FLOOD - (null) (Not found)” even if everything is working properly. [PR/60491: This issue has been resolved.]
- When the routing platform uses labeled BGP to advertise reachability to destinations connected by indirect next hops, the MPLS transit route added by BGP might not correctly track the forwarding next-hop changes on the indirect next hops. [PR/61225: This issue has been resolved.]
- If you issue an L2VPN or VPLS MIB walk of the pseudowire table, the routing protocol process (rpd) might stop operating. [PR/61626: This issue has been resolved.]
- If Layer 3 VPN interface up/down events occur, Layer 3 VPN interface up/down traps might not be sent. [PR/63071: This issue has been resolved.]

Forwarding and Sampling

- When a large sampling dump needs to be gzipped, the sampling process (sampled) might leave at most one gzip process in a zombie state. [PR/60545: This issue has been resolved.]
- When output packet filtering is performed on packets generated by the Routing Engine, the egress interface might be mistaken for the ingress interface. [PR/60726: This issue has been resolved.]
- If you upgrade a routing platform that has a configuration with prefix lists containing the `except` option in the firewall filter and the `apply-path` statement in the policy options, the configuration fails the upgrade validation check. As a workaround, configure the prefix list manually instead of using the `apply path`, or include at least one manually added entry in the prefix list in addition to the `apply-path` statement. [PR/61965: This issue has been resolved.]

Routing Policy and Firewall Filters

- If you reference an unused routing table in a policy statement, then issue the `commit` command several times, the policy might become corrupt and display the name of the routing table incorrectly. [PR/63351: This issue has been resolved.]

Network Management

- When a subagent (SA) control block is not found and a duplicate request is filtered, the SNMP process might leak memory. [PR/58353: This issue has been resolved.]
- Aggregated SONET is not reported as a composite link in the MIB. [PR/61061: This issue has been resolved.]
- If you issue an SNMP request to query LDP MIB statistics (jnxLdpStats), the request might time out. [PR/62109: This issue has been resolved.]

Release 7.2R1

The following issues have been resolved since JUNOS Release 7.1R1. The identifier following the description is the tracking number in our bug database.

Platform and Infrastructure

- After a Routing Engine switchover, the ipip interface goes down and might stop forwarding traffic. [PR/37021: This issue has been resolved.]
- When a target address was used as a next hop and static route reachability changed from *reachable* to *stale*, IPv6 neighbor solicitation (NS) packets might have been sent as unicast instead of multicast at the Media Access Control (MAC) address level, causing other vendor's equipment to discard these unicast NS packets. [PR/45704: This issue has been resolved.]
- When you configure a T-series routing platform or M320 with the `no-propagate-ttl` statement at the `[edit protocols mpls]` hierarchy level, the router might assign transit MPLS packets a time-to-live (TTL) value of 255 after a swap operation. In JUNOS Releases 7.1R1.2 and 7.2, the issue is resolved for T-series and M320 routing platforms. [PR/51663: This issue has been resolved.]
- Virtual Router Redundancy Protocol (VRRP) packets are not filtered by a loopback interface (lo0) firewall. As a workaround, configure the VRRP filter on a logical interface, rather than on lo0. [PR/52146: This issue has been resolved.]
- On J4300 and J6300 Services Routers, the `request system snapshot media usb partition as-primary` command does not work properly. It works correctly on J2300 Services Routers. [PR/55265: This issue has been resolved.]
- When a `traceroute` operation resolves over a label-switched path (LSP), the `show` command output does not display MPLS label information. [PR/55379: This issue has been resolved.]
- In certain scenarios, a Monitoring Services PIC might not come up again after being restarted. [PR/55868: This issue has been resolved.]
- Requests for statistics from ES interfaces might produce incorrect SA statistics and report an error in the log file. [PR/55970: This issue has been resolved.]

- On non-Enhanced FPCs on M-series routers, if you configure the `no-propagate-ttl` statement at the `[edit protocols mpls]` hierarchy level, the time to live (TTL) for IP packets transiting a label-switched path (LSP) is reset to the TTL of the MPLS packet. This often causes an increase in the IP TTL value. [PR/56025: This issue has been resolved.]
- When you configure and enable the Virtual Router Redundancy Protocol (VRRP) on a router, Dynamic Host Configuration Protocol (DHCP) packets might be forwarded with an incorrect source address. [PR/56117: This issue has been resolved.]
- If you enable load balancing, and MPLS labels and the IP payload are used to calculate the hashing index, the J-tree SRAM memory might leak when the label-switched path (LSP) flaps. [PR/56213: This issue has been resolved.]
- When the master Routing Engine is in alarm indication signal (AIS) / remote defect indication (RDI) state, the backup Routing Engine incorrectly adds one extra timeout call after Operation, Administration, and Maintenance (OAM) timer expiration. If the AIS/RDI condition persists for more than 9 hours, the backup Routing Engine resets after running out of kernel callout. [PR/56787: This issue has been resolved.]
- On non-Enhanced FPCs on M-series routers, label-switched paths (LSPs) configured with the `no-propagate-ttl` statement at the `[edit protocols mpls]` hierarchy level might fail to pass traffic. [PR/57257: This issue has been resolved.]
- Use of a NULL pointer in the kernel's tracing facility caused the Routing Engine to restart. [PR/57355: This issue has been resolved.]

User Interface and Configuration

- On a backup Routing Engine, extended user permissions were not replicated for template users. A workaround was to update both Routing Engines with the same version of the JUNOS software. [PR/55428: This issue has been resolved.]
- Using the J-Web interface to set OSPF interface authentication does not work properly. As a workaround, use the CLI to configure OSPF interfaces that require authentication, so that you can configure the OSPF interface and its authentication at the same time. [PR/55840: This issue has been resolved.]
- Inactive configurations were showing up as changed even after a fresh commit. [PR/57593: This issue has been resolved.]

Interfaces and Chassis

- You cannot configure maximum transmission unit (MTU) values on generic routing encapsulation (GRE) interfaces on routing platforms running JUNOS Release 6.3 and later. [PR/27357: This issue has been resolved.]
- On 4-port OC3 SONET/SDH interfaces, when you commit a configuration containing an invalid maximum transmission unit (MTU), the routing

platform might not generate an error message. [PR/46190: This issue has been resolved.]

- On Channelized intelligent queuing (IQ) OC12 PICs, the LOL (loss of light) defect and alarm were not detected and reported. [PR/46888: This issue has been resolved.]
- On Adaptive Services PICs, when you configure dynamic source Network Address Translation (NAT), and the routing platform establishes two consecutive sessions using the same client-server and same application service, some sessions might stall temporarily and then become established. [PR/48015: This issue has been resolved.]
- On TX Matrix platforms, when you take a 10 Gigabit Ethernet PIC offline and bring it online again, the `show chassis hardware` command output displays inconsistent small form-factor pluggable transceiver (SFP) information. [PR/51389: This issue has been resolved.]
- On aggregated Ethernet interfaces, a next-hop database update is not performed for logical interface link-state changes. This update is done only for physical interface link-state changes. [PR/51402: This issue has been resolved.]
- Virtual private LAN service (VPLS) circuits with IPSec tunnels configured on an Adaptive Services PIC might drop packets with a maximum transmission unit (MTU) value greater than 1400 unless the don't-fragment (df) bit is set. [PR/52835: This issue has been resolved.]
- On LSQ interfaces, Layer 2 overhead was not considered in QoS computations. This might have caused fragment loss at egress interfaces as a result of link oversubscription. [PR/53156: This issue has been resolved.]
- Under certain traffic load conditions, PPP keep-alive packets might be dropped and a PPP over Ethernet (PPPoE) session might go down. [PR/54995: This issue has been resolved.]
- On ATM interfaces with Automatic Protection Switching (APS), both the working and protect circuits were erroneously placed in enabled state at the same time because of a file corruption issue. [PR/55493: This issue has been resolved.]
- The source IP address of ICMP packets sent by intermediate nodes is not subjected to Network Address Translation. [PR/55605: This issue has been resolved.]
- To enable CoS to work correctly with a generic routing encapsulation (GRE) tunnel key, you might have to delete the GRE key and add it back again. [PR/55687: This issue has been resolved.]
- In certain scenarios on flow collector PICs, a memory overload condition might cause the PIC to reset. [PR/55700: This issue has been resolved.]
- On Adaptive Services PICs, if a UDP port scan is sent from an untrusted host to a trusted host, the intrusion detection system (IDS) table entries and

system log messages are listed correctly, but might indicate incorrectly that the attack originates from the trusted host. Additionally, if a TCP port scan is sent from an untrusted host to a trusted host, system log messages might lack the physical interface and logical interface unit of the attack source. [PR/56054: This issue has been resolved.]

- If you assign an identical name in a class-of-service fragmentation map and a scheduler map, the fragmentation map might not be correctly installed on a Link Services II bundle interface. As a workaround, do not assign the same name in both mappings. [PR/56083: This issue has been resolved.]
- External clocking mode was not set on T1 interfaces. [PR/56131: This issue has been resolved.]
- On Channelized STM1 intelligent queuing (IQ) PICs, an E1 channel in unframed framing mode might erroneously report an alarm indication signal path (AIS-P) error on the remote end. A workaround is to change the framing mode to G704. [PR/56141: This issue has been resolved.]
- Automatic Protection Switching (APS) does not support graceful restart. [PR/56190: This issue has been resolved.]
- If you configure a maximum transmission unit (MTU) value on an underlying interface, the forwarding process (fwdd) might dump core. Configure the value on a PPP over Ethernet (PPPoE) interface rather than on the underlying interface. [PR/56388, 56393: This issue has been resolved.]
- When you assign a PPP interface an IP address with a netmask of less than 30, the interface might not come up in some cases, depending on the IP address assigned to the remote end of the link. [PR/56493: This issue has been resolved.]
- On Adaptive Services PICs, service sets configured with application-protocol values of `exec` or `rpc` at the `[edit applications application name]` hierarchy level might drop flows. [PR/56623]
- When you use modems and Ascend L2TP access concentrators (LACs) to run L2TP multilink and do not configure Link Control Protocol (LCP) renegotiation, the L2TP process (lt2pd) might reset. [PR/57321, 57569: This issue has been resolved.]

General Routing

- When you include the `auto-export` statement at the `[edit routing-options]` hierarchy level, the routing process might restart unexpectedly. [PR/55461: This issue has been resolved.]

Routing Protocols

- Processing a reverse path forwarding (RPF) change might cause the routing protocol process (rpd) to dump core. [PR/45801: This issue has been resolved.]

- When you configure logical routers, Bidirectional Forwarding Detection (BFD) support is not available. [PR/51924: This issue has been resolved.]
- When another vendor's router is acting as an upstream router and there are multiple downstream routers, PIM processing of multicast VPNs might cause interoperability issues. If one of the downstream routers sends a prune for an earlier join, another router on the same LAN must send a prune override (if it still has the receivers) to continue receiving the traffic. [PR/55730: This issue has been resolved.]
- Under certain circumstances, the Multicast Source Discovery Protocol (MSDP) can consume large quantities of memory. [PR/55807: This issue has been resolved.]
- When the routing protocol process generates a PIM Join/Prune message for a large number of sources to a single group, a memory corruption might occur. [PR/55948: This issue has been resolved.]
- PIM sparse mode Rendezvous Point (RP) functionality does not work properly on provider edge J-series Services Routers. A workaround is to configure an available customer edge router as the local RP. [PR/56542: This issue has been resolved.]
- If you establish dynamic tunnels between two provider edge (PE) routers in Layer 3 VPNs and then unconfigure the tunnels and configure an RSVP label-switched path (LSP) between the two PE routers in the same commit, the routing protocol process (rpd) dumps core. [PR/56580: This issue has been resolved.]
- When you have configured a large number of groups, the PIM join information sent at the first periodic join might not include all groups. [PR/56605: This issue has been resolved.]
- Under some circumstances, when you configure multicast routing and perform mtrace operations, the routing protocol process might restart. [PR/56636: This issue has been resolved.]
- When Juniper Networks and other vendors' routing platforms have bootstrap router-related configurations in which the router's priority to be elected the bootstrap router is set to 0, it might cause interoperability issues resulting in constant flapping of rendezvous point (RP) data sent by the bootstrap router. As a workaround, either configure a non-zero bootstrap router priority on the other vendor's router or ensure that its IP address is higher than that of the Juniper Networks routing platform. [PR/56660: This issue has been resolved.]
- After a reverse path forwarding (RPF) change, the initial PIM trigger join does not contain all the (S,G) nodes. [PR/57144: This issue has been resolved.]

MPLS Applications

- In some complex topologies, RSVP fast reroute configuration might cause detours at a transit hop to flap continuously for indefinite periods. You can

observe a continually changing recorded route at the ingress router in this situation. [PR/56656: This issue has been resolved.]

- In LSP Ping echo request packets, the IP time to live (TTL) is not set to 1 as per the latest draft standard. [PR/56939: This issue has been resolved.]
- When you configure the `traceoptions` statement at the `[edit routing-options]` hierarchy level and set the `state` flag, the router generates a number of unnecessary traffic engineering messages. [PR/57117: This issue has been resolved.]
- Because of topology constraints, fast-reroute detours might perform link protection only. They do not revert to performing node protection when it becomes available. [PR/57146: This issue has been resolved.]

Class of Service

- When the JUNOS software pops the outer label of a payload header to encode a new label-switched path (LSP), the inner label's EXP field is rewritten with the current classification result, even when you have explicitly disabled EXP rewriting. [PR/42244: This issue has been resolved.]
- If you include the `class-of-service` statement at the `[edit protocols mpls label-switched-path]` hierarchy level with a nonzero value, this setting might affect other label-switched paths (LSPs) on the same logical interface. To restore normal rewrite operation, remove the `class-of-service` statement from LSP configuration, then disable and reenables the affected transit LSPs. [PR/51025: This issue has been resolved.]
- On Gigabit Ethernet IQ PICs, if you apply class of service to logical interfaces without a default classifier, all packets sent to 0 percent queues (queues 1 and 2) might be dropped. As a workaround, manually specify a transmission rate and buffer size of 1 percent for queues 1 and 2. Another workaround is to include the `per-unit-scheduler` statement at the `[edit interfaces ge-0/0/0]` hierarchy level and use VLAN encapsulation instead of Ethernet encapsulation. [PR/55048: This issue has been resolved.]

Routing Policy and Firewall Filters

- On M320 and T-series routing platforms, if you configure the `from forwarding-class` statement at the `[edit firewall family ccc filter filter-name term term-name]` hierarchy level, the firewall filter compiler (dfwc) might terminate. [PR/55573: This issue has been resolved.]

Network Management

- When you configure both passive monitoring and flow collector functionality for multiple PICs and SNMP is polling `jnxPMonFlowTable` and `jnxCollFileState`, the router might encounter SNMP `get-next` failures after a reboot. As a workaround, either stop SNMP polling during a router reboot or deactivate passive monitoring during reboot. [PR/55816: This issue has been resolved.]

Errata

This section lists outstanding issues with the documentation.

Feature Guide

- Next-hop groups support (M-series routers, except the M320 router)—You can configure the `next-hop-group` statement at the `[edit forwarding-options]` hierarchy level only on M5, M7i, M10, M10i, M20, M40, M40e, and M160 routers. [*Feature Guide*]

Interfaces and Chassis

- The AS PIC has a limit of 255 logical interfaces, where each logical interface is either an MLPPP bundle, an FRF.15 bundle, or an FRF.16 DLCI. [*Network Interfaces, Services Interfaces*]
- The 10-Gigabit Ethernet DWDM PIC is not available in JUNOS Release 7.2. This PIC is for M320, T320, and T640 routing platforms, and it will enable you to configure 10-Gigabit Ethernet DWDM interfaces with full C-band ITU-Grid tunable optics. [*Network Interfaces*]
- LSQ interfaces are not supported on T-Series routing platforms in JUNOS Release 7.2. [*Network Interfaces*]

MPLS Applications

- The `load-balance` statement at the `[edit protocols rsvp]` hierarchy level is not supported in JUNOS 7.2. [*MPLS Applications*]

Multicast

- Enabling PGM—To configure the Pragmatic General Multicast (PGM) protocol, you must include the `pgm` statement at the `[edit protocols]` hierarchy level. [*Multicast*]
- MDTs and Tunnel PICs—When configuring multicast over VPNs according to Internet draft draft-rosen-vpn-mcast-07.txt, each tunnel PIC supports 512 multicast tunnel (`mt`) interfaces. Configurations that allow more than 512 multicast tunnels require another tunnel PIC. Both default and data multicast distribution trees (MDTs) contribute to this total. There are typically two default multicast tunnels (one for encapsulation and the other for decapsulation). If a router with a single tunnel PIC tries to create more than 512 default or data MDTs, no traffic will flow for tunnels created in excess of 512. For example, a configuration that allows 500 data MDTs requires only a single tunnel PIC ($500 + 2 = 502$). However, a configuration that allows 1000 data MDTs requires two tunnel PICs ($1000 + 2 = 1002$). Up to 1024 multicast tunnels are supported with two tunnel PICs. [*Multicast*]

Routing Protocols

- BGP multipath enhancement—Enables you to disable the default requirement that paths accepted by BGP multipath must have the same neighboring AS. To configure, include the `multiple-as` statement at the `[edit protocols bgp group group-name multipath]` or `[edit protocols bgp group group-name neighbor name multipath]` hierarchy level. *[Routing]*

Services Interfaces

- AS PIC—An AS PIC installed on M10i, M20, and M40e routing platforms does support LNS services. *[Services Interfaces]*

System Log

- The correct name of the system log message code is `LIBJNX_INVALID_RE_SLOT_ID`, not `LIBJNX_INVALID_RE_SLOTID`. *[System Log]*

M-series and T-series Upgrade and Downgrade Instructions

This section discusses the following topics:

- Upgrade to Release 7.2 on page 46
- Downgrade from Release 7.2 on page 48

Upgrade to Release 7.2

When upgrading or downgrading the JUNOS software, 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 System Basics Configuration Guide*.



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 the JUNOS software. 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) may 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 System Basics Configuration Guide*.

The download and installation process for JUNOS Release 7.2R4 is the same as for previous JUNOS 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-7.2R4.2-domestic-signed.tgz
```

All other customers use the following command:

```
user@host> request system software add validate reboot
source /jinstall-7.2R4.2-export-signed.tgz
```

Replace `source` with one of the following:

- `/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 7.2 `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.

Downgrade from Release 7.2

To downgrade from Release 7.2 to another supported release, follow the procedure for upgrading, but replace the 7.2 `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 Release 7.5, you can downgrade the software to Release 7.2 directly, but not to Release 7.1; as a workaround, you can first downgrade to Release 7.2 and then downgrade to Release 7.1.

For more information, see the *JUNOS System Basics Configuration Guide*.

J-series Upgrade and Downgrade Instructions

This section contains the following topics:

- Upgrade Instructions on page 48
- Downgrade Instructions on page 52

Upgrade Instructions

This section contains the following topics:

- Before You Begin on page 49
- About the `junos-jseries` Package on page 49

- Installing Software Upgrades with the J-Web Interface on page 50
- Installing Software Upgrades with the CLI on page 51

Before You Begin

Before upgrading, be sure to back up the currently running and active file system and configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. To back up the file system, you must have a removable compact flash disk installed on the J4300 or J6300 Services Router, or a USB drive installed on any J-series Services Router. The backup device must have a storage capacity of at least 256 MB.

To back up the file system to the removable compact flash disk, issue the following command:

```
user@host> request system snapshot media removable-compact-flash
```

To back up the file system to the removable USB drive, issue the following command:

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

Before installing the software upgrade, issue the following command, which frees storage by rotating noncurrent log files in `/var/log`, deleting files in `/var/tmp` that have not been modified in two days, and deleting all crash files in `/var/crash`:

```
user@host> request system storage cleanup
```

Before deleting the files, you can view the files to be deleted by issuing the following command:

```
user@host> request system storage cleanup dry-run
```

About the junos-jseries Package

All junos-jseries software is delivered in signed packages that contain digital signatures. A package is installed only if the digital signature within it matches the signature recorded in its corresponding `.sig` file. (For example, `-export.tgz` contains `-export.tgz` and `-export.tgz.sig`. The `junos-jseries-release-export.tgz` package is installed only if the digital signatures match in the two `-export.tgz.sig` files.)

The junos-jseries package completely reinstalls the software. This package rebuilds the file system but retains configuration files and similar information from the previous version.

For more information, see the *J-series Services Router Administration Guide*.



NOTE: If the router is running a software version previous to JUNOS Release 7.2R3 or 7.3R2, you might need to upgrade to one of these interim software releases before you can upgrade to JUNOS Release 7.4.

Installing Software Upgrades with the J-Web Interface

You can install software upgrades from a remote server, or by uploading files to the Services Router.

Installing Software Upgrades from a Remote Server

You can use the J-Web interface to install software upgrades on the Services Router from a remote server.

To install software upgrades from a remote server:

1. Using a Web browser, follow the links to the following 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/>
 - <https://www.juniper.net/support/csc/swdist-ww/>
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 your local host or internal software distribution site.
4. In the J-Web interface, select **Manage > Software > Install Remote**.
5. On the Install Remote Quick Configuration page, enter information into the fields described in Table 2.
6. Click **Fetch and Install Package**. The software is activated after the router has rebooted.

Table 2: Install Remote Quick Configuration Field Descriptions

Field	Function	Your Action
Package Location (required)	Specifies the FTP or HTTP server, file path, and software package name location.	Type the full address of the software package location on the FTP or HTTP server.
User	Specifies the username, if the server requires one.	Type the username.
Password	Specifies the password, if the server requires one.	Type the password.
Reboot If Required	If this box is checked, the router is automatically rebooted when the upgrade is complete.	Check the box if you want the router to automatically reboot when the upgrade is complete.

Installing Software Upgrades by Uploading Files

You can use the J-Web interface to install software upgrades by uploading files to the Services Router.

To install software upgrades by uploading files:

- Using a Web browser, follow the links to the following 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/>
 - <https://www.juniper.net/support/csc/swdist-ww/>
- Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
- Download the software to your local host or internal software distribution site.
- In the J-Web interface, select **Manage > Software > Upload Package**.
- On the Upload Package Quick Configuration page, enter information into the fields described in Table 3.
- Click **Upload Package**. The software is activated after the router has rebooted.

Table 3: Upload Package Quick Configuration Field Descriptions

Field	Function	Your Action
File to Upload (required)	Specifies the location of the software package.	Type the location of the software package, or click Browse to navigate to the location.
Reboot If Required	If this box is checked, the router is automatically rebooted when the upgrade is complete.	Select the check box if you want the router to automatically reboot when the upgrade is complete.

Installing Software Upgrades with the CLI

To install software upgrades on a router using the CLI:

- Using a Web browser, follow the links to the following 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/>
 - <https://www.juniper.net/support/csc/swdist-ww/>

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 your local host.
4. Install the new package on the router:

```
user@host> request system software add validate unlink reboot source
```

Replace *source* with one of the following:

- */pathname/package-name*—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/package-name*
 - *http://hostname/pathname/package-name*

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.

The *unlink* option removes the package at the earliest opportunity in order to make room to complete the installation.

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.

Rebooting occurs only if the upgrade is successful.

Downgrade Instructions

This section contains the following topics:

- Downgrading the Software with the J-Web Interface on page 53
- Downgrading the Software with the CLI on page 53



NOTE: You cannot downgrade more than three releases. For example, if your routing platform is running JUNOS Release 7.5, you can downgrade the software to Release 7.2 directly, but not to Release 7.1. As a workaround, first downgrade to Release 7.2 and then downgrade to Release 7.1.

Downgrading the Software with the J-Web Interface

You can downgrade the software using the J-Web interface. When you downgrade the software to a previous version, the software version that is saved in `junos.old` is the version of the JUNOS software that your router is downgraded to. For your changes to take effect, you must reboot the router.

1. Go to **Manage > Software > Downgrade**. The previous version (if any) is displayed on this page.



NOTE: After you perform this operation, you cannot undo it.

2. Select **Downgrade** to downgrade to the previous version of the software or **Cancel** to cancel the downgrade process.
3. When the downgrade process is complete, for the new software to take effect, click **Manage > Reboot** to reboot the router.

Downgrading the Software with the CLI

You can revert to the previous set of software using the `request system software rollback` command in the CLI.

You can issue the `request system software rollback` command only once. Issuing the `request system software rollback` command again results in an error.

To downgrade to an earlier version of software, follow the procedure for upgrading, using the `junos-jseries` software bundle labeled for the appropriate release.

List of Technical Publications

Table 4 lists the software and hardware guides and release notes for Juniper Networks J-series, M-series, and T-series routing platforms and describes the contents of each document. Table 5 lists the books included in the *Network Operations Guide* series.

Table 4: Technical Documentation for J-series, M-series, and T-series Routing Platforms

Book	Description
	JUNOS Internet Software for J-series, M-series, and T-series Routing Platforms Configuration Guides

Book	Description
<i>Class of Service</i>	Provides an overview of the class-of-service (CoS) functions of the JUNOS software and describes how to configure CoS features, including configuring multiple forwarding classes for transmitting packets, defining which packets are placed into each output queue, scheduling the transmission service level for each queue, and managing congestion through the random early detection (RED) algorithm.
<i>CLI User Guide</i>	Describes how to use the JUNOS command-line interface (CLI) to configure, monitor, and manage Juniper Networks routing platforms. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Feature Guide</i>	Provides a detailed explanation and configuration examples for several of the most complex features in the JUNOS software.
<i>JUNOS-FIPS Configuration Guide</i>	(M-series and T-series routing platforms only) Provides an overview of JUNOS-FIPS 140-2 concepts and describes how to install and configure the JUNOS-FIPS software. Describes FIPS-related commands and how to configure, authorize, and zeroize the AS II FIPS PIC.
<i>MPLS Applications</i>	Provides an overview of traffic engineering concepts and describes how to configure traffic engineering protocols.
<i>Multicast Protocols</i>	Provides an overview of multicast concepts and describes how to configure multicast routing protocols.
<i>Network Interfaces</i>	Provides an overview of the network interface functions of the JUNOS software and describes how to configure the network interfaces on the routing platform.
<i>Network Management</i>	Provides an overview of network management concepts and describes how to configure various network management features, such as SNMP and accounting options.
<i>Policy Framework</i>	Provides an overview of policy concepts and describes how to configure routing policy, firewall filters, and forwarding options.
<i>Routing Protocols</i>	Provides an overview of routing concepts and describes how to configure routing, routing instances, and unicast routing protocols.
<i>Services Interfaces</i>	Provides an overview of the services interfaces functions of the JUNOS software and describes how to configure the services interfaces on the router.
<i>Software Installation and Upgrade Guide</i>	Provides a description of JUNOS software components and packaging, and includes detailed information about how to initially configure, reinstall, and upgrade the JUNOS system software. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>System Basics</i>	Describes Juniper Networks routing platforms, and provides information about how to configure basic system parameters, supported protocols and software processes, authentication, and a variety of utilities for managing your router on the network.
<i>VPNs</i>	Provides an overview and describes how to configure Layer 2 and Layer 3 virtual private networks (VPNs), virtual private LAN service (VPLS), and Layer 2 circuits. Provides configuration examples.
JUNOS References	

Book	Description
<i>Hierarchy and RFC Reference</i>	Describes the JUNOS configuration mode commands. Provides a hierarchy reference that displays each level of a configuration hierarchy, and includes all possible configuration statements that can be used at that level. This material was formerly covered in the <i>JUNOS System Basics Configuration Guide</i> .
<i>Interfaces Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot interfaces.
<i>Routing Protocols and Policies Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot routing policies and protocols, including firewall filters.
<i>System Basics and Services Command Reference</i>	Describes the JUNOS software operational mode commands you use to monitor and troubleshoot system basics, including commands for real-time monitoring and route (or path) tracing, system software management, and chassis management. Also describes commands for monitoring and troubleshooting services such as class of service (CoS), IP Security (IPSec), stateful firewalls, flow collection, and flow monitoring.
<i>System Log Messages Reference</i>	Describes how to access and interpret system log messages generated by JUNOS software modules and provides a reference page for each message.
J-Web User Guide	
<i>J-Web Interface User Guide</i>	Describes how to use the J-Web graphical user interface (GUI) to configure, monitor, and manage Juniper Networks routing platforms.
JUNOS API and Scripting Documentation	
<i>JUNOScript API Guide</i>	Describes how to use the JUNOScript application programming interface (API) to monitor and configure Juniper Networks routers.
<i>JUNOScript API Configuration Reference</i>	Provides reference pages for the configuration tag elements in the JUNOS XML API.
<i>JUNOScript API Operational Reference</i>	Provides reference pages for the operational tag elements in the JUNOS XML API.
NETCONF API Guide	Describes how to use the NETCONF API to monitor and configure Juniper Networks routing platforms.
<i>JUNOS Configuration and Diagnostic Automation Guide</i>	Provides an overview, instructions for using, and examples of the commit script and self-diagnosis features of the JUNOS software. This guide explains how to enforce custom configuration rules defined in scripts that run at commit time; how to use commit script macros to provide simplified aliases for frequently used configuration statements; and how to configure diagnostic event policies and actions associated with each policy.
JUNOS Comprehensive Index and Glossary	
JUNOS Internet Software Comprehensive Index and Glossary	Provides a complete index of all JUNOS Internet software books, the <i>JUNOScript API Guide</i> , and the NETCONF API Guide. Also provides a comprehensive glossary.
Hardware Documentation	
<i>Hardware Guide</i>	Describes how to install, maintain, and troubleshoot routing platforms and components. Each platform has its own hardware guide.

Book	Description
<i>PIC Guide</i>	Describes the routing platform's Physical Interface Cards (PICs). Each platform has its own PIC guide.
JUNOScope Documentation	
<i>JUNOScope Software User Guide</i>	Describes the JUNOScope software graphical user interface (GUI), how to install and administer the software, and how to use the software to manage router configuration files and monitor router operations.
J-series Services Router Documentation	
<i>Getting Started Guide</i>	Provides an overview, basic instructions, and specifications for J-series Services Routers. The guide explains how to prepare your site for installation, unpack and install the router and its components, install licenses, and establish basic connectivity.
J-series Services Router Basic LAN and WAN Access Configuration Guide	Explains how to configure the interfaces on J-series Services Routers for basic IP routing with standard routing protocols, ISDN backup, and digital subscriber line (DSL) connections.
J-series Services Router Advanced WAN Access Configuration Guide	Explains how to configure J-series Services Routers in virtual private networks (VPNs) and multicast networks, configure data link switching (DLSw) services, and apply routing techniques such as policies, stateless and stateful firewall filters, IP Security (IPSec) tunnels, and class-of-service (CoS) classification for safer, more efficient routing.
<i>J-series Services Router Administration Guide</i>	Shows how to manage users and operations, monitor network performance, upgrade software, and diagnose common problems on J-series Services Routers.
Release Notes	
<i>JUNOS Release Notes</i>	Summarize new features and known problems for a particular software release, provide corrections and updates to published JUNOS, JUNOScript, and NETCONF manuals, provide information that might have been omitted from the manuals, and describe upgrade and downgrade procedures.
<i>Hardware Release Notes</i>	Describe the available documentation for the routing platform and summarize known problems with the hardware and accompanying software. Each platform has its own release notes.
<i>JUNOScope Release Notes</i>	Contain corrections and updates to the published JUNOScope manual, provide information that might have been omitted from the manual, and describe upgrade and downgrade procedures.
<i>J-series Services Router Release Notes</i>	Briefly describe Services Router features, identify known hardware problems, and provide upgrade and downgrade instructions

Table 5: JUNOS Internet Software Network Operations Guides

Book	Description
JUNOS Internet Software for M-series and T-series Routing Platforms Network Operations Guides	

Book	Description
<i>Baseline</i>	Describes the most basic tasks for running a network using Juniper Networks products. Tasks include upgrading and reinstalling JUNOS software, gathering basic system management information, verifying your network topology, and searching log messages.
<i>Interfaces</i>	Describes tasks for monitoring interfaces. Tasks include using loopback testing and locating alarms.
<i>MPLS</i>	Describes tasks for configuring, monitoring, and troubleshooting an example MPLS network. Tasks include verifying the correct configuration of the MPLS and RSVP protocols, displaying the status and statistics of MPLS running on all routers in the network, and using the layered MPLS troubleshooting model to investigate problems with an MPLS network.
<i>MPLS Log Reference</i>	Describes MPLS status and error messages that appear in the output of the <code>show mpls lsp extensive</code> command. The guide also describes how and when to configure Constrained Shortest Path First (CSPF) and RSVP trace options, and how to examine a CSPF or RSVP failure in a sample network.
<i>Hardware</i>	Describes tasks for monitoring M-series and T-series routing platforms.

Requesting Support

For technical support, open a support case with the Case Manager link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

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://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 <http://www.juniper.net/techpubs/docbug/docbugreport.html>.

For documentation issues, fill out the bug report form located at <http://www.juniper.net/techpubs/docbug/docbugreport.html>.

Revision History

15 August 2006—Added section on the **include-any** statement to the *Changes in Default Behavior and Syntax* section

14 February 2006—Revision 4, JUNOS Release 7.2R4

8 November 2005—Revision 3, JUNOS Release 7.2R3

6 July 2005—Revision 2, JUNOS Release 7.2R2

22 April 2005—Revision 1, JUNOS Release 7.2R1

Copyright © 2006, Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. JUNOS and JUNOSe are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.