JUNOS® OS 14.1 RELEASE NOTES

INSIDE THIS RELEASE

Supported on EX Series, M Series, MX Series, PTX Series, and T Series

NEW SOFTWARE FEATURES

- EX9200-SF2 enhanced switch fabric (EX9204, EX9208, and EX9214)
- Egress protection for BGP labeled unicast (M Series, MX Series, T Series)
- IRB interface on EVPNs (MX Series)
- Virtual switch support for EVPNs (MX Series)
- BGP multihoming support for EVPNs (MX Series)
- Group VPN member support (MX240, MX480, and MX960)
- Selecting backup LFA for IS-IS routing protocol (M Series, MX Series, and T Series)
- Recursive DNS server ICMPv6 router advertisement option support (M Series, MX Series, and T Series)
- Adaptive Load Balancing (ALB) for aggregated Ethernet bundles (PTX Series)
- Physical interface damping (PTX and T Series)
- Subscriber accounting MIB support (M Series, MX Series, and T Series)
- Advertising multiple paths in BGP (MX Series and T Series)

NEW DEVICES AND MODULES

- Guided cabling (TX Matrix Plus routers with 3D SIBs)
- Simultaneous BITS/BITS redundancy on SCBE2 (MX240, MX480, and MX960)
- FPC with eight Packet Forwarding Engines (PTX5000)
- 4-port 100-Gigabit Ethernet PIC (PTX5000)
- SIB to support high density FPC (PTX5000)
- High-capacity DC PSM and PDU (PTX5000)

RECENTLY RELEASED DOCUMENTATION

- Day One: MPLS for Enterprise Engineers
- MetaFabric Architecture Virtualized Data Center Design and Implementation Guide
- Enterprise WAN Aggregation and Internet Edge Design and Implementation Guide
- NCE—Frequently Asked Questions: MPLS in Juniper Networks Switches
- Business Edge Design Guide
- Flow Monitoring Feature Guide
- Learn About Differences in Addressing between IPv4 and IPv6
- Learn About Data Center Bridging
- Learn About Secure VPNs

Release Notes: Junos® OS Release 14.1R1 for the EX Series, M Series, MX Series, PTX Series, and T Series

24 July 2014

Contents

Introduction

Junos OS runs on the following Juniper Networks® hardware: ACX Series, EX Series, J Series, M Series, MX Series, PTX Series, QFabric, QFX Series, SRX Series, and T Series.

These release notes accompany Junos OS Release 14.1R1 for the EX Series, M Series, MX Series, PTX Series, and T Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

Junos OS Release Notes for EX Series Switches

These release notes accompany Junos OS Release 14.1R1 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at http://www.juniper.net/techpubs/software/junos/.

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 14.1R1 for the EX Series.

Hardware

- **High-speed switch fabric module for EX9200 switches**—Starting with Junos OS Release 14.1, a high-speed SF module, EX9200-SF2, is supported. The Switch Fabric serves as the central nonblocking matrix through which all network data passes. Compared to the original SF module, EX9200-SF, the EX9200-SF2 offers increased bandwidth, providing higher-capacity traffic support in settings that require greater interface density (slot and capacity scale).

  SF modules are installed horizontally on the front panel of the switch chassis. You can install either one or two SF modules in an EX9204 or EX9208 switch and either two or three SF modules in an EX9214 switch.

  The key functions of the Switch Fabric are:

- Monitor and control system functions
- Interconnection of all line cards
- Clocking, system resets, and booting control
- Routing Engine carrier

The EX9200-SF2 supports all EX9200 line cards.

NOTE: When you upgrade from an EX9200-SF module to an EX9200-SF2 module in an EX9200 switch, the SF module types can co-exist in the switch *during* the upgrade. You must replace that EX9200-SF module with another EX9200-SF2 module for normal switch operation.

VPNs

- **Multihoming support for EVPNs (EX9200)**—Starting with Junos OS Release 14.1, the Ethernet VPN (EVPN) solution is extended to provide multihoming functionality in the active-standby redundancy mode of operation.

  To enable EVPN active-standby multihoming, include the **single-active** statement at the **[edit interfaces esi]** hierarchy level.

  [See Example: Configuring EVPN Multihoming.]

Related Documentation

- Changes in Behavior and Syntax on page 5
- Known Behavior on page 6
- Known Issues on page 6
- Documentation Updates on page 7
- Migration, Upgrade, and Downgrade Instructions on page 7
- Product Compatibility on page 8

Changes in Behavior and Syntax

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 14.1R1 for the EX Series.

- Platform and Infrastructure

Platform and Infrastructure

- **Changes in show chassis hardware command output descriptions for EX9200 components**—Starting with Junos OS Release 14.1, the output of the **show chassis hardware** command includes descriptions for enhanced midplanes on EX9204 and EX9208 switches (enhanced midplanes are already on EX9214 switches) and the high-speed SF module, as highlighted in the following sample:

  ```
  user@switch> show chassis hardware
  ```

```
Hardware inventory:
Item             Version  Part number  Serial number     Description
Chassis                                JN1221A03RFC      EX9204
Midplane         REV 01   750-053633   ACRA1451          EX9204-BP
FPM Board        REV 04   760-021392   ABCB4822          Front Panel Display
PEM 0            Rev 10   740-029970   QCS1251U020       PS 1.4-2.52kW; 90-264V
 AC in
PEM 1            Rev 10   740-029970   QCS1251U028       PS 1.4-2.52kW; 90-264V
 AC in
Routing Engine 0 REV 02   740-049603   9009153805         RE-S-EX9200-1800X4
Routing Engine 1 REV 02   740-049603   9009153993         RE-S-EX9200-1800X4
CB 0              REV 08   750-048307   CABC6474          EX9200-SF2
CB 1              REV 10   750-048307   CABH8948          EX9200-SF2
...
```

Related Documentation

- New and Changed Features on page 4
- Known Behavior on page 6
- Known Issues on page 6
- Documentation Updates on page 7
- Migration, Upgrade, and Downgrade Instructions on page 7
- Product Compatibility on page 8

Known Behavior

There are no changes in known behavior in Junos OS Release 14.1R1 for the EX Series.

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

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 5
- Known Issues on page 6
- Documentation Updates on page 7
- Migration, Upgrade, and Downgrade Instructions on page 7
- Product Compatibility on page 8

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 14.1R1 for the EX Series.

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

- Interfaces and Chassis

Interfaces and Chassis

- On an EX9200 switch working as a DHCP server, when you delete an IRB interface or change the VLAN ID of a VLAN corresponding with an IRB interface, the DHCP process (jdhcpd) might create a core file after commit, because a stale interface entry in the jdhcpd database has been accessed. PR979565
- On EX9200 switches, the configuration statement **mcae-mac-flush** is not available in the CLI; it is missing from the **[edit vlans]** hierarchy. PR984393
- On an EX9200 switch, if the underlying Layer 2 interface of an IRB interface is changed from access mode to trunk mode and bi-directional traffic is sent from an interface on the same switch that has been changed from IRB over Layer 2 to Layer 3 mode, the Layer 3 traffic toward the IRB interface might be dropped and PPE thread timeout errors might be displayed. As a workaround, deactivate and then reactivate the Layer 2 trunk interface underlying the IRB interface where the dropped traffic is occurring. PR995845

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 5
- Known Behavior on page 6
- Documentation Updates on page 7
- Migration, Upgrade, and Downgrade Instructions on page 7
- Product Compatibility on page 8

Documentation Updates

There are no errata or changes in Junos OS Release 14.1R1 for the EX Series switches documentation.

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 5
- Known Behavior on page 6
- Known Issues on page 6
- Migration, Upgrade, and Downgrade Instructions on page 7
- Product Compatibility on page 8

Migration, Upgrade, and Downgrade Instructions

This section contains upgrade and downgrade policies for Junos OS for the EX Series. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

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

- Upgrade and Downgrade Support Policy for Junos OS Releases on page 8

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

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

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 5
- Known Behavior on page 6
- Known Issues on page 6
- Documentation Updates on page 7
- Product Compatibility on page 8

Product Compatibility

- Hardware Compatibility on page 8

Hardware Compatibility

To obtain information about the components that are supported on the devices, and special compatibility guidelines with the release, see the Hardware Guide for the product.

To determine the features supported on EX Series switches in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and

compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at:
http://pathfinder.juniper.net/feature-explorer/

Related Documentation

- New and Changed Features on page 4
- Changes in Behavior and Syntax on page 5
- Known Behavior on page 6
- Known Issues on page 6
- Documentation Updates on page 7
- Migration, Upgrade, and Downgrade Instructions on page 7

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

These release notes accompany Junos OS Release 14.1R1 for the M Series, MX Series, and T Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at http://www.juniper.net/techpubs/software/junos/.

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 14.1R1 for the M Series, MX Series, and T Series.

Hardware

- **Support for guided cabling (TX Matrix Plus routers with 3D SIBs)**—Junos OS Release 14.1 supports guided cabling in a routing matrix based on a TX Matrix Plus router with 3D SIBs. When you enable guided cabling, blinking LEDs on unconnected ports help you connect cables between the TXP-F13-3D and the TXP-LCC-3D SIBs.

  Use the following commands to enable or disable guided cabling:

  - To enable guided cabling, use the **request chassis fabric guided-cabling (all-lcc | lcc *lcc-number*) enable (plane-by-plane | port-by-port)** operational mode command.
  - To disable guided cabling, use the **request chassis fabric guided-cabling (all-lcc | lcc *lcc-number*) disable** operational mode command.

  [See Guided Cabling Overview , request chassis fabric guided-cabling enable , and request chassis fabric guided-cabling disable]

- **Support for simultaneous BITS/BITS redundancy on SCBE2 (MX240, MX480, and MX960)**—Starting with Junos OS Release 14.1, simultaneous BITS/BITS redundancy is supported on SCBE2 on MX240, MX480, and MX960 routers. You can configure both the external interfaces for BITS input. One of the BITS inputs is considered as a primary clock source and the other as a secondary clock source on the basis of the configured clock quality.

  [See Centralized Clocking Overview.]

- **Unified ISSU support (TX Matrix Plus router with 3D SIBs)**—Unified in-service software upgrade (ISSU) is supported on a TX Matrix Plus router with 3D SIBs. Unified ISSU enables you to upgrade from an earlier Junos OS release to a later one with no disruption on the control plane and with minimal disruption of traffic.

  [See Unified ISSU Concepts]

Class of Service (CoS)

- **Distributed periodic packet management support for aggregated Ethernet interfaces (T4000)**—Starting with Release 14.1, Junos OS extends support on T4000 routers for the Bidirectional Forwarding Detection (BFD) protocol to use the periodic packet management daemon (ppmd) to distribute IPv4 sessions over aggregated Ethernet interfaces. Only IPv4 BFD sessions over aggregated Ethernet interfaces are supported. The ppmd process automatically runs on the Routing Engine and the Packet Forwarding Engine. To disable ppmd on the Packet Forwarding Engine only, include the **no-delegate-processing** statement at the **[edit routing-options ppm]** hierarchy level. The ppmd process does not support IPv6 BFD sessions or MPLS BFD sessions over an aggregated Ethernet interface.

  [See ppm and no-delegate-processing.]

- **Support for limiting traffic black-hole time by detecting Packet Forwarding Engine destinations that are unreachable (T4000)**—Junos OS Release 14.1 and later releases extend support for T4000 routers to limit traffic black-hole time by detecting unreachable destination Packet Forwarding Engines. The router signals neighboring routers when it cannot carry traffic because of the inability of some or all source Packet Forwarding Engines to forward traffic to some or all destination Packet Forwarding Engines on any fabric plane, after interfaces have been created. This inability to forward traffic results in a traffic black hole. By default, the system limits traffic black-hole time by detecting severely degraded fabric. No user interaction is necessary.

  [See Traffic Blackholing Caused by Fabric Degradation, Disabling FPC Restart, degraded, action-fpc-restart-disable, show chassis fabric reachability, and show chassis fabric unreachable-destinations.]

- **Setting IPv4 and IPv6 DSCP and MPLS EXP bits independently (T4000 and TXP-4000-3D)**—Junos OS Release 14.1and later releases extend support to set the packet DSCP and MPLS EXP bits independently on IPv4 and IPv6 packets on T4000 Type 5 FPCs (model numbers: T4000-FBC5-3D and T4000-FPC5-LSR) in T4000 routers and the TXP-4000-3D chassis. To enable this feature for IPv4, include the **protocol mpls** statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number* rewrite-rules dscp *rewrite-name*]** hierarchy level. To enable this feature for IPv6, include the **protocol mpls** statement at the **[edit class-of-service interfaces *interface-name* unit *logical-unit-number* rewrite-rules dscp-ipv6 *rewrite-name*]** hierarchy level. You can set DSCP IPv4 and IPv6 values only at the ingress MPLS node. The following rewrite combinations are supported:

  - DSCP or inet-precedence and EXP rewrite on IPv4 packets
  - DSCPv6 and EXP rewrite on IPv6 packets

  [See Applying Rewrite Rules to Output Logical Interfaces, Setting IPv6 DSCP and MPLS EXP Values Independently, Configuring DSCP Values for IPv6 Packets Entering the MPLS Tunnel, and Configuring Rewrite Rules.]

- **Layer 2 CoS-based traffic metering (MX80 and MX Series with MPCs)**—Starting with Junos OS Release 14.1, Layer 2 accounting statistics are available on a per class-of-service basis. Both bytes and packet total are counted (flow rates are not).

A single, aggregate counter can be used with each forwarding class to count inet and inet6 flows. For ingress, only packets forwarded to the fabric are counted, and for egress, only packets forwarded to the WAN are counted. You can exclude overhead bytes from the count, as well as dropped packets and non-relevant network protocols such as ARP, BFD, and EOAM. Counters can be configured with any or all of the following parameters:

- logical/physical interfaces
- IPv4/IPv6 traffic types
- unicast/multicast traffic
- ingress/egress flows

Configure the counters using the **enhanced** command under **forwarding-class-accounting** in the CLI.

Dynamic Host Configuration Protocol (DHCP)

- **Recursive DNS server ICMPv6 router advertisement option support (M Series, MX Series, and T Series)**—Beginning with Junos OS Release 14.1, you can configure a maximum of three recursive DNS server addresses and their respective lifetimes through static configuration at the interface level for IPv6 hosts. Previously, rpd supported only link-local address information, prefix information, and the link MTU. The router advertisement-based DNS configuration is useful in networks where an IPv6 host's address is auto-configured through an IPv6 stateless address and where there is no DHCPv6 infrastructure available.

  To configure the recursive DNS server address, include the **dns-server-address** statement at the **[edit protocols router-advertisement interface *interface-name*]** hierarchy level.

  [See Example: Configuring Recursive DNS Address.]

Forwarding and Sampling

- **Native analyzer support (MX240, MX480, and MX960)**—Starting in Junos OS Release 14.1, support is provided for native analyzers and remote port-mirroring capabilities on the MX240, MX480, and MX960. A native analyzer configuration contains both an input stanza and an output stanza in the analyzer hierarchy for mirroring packets. In remote port mirroring, the mirrored traffic is flooded into a remote mirroring VLAN that can be specifically created for the purpose of receiving mirrored traffic. The analyzer configuration is available at the **[edit-forwarding-options]** hierarchy level.

General Routing

- **Updated behavior in static link protection Mode (M Series, MX Series, and T Series)**—In static link protection mode you can designate a primary and backup physical link to support aggregated interfaces link protection. Starting with Junos OS Release 14.1, a backup link can be configured to either accept ingress traffic, discard ingress traffic, or remain down until it becomes active and starts carrying traffic. By default, the backup link accepts ingress traffic. The following new attributes have been added to **link-protection** to control these settings:

  - bkp-state-accept: Default, accept ingress traffic on the backup link
  - bkp-state-discard: Discard ingress traffic on the backup link
  - bkp-state-down: Mark the backup link as Down while the primary link is active

- **Support for preserving prenormalized ToS value in an egress mirrored or sampled packet (M Series, MX Series, and T Series)**—Beginning with Junos OS Release 14.1, on MPC-based interfaces, you can preserve the prenormalized type-of-service (ToS) value for egress mirrored or sampled packets. To retain the pre-rewrite ToS value in mirrored or sampled packets, configure the **pre-rewrite-tos** statement at the **[edit forwarding-options sampling]** hierarchy level. This preserves the pre-rewrite ToS value for all forms of sampling, such as Routing Engine-based sampling, port mirroring, flow monitoring, and so on. This statement is effective for egress sampling only.

High Availability (HA) and Resiliency

- **MX Series Virtual Chassis support for determining member router health (MX Series routers with MPCs)**—Starting in Junos OS Release 14.1, you can configure an IP-based packet connection, known as a *heartbeat connection*, between the master router and backup router in an MX Series Virtual Chassis. The heartbeat connection exchanges *heartbeat packets* that provide important information about the availability and health of each member router.

  If a disruption or split occurs in the Virtual Chassis configuration, the heartbeat connection helps prevent the member routers from changing roles, which could cause undesirable results.

  To configure a heartbeat connection, first create a secure and reliable route between the master router and backup router. You can then configure the connection by including the **heartbeat-address** and **heartbeat-timeout** statements at the **[edit virtual-chassis]** hierarchy level.

- **MX Series Virtual Chassis support for locality bias (MX Series routers with MPCs)**—Starting in Junos OS Release 14.1, you can configure *locality bias* for aggregated Ethernet and equal-cost multipath (ECMP) traffic in an MX Series Virtual Chassis. Locality bias directs unicast transit traffic for ECMP groups and aggregated Ethernet bundles to egress links in the same (local) member router in the Virtual Chassis rather than to egress links in the remote member router, provided that the local member router has an equal or larger number of available egress links than the remote member router.

  Configuring locality bias enables you to conserve bandwidth on the Virtual Chassis port links by directing all ECMP and aggregated Ethernet data traffic to local egress links rather than across the Virtual Chassis port links between member routers.

  To enable locality bias, configure the **locality-bias** statement at the **[edit virtual-chassis]** hierarchy level.

  

  BEST PRACTICE: To avoid possible traffic loss and oversubscription on egress interfaces, make sure that you understand the utilization

requirements for the local links in your network before changing the locality bias configuration.

- **MX Series Virtual Chassis support for unified ISSU (MX Series with MPCs/MICs)**—Starting in Junos OS Release 14.1, you can perform a unified in-service software upgrade (unified ISSU) on member routers in an MX Series Virtual Chassis configuration. Unified ISSU enables you to upgrade the the system software on the Virtual Chassis member routers with minimal traffic disruption and no disruption on the control plane.

  To start a unified ISSU in an MX Series Virtual Chassis, issue the **request system software in-service-upgrade *package-name*** command from the master Routing Engine in the Virtual Chassis master router (VC-Mm). This command always reboots each of the four Routing Engines in the Virtual Chassis.

  [See Unified ISSU in a Virtual Chassis, Unified ISSU System Requirements.]

- **MX Series Virtual Chassis support for Layer 2 spanning-tree protocols (MX Series with MPCs)**—Starting in Junos OS Release 14.1, an MX Series Virtual Chassis configuration supports the following Layer 2 Control Protocol (L2CP) features, known collectively as xSTP:

  - Spanning Tree Protocol (STP)
  - Rapid Spanning Tree Protocol (RSTP)
  - Multiple Spanning Tree Protocol (MSTP)
  - VLAN Spanning Tree Protocol (VSTP)

  Spanning-tree protocols resolve the forwarding loops in a Layer 2 network, thereby creating a loop-free tree topology. Configuring spanning-tree protocols provides link redundancy in case of link failures, and prevents undesirable loops in the data path.

  To configure and manage STP, RSTP, MSTP, or VSTP in a Virtual Chassis, you use the same procedures for a member router in an MX Series Virtual Chassis as you do for a standalone MX Series router.

  [See Spanning-Tree Protocols Supported and Virtual Chassis Components Overview.]

- **MX Series Virtual Chassis support for inline flow monitoring (MX Series routers with MPCs)**—Starting in Junos OS Release 14.1, you can configure inline flow monitoring for an MX Series Virtual Chassis. Inline flow monitoring enables you to actively monitor the flow of traffic by means of a router participating in the network.

  Inline flow monitoring for an MX Series Virtual Chassis provides the following support:

  - Active sampling and exporting of both IPv4 and IPv6 traffic flows
  - Sampling traffic flows in both the ingress and egress directions

  - Configuration of flow collection on either IPv4 or IPv6 devices
  - Use of the IPFIX flow collection template for traffic sampling (both IPv4 and IPv6 export records)

- **Support for LACP with Fast Hellos During ISSU**—MX Series routers now support LACP with fast hellos during ISSU. This support is disabled by default. To enable it you need to enter the new CLI knob **set protocols lacp fast-hello-issu** on both the DUT and peer routers before starting ISSU. The peer router must also be a MX Series Router for this functionality to work.

Interfaces and Chassis

- **Support for physical interface damping (T Series)**—Beginning with Junos OS Release 14.1, interface damping is supported on *physical interfaces* to address longer periodic flapping lasting 5 seconds or more, with an up and down duration of 1 second. This damping method limits the number of advertisements of longer interface up and down events to the upper-level protocols. For longer periodic interface flaps, configure interface damping with the **damping** statement at the **[edit interfaces *interface-name*]** hierarchy level. You use the **show interfaces extensive** command to view the interface damping values and link state.

  [See Damping Longer Physical Interface Transitions.]

- **Support for MC-LAG on logical systems**—Starting with Junos OS Release 14.1, you can configure multichassis link aggregation (MC-LAG) interfaces on logical systems within a router. To configure ICCP for MC-LAG interfaces on logical systems, include the **iccp** statement at the **[edit logical-systems *logical-system-name* protocols]** hierarchy level. To view ICCP information for MC-LAG on logical systems, use the **show iccp logical-system *logical-system-name*** command. To view ARP statistics or remote MAC addresses for the multichassis aggregated Ethernet (MC-AE) nodes for all or specified redundancy groups on a logical system, use the **show l2-learning redundancy-groups *group-name* logical-system *logical-system-name* (arp-statistics | remote-macs)** command. To view neighbor discovery statistical details for MC-AE nodes on redundancy groups of a logical group, use the **show l2-learning redundancy-groups *group-name* logical-system *logical-system-name* nd-statistics** command.

  [See Multichassis Link Aggregation on Logical Systems Overview.]

- **Inline Multilink PPP, Multilink Frame Relay, and Multilink Frame Relay End-to-End for time-division multiplexing WAN interfaces (MX Series)**— Starting in Junos OS Release 14.1, this feature allows support of Inline Multilink PPP (MLPPP), Multilink Frame Relay (FRF.16), and Multilink Frame Relay End-to-End (FRF.15) for time-division multiplexing (TDM) WAN interfaces provide bundling services through the Packet Forwarding Engine without requiring a PIC or Dense Port Concentrator (DPC).

  Traditionally, bundling services are used to bundle multiple low-speed links to create a higher bandwidth pipe. This combined bandwidth is available to traffic from all links and supports link fragmentation and interleaving (LFI) on the bundle, reducing high priority packet transmission delay.

This support includes multiple links on the same bundle as well as multiclass extension for MLPPP. Through this service you can enable bundling services without additional DPC slots to support Service DPC and free up the slots for other MICs.

For connecting many smaller sites in VPNs, bundling the TDM circuits with MLPPP/MLFR technology is the *only* way to offer higher bandwidth and link redundancy.

MLPPP enables you to bundle multiple PPP links into a single multilink bundle, and MLFR enables you to bundle multiple Frame Relay data-link connection identifiers (DLCIs) into a single multilink bundle. Multilink bundles provide additional bandwidth, load balancing, and redundancy by aggregating low-speed links, such as T1, E1, and serial links.

[See Inline MLPPP for WAN Interfaces Overview, Example: Configuring Inline MLPPP and Multilink Frame Relay End-to-End (FRF.15) for WAN Interfaces, and Example: Configuring Inline Multilink Frame Relay (FRF.16) for WAN Interfaces.]

- **SFPP-10G-CT50-ZR (MX Series)**—The SPFF-10G-CT50-ZR tunable transceiver provides a duplex LC connector and supports the 10GBASE-Z optical interface specification and monitoring. The transceiver is not specified as part of the 10-Gigabit Ethernet standard and is instead built according to Juniper Networks specifications. Only WAN-PHY and LAN-PHY modes are supported. To configure the wavelength on the transceiver, use the **wavelength** statement at the **[edit interfaces *interface-name* optics-options]** hierarchy level. The following interface modules support the SPFF-10G-CT50-ZR transceiver:

  MX Series:

  - 16-port 10-Gigabit Ethernet MPC (model number: MPC-3D-16XGE-SFPP)—Supported in Junos OS Release 12.3R6, 13.2R3, 13.3R2, 14.1, and later.

  For more information about interface modules, see the "Cables and Connectors" section in the *Interface Module Reference* for your router.

  [See 10-Gigabit Ethernet 10GBASE Optical Interface Specifications and wavelength.]

- **SFPP-10G-ZR-OTN-XT (MX Series, T1600, and T4000)**—The SFPP-10G-ZR-OTN-XT dual-rate extended temperature transceiver provides a duplex LC connector and supports the 10GBASE-Z optical interface specification and monitoring. The transceiver is not specified as part of the 10-Gigabit Ethernet standard and is instead built according to ITU-T and Juniper specifications. In addition, the transceiver supports LAN-PHY and WAN-PHY modes and OTN rates and provides a NEBS-compliant 10-Gigabit Ethernet ZR transceiver for the MX Series interface modules listed below. The following interface modules support the SFPP-10G-ZR-OTN-XT transceiver:

  MX Series:

  - 10-Gigabit Ethernet MIC with SFP+ (model number: MIC3-3D-10XGE-SFPP)—Supported in Junos OS Release 12.3R5, 13.2R3, 13.3, and later
  - 16-port 10-Gigabit Ethernet (model number: MPC-3D-16XGE-SFPP)—Supported in Junos OS Release 12.3R5, 13.2R3, 13.3, and later

- 32-port 10-Gigabit Ethernet MPC4E (model number: MPC4E-3D-32XGE-SFPP)—Supported in Junos OS Release 12.3R5, 13.2R3, 13.3, and later
- 2-port 100-Gigabit Ethernet + 8-port 10-Gigabit Ethernet MPC4E (model number: MPC4E-3D-2CGE-8XGE)—Supported in Junos OS Release 12.3R5, 13.2R3, 13.3, and later

T1600 and T4000 routers:

- 10-Gigabit Ethernet LAN/WAN PIC with Oversubscription and SFP+ (model numbers: PD-5-10XGE-SFPP and PF-24XGE-SFPP)—Supported in Junos OS Release 12.3R5, 13.2R3, 13.3, and later
- 10-Gigabit Ethernet LAN/WAN PIC with SFP+ (model number: PF-12XGE-SFPP)—Supported in Junos OS Release 12.3R5, 13.2R3, 13.3, and later

For more information about interface modules, see the "Cables and Connectors" section in the *Interface Module Reference* for your router.

[See 10-Gigabit Ethernet 10GBASE Optical Interface Specifications.]

IPv6

- **Expanded ALG support with NAT64 (MX Series routers with MS-MPC or MS-MIC lines cards)**—Starting with Junos OS Release 14.1, the FTP, TFPT, SIP, RTSP, and PPPT ALGs are supported. To configure the ALGs, include the **applications [*applications-list*]** statement at the **[edit services nat rule *rule-name* term *termname* from]** hierarchy level.

  Include in the ALG list, *applications-list*, Junos OS identifiers for desired ALGs:

  - **junos-ftp** for FTP
  - **junos-tftp** for TFTP
  - **junos-sip** for SIP
  - **junos-rtsp** for RTSP
  - **junos-pppt** for PPPT

- **Limit softwire flows per IPv6 prefix for DS-Lite (MX Series routers with MS-DPC interface cards)**—Junos OS provides a configurable option to limit the number of softwire flows from a subscriber's Basic Bridging Broadband (B4) device at a given point in time, thus limiting excessive use of addresses within the subnet available to a subscriber. This limitation reduces the risk of denial-of-service (DOS) attacks.

  To specify the size of the subnet subject to limitation, include the **dslite-ipv6-prefix-length *prefix-length*** statement at the **[edit services service-set *service-set-name* softwire-options]** hierarchy level. Specify a prefix length of 56, 64, 98, or 128.

  Starting in Junos OS Release 14.1, the **show services nat mappings address-pooling-paired** operational command output shows the mapping for the prefix. The mapping shows the address of the active B4.

The **show services softwire flows** output shows active and inactive softwire flows from the same prefix.

Layer 2 Features

- **Support for configuring PPP NCP negotiation mode (MX Series routers with MPCs)**—Starting in Junos OS Release 14.1, both static and dynamic subscriber interfaces use passive PPP NCP negotiation by default. To enable active negotiation, use the new **initiate-ncp** configuration statement with the appropriate option:
  - For IPv4 (**inet** family) subscriber interfaces, use the **initiate-ncp ip** statement.
  - For IPv6 (**inet6** family) subscriber interfaces, use the **initiate-ncp ipv6** statement.

  You can also configure the negotiation mode for the PPP server in an IPv4/IPv6 dual-stack configuration:
  - For active negotiation, use the **initiate-ncp ip** statement for the IPv4 subscriber interface and the **initiate-ncp ipv6** statement for the IPv6 subscriber interface.
  - For passive negotiation, use the **initiate-ncp dual-stack-passive** statement, which overrides the **initiate-ncp ip** and **initiate-ncp ipv6** statements if they are configured.

  [See PPP Network Control Protocol Negotiation Mode Overview.]

- **Global configuration for LAC interoperation using Cisco NAS Port Info AVP (MX Series)**—Starting in Junos OS Release 14.1, you can globally configure LAC interoperation with a Cisco Systems LNS by specifying the LAC's NAS port method as **cisco-avp** with the **nas-port** statement at the **[edit services l2tp tunnel]** hierarchy level. This causes the LAC to include the Cisco NAS Port Info AVP (100) in the ICRQ messages it sends to the LNS for all tunnels.

  In earlier releases, you can configure interoperation only in a tunnel profile, so that it applies only to tunnels instantiated with that profile. The tunnel profile configuration now has precedence over the global configuration. You can override both by including the Tunnel-Nas-Port-Method VSA [26–30] in a RADIUS server configuration that modifies or creates a tunnel profile.

  [See Globally Configuring the LAC to Interoperate with Cisco LNS Devices.]

- **Enhanced support for firewall filter match conditions based on IEEE 802.1p VLAN priority bits (M320 and MX Series)**—Starting in Junos OS Release 14.1, the M320 router supports firewall filter match conditions based on IEEE 802.1p VLAN priority bits. The M320 router also supports these match conditions with the presence of a control word in a VPLS instance. Also starting with Junos OS Release 14.1, MX Series routers support firewall filter match conditions based on IEEE 802.1p VLAN priority bits in both a VPLS instance and a Layer 2 VPN instance.

  [See Firewall Filter Match Conditions for VPLS Traffic and Firewall Filter Match Conditions for Layer 2 CCC Traffic.]

MPLS

- **LSP selection for default forwarding class using CBF (M Series, MX Series, and T Series)**—When CoS-based forwarding (CBF) is configured on a VPLS PE router, VPLS BUM traffic (broadcast, unknown, and multicast traffic) uses the default forwarding class for label-switched path (LSP) selection. Starting in Junos OS Release 14.1, the LSP for the default forwarding class is configurable, enabling the association of VPLS BUM traffic with an LSP through CBF configuration.

  [See Load Balancing VPLS Non-Unicast Traffic Across Member Links of an Aggregate Interface.]

- **Support for load balancing VPLS non-unicast traffic across member links of an aggregate interface (M Series, MX Series, and T Series)**—By default, VPLS non-unicast (or BUM — broadcast, unknown, and multicast) traffic sent across aggregate Ethernet interfaces is sent across only one member link of the aggregate interface. Starting in Junos OS Release 14.1, load balancing VPLS BUM traffic across all members of an aggregate interface can be enabled for each VPLS instance.

  [See Load Balancing VPLS Non-Unicast Traffic Across Member Links of an Aggregate Interface.]

- **Entropy label and FAT label support (MX Series and T Series)**—Starting in Release 14.1, the Junos OS supports entropy labels and Flow Aware Transport for Psuedowires (FAT) labels. Entropy label and FAT label when configured on the label-switching routers (LSRs) and label edge routers (LEs) perform load-balancing of MPLS packets across equal-cost multipath (ECMP) paths or link aggregation groups (LAG) without the need for deep packet inspection of the payload.

  In Junos OS Release 14.1, entropy labels can be used for RSVP-signaled label-switched paths (LSPs) and point-to-point LDP-signaled LSPs. FAT flow labels can be used for LDP-signaled forwarding equivalence class (FEC 128 and FEC 129) pseudowires for virtual private LAN service (VPLS) and virtual private wire service (VPWS) networks.

  [See Configuring the Entropy Label for LSPs and FAT Flow Labels Overview.]

Multicast

- **Multicast-only fast reroute (MoFRR) (MX Series)**—Starting in Junos OS Release 14.1, MoFRR functionality is available, in which packet loss is minimalized in PIM and multipoint LDP domains. This enhancement is available on the MX Series operating in enhanced IP mode and with MPC line cards. A new configuration statement, **stream-protection**, enables MoFRR. When establishing the primary and backup ECMPs, MoFRR attempts to select two separate upstream routers, if two such routers are available. If separate upstream routers are not available, but there are two links through the same upstream router, the protocol selects that router for both paths.

  

  NOTE: MoFRR might select the same upstream router to establish the primary and the backup paths, even when two separate upstream routers are available.

  [See Example: Configuring Multicast-Only Fast Reroute in a PIM Domain and Example: Configuring Multicast-Only Fast Reroute in a Multipoint LDP Domain.]

Network Management and Monitoring

- **Forwarding Class extension to Interface MIB (MX Series)**—Beginning with Junos OS Release 14.1, a new Enterprise-Specific Forwarding Class MIB, **jnxIfAccountingStats**, is available to monitor the statistics for various accounting parameters configured on the interface with the available forwarding classes. This is an extension to the *Enterprise-Specific Interface MIB*. The Forwarding Class MIB is currently supported only on the MX Series.

  [See Interpreting the Enterprise-Specific Interface Accounting Forwarding MIB.]

- **SNMP notifying target for removed notify target configuration (M Series, MX Series, and T Series)**—Beginning with Junos OS Release 14.1, when a trap target is deleted from Juniper Networks devices, either a syslog event or a syslog trap is generated as per the user configuration. The existing SNMP trap **jnxSyslogTrap** is sent to all target network management systems (NMSs) specified in the SNMP agent including the target NMS, which is being deleted. By default, in the event of target deletion, only a syslog event is generated. To trigger a trap on deletion of a trap target, configure a syslog event policy, which sends the syslog as a trap to the network management systems.

- **Alarm MIB support (MX Series)**—Beginning with Release 14.1, Junos OS supports RFC 3877, *Alarm MIB*, which provides the generic SNMP-based alarm management framework to address the problems occurring on a particular network resource. The **jnxAlarmMib** reports active alarms and the history of alarms through the SNMP MIB tables. A new daemon called alarm management daemon, **AlarmMgmtD**, reports notifications defined in the alarm model table. The Alarm MIB is currently supported only on the MX Series.

  To configure alarm management, include the **alarm-management** statement at the **[edit snmp]** hierarchy level.

[See Interpreting the Enterprise-Specific Alarm MIB.]

- **SNMP MIB support for Ethernet OAM (MX Series)**—Starting in Junos OS Release 14.1, SNMP MIB support is enabled for Ethernet OAM on MX Series routers. See *Standard SNMP MIBs Supported by Junos OS* to view the standard MIBs (in IEEE 802.1ag, Connectivity Fault Management and IEEE 802.1ap, Management Information Base (MIB) definitions for VLAN Bridges) that are supported for Ethernet OAM.
- **Subscriber accounting MIB support (M Series, MX Series, and T Series)**—Starting in Junos OS Release 14.1, a new enterprise-specific Subscriber MIB, jnxSubscriberAccountingTable, has been added to the jnxSubscriberGeneral MIB to monitor subscriber sessions that are configured for RADIUS accounting. The jnxSubscriberAccountingTable MIB is a subset of the jnxSubscriberTable MIB.
- **SNMP support to monitor subscriber count per port (M Series, MX Series, and T Series)**—Beginning with Junos OS Release 14.1, a new enterprise-specific Subscriber MIB, jnxSubscriberPortCountTable, has been added to the jnxSubscriberGeneral MIB to provide the number of active subscribers per port for tunneled and terminated subscribers.
- **Enhancement for viewing the details of user authentication (M Series, MX Series, and T Series)**—Starting with Junos OS Release 14.1, you can configure the following statements to view the attribute values of a logged in user:
  - **enhanced-accounting**—This configuration statement displays the details such as access privileges, access modes, and remote port of a user logged in through the RADIUS server or the TACAC+ server or local database. To enable this feature, use the **set system radius-options enhanced-accounting** command for the RADIUS server or the **set system tacplus-options enhanced-accounting** command for the TACAC+ server.
  - **enhanced-avs-max**—This configuration statement helps to limit the number of attribute values to be displayed when **enhanced-accounting** is enabled. To enable this feature, use the **set system accounting enhanced-avs-max** command.

Network Operations and Troubleshooting Automation

- **Upgrade to automation libraries (M Series, MX Series, and T Series)**—SLAX is an alternative syntax for XSLT which is tailored for readability and familiarity, following the style of C and Perl. SLAX was originally developed as part of Junos OS. It is used for on-box scripting to allow users to customize and enhance the CLI. The Junos OS automation infrastructure uses the libslax and libxslt open source libraries. Beginning in Junos OS Release 14.1, these libraries have been upgraded to libxslt-1.1.28 and libslax.0.14.1.
- **Script dampening (M Series, MX Series, and T Series)**—Beginning in Junos OS Release 14.1, the impact of processor-intensive scripts on the performance of the Routing Engine can be minimized by configuring Junos OS to dampen or slow down the execution of any commit, op, or event script. To slow down script execution, include the **dampen** statement at the **[edit event-options event-script]**, **[edit system scripts commit]**, or **[edit system scripts op]** hierarchy level.

  [See Dampening Script Execution.]

Port Security

- **Storm control support (MX240, MX480, and MX960)**—Starting in Junos OS Release 14.1, support exists for storm control that enables the router to monitor traffic levels and to drop broadcast, multicast, and unknown unicast packets when a specified traffic level – called the storm control level- is exceeded, thereby preventing packets from proliferating and degrading the LAN.

  You can modify the storm-control configuration by configuring a storm control profile at the **[edit forwarding-options]** hierarchy level, and then binding the storm control profile to a specific logical interface or to a group of logical interfaces. The group can include a range of interfaces or all interfaces on the switch.

- **Access port security (MX240, MX480, and MX960)**—Starting in Junos OS Release 14.1, Layer 2 software access port security is supported on the MX240, MX480, and MX960:

  - DAI– DAI protects switches against ARP spoofing. DAI inspects ARP packets on the LAN and uses the information in the DHCP snooping database on the switch to validate ARP packets and to protect against ARP cache poisoning.
  - DHCP option 82–You can use DHCP option 82, also known as the DHCP relay agent information option, to help protect the router against attacks such as spoofing (forging) of IP addresses and MAC addresses, and DHCP IP address starvation.
  - DHCP snooping—DHCP snooping filters and blocks ingress DHCP server messages on untrusted ports, and builds and maintains an IP address to MAC address binding database. Most port security features depend on DHCP snooping.
  - IP source guard–You can use the IP source guard access port security feature to mitigate the effects of source IP address spoofing and source MAC address spoofing.
  - Static IP–You can add static (fixed) IP addresses and bind them to fixed MAC addresses in the DHCP snooping database.
  - Trusted DHCP server interface–You can configure any interface on a switch that connects to a DHCP server as a trusted interface (port). Configuring a DHCP server on a trusted interface protects against rogue DHCP servers sending leases.

Routing Policy and Firewall Filters

- **Firewall filter match condition support for IPv6 extension headers (MX Series with MPCs)**—Starting in Junos OS Release 14.1, IPv6 firewall filters support extension header types as match conditions. This feature enables you to control the transmission of IPv6 packets based on the presence of specified extension header types in the packet. In the first fragment of a packet, the filter searches for a match in any of the extension header types. When a packet with a fragment header is found (a subsequent fragment), the filter only searches for a match of the next extension header type.

  [See Standard Firewall Filter Match Conditions for IPv6 Traffic.]

- **Firewall filter match condition support for additional ICMPv6 types (MX Series with MPCs)**—Starting in Junos OS Release 14.1, IPv6 firewall filters support several additional

ICMPv6 match conditions. This feature enables you to specify match conditions for the following ICMP message types:

- certificate-path-advertisement (149)
- certificate-path-solicitation (148)
- home-agent-address-discovery-reply (145)
- home-agent-address-discovery-request (144)
- inverse-neighbor-discovery-advertisement (142)
- inverse-neighbor-discovery-solicitation (141)
- mobile-prefix-advertisement-reply (147)
- mobile-prefix-solicitation (146)
- private-experimentation-100 (100)
- private-experimentation-101 (101)
- private-experimentation-200 (200)
- private-experimentation-201 (201)

[See Standard Firewall Filter Match Conditions for IPv6 Traffic.]

Routing Protocols

- **Nonstop active routing for BGP multicast VPNs (M Series, MX Series, and T Series)** — Starting in Junos OS Release 14.1, this feature enables nonstop active routing for the BGP multicast VPNs (MVPNs). This feature synchronizes the MVPN routes, cmcast, provider-tunnel and forwarding information between the master and the backup Routing Engines.

  [See advertise-from-main-vpn-tables.]

- **Advertising multiple paths in BGP (MX Series and T Series)** — Starting in Junos OS Release 14.1, this feature allows up to 20 BGP add-paths to be advertised for a subset of prefixes that match the **add-path prefix-policy**.

  To enable this feature for a prefix, the **add-path prefix-policy** term matching the prefix should have a new **then** action to set **add-path send-count*<2...20>***. This new action is a not applicable if the policy-statement containing it is used anywhere other than **add-path prefix-policy**.

  [See Actions in Routing Policy Terms, path-count, and prefix-policy.]

- **Egress protection for BGP labeled unicast (M Series, MX Series, and T Series)**—Starting in Junos OS Release 14.1, fast protection for egress nodes is available to services in which BGP labeled unicast interconnects IGP areas, levels, or autonomous systems (ASs). If a provider router detects that an egress router (AS or area border router) is down, it immediately forwards the traffic destined to that router to a protector router that forwards the traffic downstream to the destination.

[See Egress Protection for BGP Labeled Unicast.]

- **Selecting backup LFA for IS-IS routing protocol (M Series, MX Series, and T Series)**—Starting with Junos OS Release 14.1, the default loop-free alternate (LFA) selection algorithm or criteria can be overridden with an LFA policy. These policies are configured for each destination (IPv4 and IPv6) and a primary next-hop interface. These backup policies enforce LFA selection based on admin-group, srlg, neighbor, neighbor-tag, bandwidth, protection-type, and metric attributes of the backup path. During backup shortest-path-first (SPF) computation, each attribute (both node and link) of the backup path, stored per backup-next hop, is accumulated by IGP. For the routes created internally by IGP, the attribute set of every backup path is evaluated against the policy configured per destination per prefix primary next-hop interface. The first or the best backup path is selected and installed as the backup next-hop in the routing table. To configure the backup selection policy, include the **backup-selection** configuration statement at the **[edit routing-options]** hierarchy level. The **show backup-selection** command displays the configured policies for a given interface and destination. The display can be filtered against a particular destination, prefix, interface, or logical systems.

  [See Example: Configuring Backup Selection Policy for IS-IS Protocol.]

Services Applications

- **Support for inline video monitoring (MX Series routers with MPCs)**—Starting in Junos OS Release 14.1, video monitoring using media delivery indexing (MDI) criteria is supported. MDI information enables you to identify devices that are causing excessive jitter or packet loss for streaming video applications. To configure inline video monitoring criteria, include the **templates** and **interfaces** statements at the **[edit services video-monitoring]** hierarchy level.

  Inline video monitoring is available for the following MPC interface cards:

  - MPCE1
  - MPCE2
  - MPC-16XGE

  [See *Inline Video Monitoring Feature Guide*.]

- **Enhancements to IPsec packet fragmentation (MX Series routers with MS-MICs and MS-MPCs)**—In packets that are transmitted through static and dynamic endpoint IPsec tunnels, you can enable the value set in the Don't Fragment (DF) bit of the packet entering the tunnel to be copied only to the outer header of the IPsec packet and to not cause any modification to the DF bit in the inner header of the IPsec packet. To copy the DF bit value to only the outer header and not modify the inner header, use the **copy-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level for static tunnels and at the **[edit services service-set *service-set-name* ipsec-vpn-options]** hierarchy level for dynamic endpoints. To configure the DF bit in only the outer header of the IPsec packet and to leave the inner header unmodified, include the **set-dont-fragment-bit** statement at the **[edit services ipsec-vpn rule *rule-name* term *term-name* then]** hierarchy level for static tunnels and at the **[edit**

services service-set *service-set-name* ipsec-vpn-options] hierarchy level for dynamic endpoints.

[See copy-dont-fragment-bit (Services IPsec VPN) , set-dont-fragment-bit (Services IPsec VPN), copy-dont-fragment-bit (Services Set), and set-dont-fragment-bit (Services Set).]

- **Support for configuring template ID, observation domain ID, and source ID for Version 9 and IPFIX flow templates**—Starting with Junos OS Release 14.1, you can define the template ID for version 9 and IPFIX templates for inline flow monitoring. To specify the template ID for version 9 flows, include the **template-id *id*** statement at the **[edit services flow-monitoring version9 template *template-name*]** hierarchy level. To specify the template ID for version IPFIX flows, include the **template-id** statement at the **[edit services flow-monitoring version-ipfix template *template-name*]** hierarchy level. To specify the options template ID for version 9 flows, include the **options-template-id** statement at the **[edit services flow-monitoring version9 template *template-name*]** hierarchy level. To specify the options template ID for version IPFIX flows, include the **options-template-id** statement at the **[edit services flow-monitoring version-ipfix template *template-name*]** hierarchy level. The template ID and options template ID can be a value in the range of 1024 through 65535.

  Until Junos OS Release 13.3, the observation domain ID is predefined and is set to a fixed value, which is derived from the combination of FPC slot, sampling protocol, PFE Instance and LU Instance fields. This derivation creates a unique observation domain per LU per family. Starting with Junos OS Release 14.1, you can configure the observation domain ID, which causes the first 8 bits of the field to be configured. For version 9 flows, a 32-bit value that identifies the Exporter Observation Domain is called the source ID.

  [See Configuring Observation Domain ID and Source ID for Version 9 and IPFIX Flows and Configuring Template ID and Options Template ID for Version 9 and IPFIX Flows.]

- **Increased number of IPsec tunnels (MX80, MX240, MX480, and MX960)**—Starting with Junos OS Release 14.1, you can configure a maximum of up to 8000 IPsec tunnels using 6000 service sets on a router. In such a scenario, you can employ up to 8000 logical interfaces in your environment and configure IPv4, IPv6, and dead peer detection (DPD) protocols. Until Junos OS Release 13.3, the maximum number of IPsec tunnels supported with 6000 service sets was 6000 tunnels.

Software Installation and Upgrade

- **Unified ISSU support for LFM (M Series and MX Series)**—Starting in Junos OS Release 14.1, the LFM protocol supports unified ISSU on the M Series and MX Series with some restrictions. Connectivity failures that occur during the unified ISSU period are not detected until after unified ISSU has completed. If unified ISSU is initiated while discovery is in progress, the discovery completes only after unified ISSU has finished. LFM features that require Routing Engine involvement do not work during the unified ISSU period. Unified ISSU cannot run on the local and remote ends at the same time.

- **Unified in-service software upgrade support (MX104)**—Starting with Junos OS Release 14.1, unified in-service software upgrade (unified ISSU) is supported on MX104 3D Universal Edge Routers.

Unified ISSU is supported on the following MICs on MX104 routers:

- Gigabit Ethernet MIC with SFP (MIC-3D-20GE-SFP)
- Gigabit Ethernet MIC with SFP (E) (MIC-3D-20GE-SFP-E)
- Gigabit Ethernet MIC with SFP (EH) (MIC-3D-20GE-SFP-EH)
- 10-Gigabit Ethernet MICs with XFP (MIC-3D-2XGE-XFP)
- Tri-Rate Copper Ethernet MIC (MIC-3D-40GE-TX)

When unified ISSU is not supported on a MIC, at the beginning of the upgrade, Junos OS issues a warning that the MIC will be taken offline. After the MIC is taken offline and unified ISSU is complete, the MIC is brought back online.

Unified ISSU is not supported on the following MICs on MX104 routers:

- ATM MIC with SFP (MIC-3D-8OC3-2OC12-ATM)
- Channelized E1/T1 Circuit Emulation MIC (MIC-3D-16CHE1-T1-CE)
- Channelized E1/T1 Circuit Emulation MIC (H) (MIC-3D-16CHE1-T1-CE-H)
- Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP (MIC-3D-4COC3-1COC12-CE)
- Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP (H) (MIC-4COC3-1COC12-CE-H)
- Channelized SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP (MIC-3D-4CHOC3-2CHOC12)
- Channelized SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP (MIC-3D-8CHOC3-4CHOC12)
- DS3/E3 MIC (MIC-3D-8DS3-E3)
- SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP (MIC-3D-4OC3OC12-1OC48)
- SONET/SDH OC3/STM1 (Multi-Rate) MICs with SFP (MIC-3D-8OC3OC12-4OC48)
- SONET/SDH OC192/STM64 MIC with XFP (MIC-3D-1OC192-XFP)

During unified ISSU, the protocols and applications that are not supported on MX104 routers are the same as those that are not supported on other MX Series routers undergoing unified ISSU.

[See Unified ISSU System Requirements.]

- **Support for LACP with fast hellos during unified ISSU (MX Series)**—Starting in Junos OS Release 14.1, MX Series routers support LACP with fast hellos during unified ISSU. This support is disabled by default. To enable it you need to enter the new CLI knob **set protocols lacp fast-hello-issu** on both the DUT and peer routers before starting unified ISSU. The peer router must also be an MX Series router for this functionality to work.
- **Unified ISSU support on L2TP LNS (M Series, MX Series, and T Series)**—Junos OS Release 14.1 and later releases support unified ISSU on the L2TP network server (LNS).

When an upgrade is initiated, the LNS completes any L2TP negotiations that are in progress but rejects any new negotiations until the upgrade has completed. No new tunnels or sessions are established during the upgrade.

[See L2TP for Subscriber Access Overview.]

- **Unified ISSU support (TX Matrix Plus router with 3D SIBs)**—Starting in Junos OS Release 14.1, unified ISSU is supported on TX Matrix Plus routers with 3D SIBs. Unified ISSU enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic.

  [See Unified ISSU System Requirements.]

Spanning-Tree Protocols

- **Enhancements to STP logs (MX Series)** — Beginning with Release 14.1R1, Junos OS supports:
  - Logging of information in the internal ring buffer about events like Spanning Tree (such as STP, MSTP, RSTP, or VSTP) interface role or state change without having to configure STP traceoptions.
  - Capturing information as to what triggered the spanning-tree role or state change.

  You can use the operational mode commands show spanning-tree statistics message-queues, show spanning-tree stp-buffer see-all, show spanning-tree statistics bridge, and show spanning-tree statistics interface to get the information from ring-buffer, bridge, and port statistics. clear spanning-tree stp-buffer clears the stp-buffer, and clear spanning-tree statistics bridge clears the statistics of the bridge.

  NOTE: **show spanning-tree statistics interface** is not supported in Release 14.1R1.

Subscriber Management and Services

NOTE: Although present in the code, the subscriber management features are not supported in Junos OS Release 14.1R1. Documentation for subscriber management features is included in the Junos OS Release 14.1 documentation set.

- **RADIUS VSAs in output of test aaa command when authentication is unsuccessful (MX Series)**—Starting in Junos OS Releases 13.2R3 and 14.1R1, when you run the **test aaa** command, the command output includes all subscriber attributes when authentication is unsuccessful. In previous releases, the **test aaa** command returned a partial list of attributes when authentication was unsuccessful.

  [See Testing a Subscriber AAA Configuration.]

- **Using DHCP relay agent optional information to enhance security (MX Series)**—Starting in Junos OS Release 14.1, you can provide additional security by

configuring DHCP relay agent to include optional information in client requests that the relay forwards to the DHCP server. The optional information helps minimize potential security shortcomings that might exist when a DHCP server on a central LAN allows connections from central access devices.

For DHCPv4, DHCP relay agent inserts Relay Agent Information Option (option 82) Agent Remote ID (suboption 2) into the relayed client requests. For DHCPv6, DHCPv6 relay agent inserts Relay Agent Remote-ID (option 37) into the relayed (RELAY-FORW) DHCPv6 messages.

[See Using DHCP Relay Agent Option 82 Information and DHCPv6 Relay Agent Options.]

- **Support for Agent-Remote-Id when testing subscriber authentication (MX Series)**—Starting in Junos OS Release 14.1, you can use the **agent-remote-id *ari*** option with the **test aaa dhcp user** and **test aaa ppp user** commands to verify DHCP and PPP subscriber authentication in those networks that use the DSL Forum Agent-Remote-Id (VSA 26-2). If the ARI value that you specify includes special characters, such as a phone number that includes parentheses and a hyphen, you must enclose the value in quotation marks (“”), as in the following example:

  test aaa ppp user agent-remote-id “(202)555–1212”

  [See Testing a Subscriber AAA Configuration.]

- **RADIUS-based usage thresholds for subscriber services (MX Series)**—Starting in Junos OS Release 14.1, you can set usage thresholds for subscriber services that are dynamically activated or modified.

  Subscriber management supports two types of usage thresholds—traffic volume and time. You use Juniper Networks VSAs to set the usage thresholds. The VSAs are transmitted in RADIUS Access-Accept messages for dynamically activated services, or in RADIUS-initiated CoA-Request messages for existing services. The traffic volume threshold sets the maximum amount of traffic that can use the service before the service is deactivated. The time threshold sets the maximum length of time that the service can be active.

  [See Usage Thresholds for Subscriber Services.]

- **Overriding short DHCP leases offered by third-party DHCP servers (MX Series)**—Starting in Junos OS Release 14.1, you can specify the minimum DHCP lease time allowed by the DHCP local server or DHCP relay agent. This feature enables you to avoid potential issues when a third party owns or manages the DHCP server or address-assignment pool that provides the client lease. In some cases, the third party might provide address leases that are unsuitable for the subscriber access environment. For example, extremely short lease times can create unnecessary traffic that results in reduced performance in the network.

  In addition to specifying a minimum lease time, you can also specify the action the router takes when receiving a DHCP lease time that is less than the minimum acceptable value.

  [See DHCP Lease Time Violation.]

- **Support for L2TP AVPs that report access line information to the LNS (MX Series)**—Starting in Junos OS Release 14.1, you can configure the LAC to include L2TP

AVPs in ICRQ messages to convey attributes such as line identification and traffic rates. The LAC receives the information from the DSLAM (ANCP access node) associated with the subscriber line; the values can be sourced from the ANCP agent or PPPoE intermediate agent tags carried in PADI and PADR discovery packets. You can also configure the LAC to send Connect-Speed-Update-Notification messages to the LNS to report updates to the subscriber connection speeds compared to the initial values conveyed by L2TP AVP 24 and AVP 38.

[See Forwarding of Subscriber Access Line Information by the LAC and Configuring the LAC to Report Access Line Information to the LNS.]

- **Support for RADIUS accounting message retry and timeout (MX Series)**—Starting in Junos OS Release 14.1, include the new **accounting-message-retry** and **accounting-message-timeout** statements to specify retry and timeout values for RADIUS accounting messages separately from authentication messages. When you do so, the existing **retry** and **timeout** statements apply only to authentication messages; otherwise, they also apply to accounting messages.

  Separate settings are useful for the following reasons:

  - Authentication is time critical. Consequently, dropped packets need to be retransmitted quickly and short timeouts are desirable. Fewer retransmissions are sufficient because an unsuccessful subscriber is likely to attempt another login quickly.
  - Accounting is less time critical, but it is important not to lose the accounting messages. Long timeouts and more retransmissions reduce packet loss.

    [See accounting-retry and accounting-timeout.]

- **Conserving IPv4 addresses for dual-stack PPP subscribers (MX Series routers with MPCs or MICs)**—Beginning in Junos OS Release 14.1, the IPv4 address saving feature for dual-stack PPP subscribers when they are not using the IPv4 service is expanded. During IPv4 address negotiation, if the broadband network gateway (BNG) receives an Access-Reject response from the RADIUS server that includes the Unisphere-Ipv4-release-control VSA and Reply Message attribute #18, the BNG sends an IPCP terminate request to the CPE. The CPE is then allowed to renegotiate IP NCP. However, if Unisphere-Ipv4-release-control VSA and Reply Message attribute #18 are not included in the Access-Reject response, the CPE must renegotiate the LCP link before being allowed to renegotiate IP NCP.

- **Dynamic Domain Name System (DNS) Resolver for IPv6 (MX Series)**—Beginning in Junos OS Release 14.1, in a network that uses Neighbor Discovery Router Advertisement (NDRA) to provide IPv6 addressing, the DNS server address can be provided in Router Advertisements sent to IPv6 hosts. The address is included in a field called Recursive DNS Server (RDNSS). This feature is useful in networks that are not running DHCPv6.

  To configure (the default lifetime is 1800 seconds):

  ```
  [edit dynamic-profiles profile-name protocols router-advertisement interface
    $junos-interface-name]
  user@host# set dns-server-address $junos-ipv6-dns-server-address lifetime
    #-of-seconds
  ```

  [See DNS Resolver for IPv6 DNS Overview.]

- **Subscriber interfaces over point-to-point MPLS pseudowires (MX Series routers with MPCs or MICs)**—Beginning in Junos OS Release 14.1, pseudowire subscriber interfaces support the following features:
  - Access Node Control Protocol (ANCP), which is used to monitor subscriber access lines and to report and modify subscriber traffic on the access lines between the subscribers and the access nodes.
  - Agent circuit identifier (ACI) interface sets, which are dynamic VLAN subscriber interfaces that are created based on ACI information and that originate at the same household or on the same access-loop port.
  - CoS shaping-rate and overhead-accounting attributes for dynamic ACI interface sets.
- **Minimum retransmission interval for L2TP control packets (MX Series)**—Starting in Junos OS Release 14.1, you can give a remote L2TP peer more or less time to respond to a control message sent by the local peer by including the **minimum-retransmission-interval** statement to configure the minimum interval that the local peer waits for a response. You can configure a minimum value of 1, 2, 4, 8, or 16 seconds; previously, the minimum interval was fixed at 1 second. The peer retransmits the message if a response is not received before the timeout expires, but waits for double the previous interval. The interval doubles with each retransmission until the maximum of 16 seconds is reached.

  [See Retransmission of L2TP Control Messages.]
- **Support for dynamic VLAN authentication based on subscriber packet type (MX Series)**—Starting in Junos OS Release 14.1, you can limit the packet types that trigger RADIUS authentication for dynamic, auto-sensed VLANs. In earlier releases, authentication is triggered by packet types configured with the **accept** statement in VLAN dynamic profiles.

  Now you can specify that a subset of accepted packet types triggers authentication by including the **packet-types** statement at the **[edit interfaces *interface-name* auto-configure vlan-ranges authentication]** or **[edit interfaces *interface-name* auto-configure stacked-vlan-ranges authentication]** hierarchy level.

  Because PPPoE subscribers are authenticated by PPP, you can conserve resources in a mixed PPPoE and IP environment by limiting VLAN authentication to the IP packets. You can also use this statement with the Client-Profile-Name VSA [26-174] to override a dynamic profile for certain subscriber types in a mixed access environment.
- **Clear DS-Lite mappings and flows (MX Series Routers with MS-DPC interface cards)—** In Junos OS Release 14.1 and later releases, you can clear DS-Lite mapping statistics and flows for a specific subscriber, Basic Bridging Broadband Device (B4), or host behind a B4 using the following new operational commands.
  - **clear services nat mappings app**—Clear address-pooling paired mappings.
  - **clear services nat mappings eim**—Clear endpoint independent mappings.
  - **clear services nat mappings pcp**—Clear port control protocol (PCP) mappings.

- **clear services nat mappings service-set**—Clear all NAT mappings for a service-set.
- **clear services nat flows**—Clear all NAT flows. This command has the following scope options:
  - **b4address**—Clear all flows for a subsciber B4 address.
  - **service-set**—Clear all flows for a service set.
  - **subscriber**—The subscriber address.

- **Support for ATM virtual path shaping on ATM MICs with SFP (MX Series)**—Starting in Junos OS Release 14.1, class-of-service (CoS) hierarchical shaping for ATM virtual paths (VPs) is supported on MIC-3D-8OC3-2OC12-ATM.

  The following configuration requirements apply to ATM VP shaping:

  - All ATM interfaces that are members of an interface set must share the same virtual path identifier (VPI) and have a unique virtual circuit identifier (VCI).
  - The ATM interface set can include only ATM interfaces. It cannot include Ethernet interfaces.
  - The ATM interface set cannot include PPPoE over ATM interfaces, but it can include the underlying ATM interface over which PPPoE over ATM is carried.

  To configure an ATM interface set and its members, use the **interface-set** stanza at the **[edit interfaces]** or **[edit dynamic-profiles *profile-name* interfaces]** hierarchy level, specifying the ATM physical interface (**at-*slot/mic/port***) and logical unit numbers.

  After you configure the ATM interface set, you must create a CoS traffic control profile that includes the **peak-rate** (peak cell rate, or PCR), **sustained-rate** (sustained cell rate, or SCR), and **max-burst-size** (maximum burst size, or MBS) statements to shape the ATM cells transmitted on the ATM MIC. You then associate the traffic control profile to the ATM interface set.

- **Modifications to output fields of test aaa command (MX Series)**—Starting in Junos OS Release 14.1. the output of the **test aaa [dhcp | ppp] user** command is modified to improve readability. The modifications include the following:
  - The output now includes the corresponding tag for service-related attributes. For example, the following output includes the tag number (1) for the filter-service.

    Service Name (1) - filter-service(100,200)
  - The output now includes the service activation type. For example:

    Service Activation Type (1) - 1
  - The **junos-adf-rule-v4** output field is now titled **IPv4 ADF Rule**.
  - The **junos-adf-rule-v6** output field is now titled **IPv6 ADF Rule**.

- **DHCPv6 local server and relay agent username and option 37 (MX Series)**—Starting in Junos OS Releases 12.3R7, 13.2R4, 13.3R2, and 14.1R1, the router supports the generation of an ASCII version of the authentication username. When you configure a DHCPv6 local server or relay agent to concatenate the authentication username with

the Agent Remote-ID option 37, the router uses only the remote-id portion of option 37 and ignores the enterprise number.

The router no longer supports the **enterprise-id** and **remote-id** options for the **relay-agent–remote-id** statement.

- **Realm name parsing (MX Series)**—Starting in Junos OS Release 14.1, the router supports realm name delimiters and parsing, when determining domain names that are used for the domain mapping feature. The realm name support is similar to the existing domain name support, and is used when subscriber usernames are presented in the realm name format (such as, **abc.com\marilyn**) rather than in the typical domain name format (such as, **joseph@abc.com**). You use the **parse-order** statement to specify the order in which the router searches for the domain name—you can specify that the router searches first for either the domain name or the realm name in the subscriber username. You can also specify the unique character that is the realm name delimiter, and the parsing direction the router uses to identify the resulting domain name that is used for domain mapping operations.

- **Specifying a domain map for usernames without a domain or realm name (MX Series)**—Starting in Junos OS Release 14.1, you can specify a domain map name of **none** for the **map** ***domain-map-name*** statement at the **[edit access domain]** hierarchy level. The router uses the domain map named **none** to perform domain map operations for subscriber usernames that do not include a domain or realm name.

- **MLPPP support for LNS and PPPoE subscribers (MX Series)**—Starting in Junos OS Release 13.3, Multilink PPP (MLPPP) support is provided for static and dynamic LNS (L2TP network server) and PPPoE (Point-to-Point Protocol over Ethernet) terminated and tunneled subscribers running on the MX Series with access-facing MPC2 slots. The following features are supported:

  - Mixed mode for customers with both MLPPP and single link PPP subscribers
  - Fragmentation-maps for both static and dynamic inline service **si** interfaces
  - Co-existence support for member link IFL and the bundle IFL on different lookup engines
  - Link fragmentation and interleaving (LFI) for a single-link bundle
  - Minimization of fragment reordering

- **Subscriber management and services feature and scaling parity (MX104)**—Starting in Junos OS Release 14.1, the MX104 router supports all subscriber management and services features that are supported by the MX80 router. In addition, the scaling and performance values for the MX104 router match those of the MX80 router.

  [See Protocols and Applications Supported by MX5, MX10, MX40, and MX80 Routers.]

User Interface and Configuration

- **New commit check for static label uniqeness**—Previously, applications, such as MPLS LSPs and Layer 2 circuits that use static labels, did not check to ensure that an incoming label name was not being used by another application. This causes the routing protocol process (RPD) to generate a core file. Starting in Junos OS Release 14.1, a commit check has been implemented to ensure the uniqueness of static labels across applications.

VLAN Infrastructure

- **VXLAN gateway support (MX80, MX240, MX480, MX960, MX2010, and MX2020)—Starting in Junos OS Release 14.1, the MX80, MX240, MX480, MX960, MX2010, and MX2020 support Virtual Extensible Local Area Network (VXLAN) Gateways. Each VXLAN Gateway supports the following functionalities:**
  - 32,000 VXLANs with one VXLAN per bridge domain
  - 8,000 VXLAN Tunnel End Points (VTEPs)
  - 32,000 multicast groups
  - Switching functionality with traditional L2 networks and VPLS networks
  - Inter VXLAN routing and VXLAN-only bridging domain with IRB
  - Virtual switches
  - VXLAN with VRF functionality
  - Configurable load balancing
  - Statistics for remote VTEP

VPNs

- **Control word for BGP VPLS (M320 and MX Series)**—For hash calculation, transit routers must determine the payload. While parsing an MPLS encapsulated packet for hashing, a transit router can incorrectly calculate an Ethernet payload as an IPv4 or IPv6 payload if the first nibble of the DA MAC is 0x4 or 0x6, respectively. This false positive can cause out-of-order packet delivery over a pseudowire. Starting in Junos OS Release 14.1, this issue can be avoided by configuring a BGP VPLS PE router to request that other BGP VPLS PE routers insert a control word between the label stack and the MPLS payload.

  [See Control Word for BGP VPLS Overview.]

- **Group VPN member support (MX240, MX480, and MX960)**—Starting with Junos OS Release 14.1, the MX Series 3D Universal Edge Routers with MS-MPC-PIC and MS-MIC-16G line cards provide the group VPN member functionality support with one or more Cisco group controller or key servers (GC/KS). The group members can connect to a maximum of four Cisco GC/KSs with minimum interoperability with the cooperative servers.

  This feature also provides system logging support for the group VPN functionality and routing instance support for both control and data traffic.

[See Example: Configuring Group VPN on Routing Devices.]

- **IRB interface on EVPNs (MX Series routers with MPCs and MICs only)**—In an Ethernet VPN (EVPN) solution, multiple bridge domains can be defined within a particular EVPN instance, and one or more EVPN instances can be associated with a single Layer 3 VPN VRF. In general, each data center tenant is assigned a unique Layer 3 VPN VRF, although the tenant can be comprised of one or more EVPN instances or bridge domains per EVPN instance.

  To support this flexibility and scalability factor, beginning with Junos OS Release 14.1, the EVPN solution provides support for the integrated routing and bridging (IRB) interface on MX Series routers containing MPC interfaces to facilitate optimal Layer 2 and Layer 3 forwarding along with virtual machine mobility. The IRB interfaces are configured on each configured bridge domain including the default bridge domain for an EVPN instance.

  [See Example: Configuring EVPN with IRB Solution.]

- **Virtual switch support for EVPNs (MX Series routers with MPCs and MICs only)**—Starting with Junos OS Release 14.1, the Ethernet VPN (EVPN) solution on MX Series routers with MPC interfaces is extended to provide virtual switch support that enables multiple tenants with independent VLAN and subnet space within an EVPN instance. Virtual switch provides the ability to extend Ethernet VLANs over a WAN using a single EVPN instance while maintaining data-plane separation between the various VLANs associated with that instance. A single EVPN instance can stretch up to 4094 bridge domains defined in a virtual switch to remote sites.

  [See Example: Configuring EVPN with Support for Virtual Switch.]

- **Multihoming support for EVPNs (MX Series routers with MPCs and MICs only)**—Starting with Junos OS Release 14.1, the Ethernet VPN (EVPN) solution on MX Series routers with MPC interfaces is extended to provide multihoming functionality in the active-standby redundancy mode of operation.

  To enable EVPN active-standby multihoming, include the **single-active** statement at the **[edit interfaces esi]** hierarchy level.

  [See Example: Configuring EVPN Multihoming.]

Related Documentation

- Changes in Behavior and Syntax on page 36
- Known Behavior on page 44
- Known Issues on page 44
- Documentation Updates on page 51
- Migration, Upgrade, and Downgrade Instructions on page 53
- Product Compatibility on page 63

Changes in Behavior and Syntax

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 14.1R1 for the M Series, MX Series, and T Series.

Application Layer Gateways (ALGs)

- **Handling noncompliant IPv6 address in RTSP ALG (MX Series)**—Starting in Junos OS Release 14.1, Real-Time Streaming Protocol (RTSP) application-level gateway (ALG) cannot convert a noncompliant IPv6 address in its payload to an IPv4 address. The packet is not dropped, but it is forwarded to the receiving end of RTSP, which decides further processing of the packet.

Changes to MPLS Protection Options

- In Junos OS releases prior to 14.1, you can configure both fast reroute and node and link protection on the same LSP. In Junos OS Releases 14.1, you can still configure both fast reroute and node and link protection on the same LSP; however, when you attempt to commit a configuration where both features are enabled, a syslog warning message is displayed that states: **The ability to configure both fast-reroute and link/node-link protection on the same LSP is deprecated and will be removed in a future release.**

Class of Service (CoS)

- Beginning with Junos OS Release 14.1, a TWAMP connection/session will come up only if the session padding length is greater than or equal to 27 bytes on the TWAMP Client. The valid range of padding length supported by the TWAMP Server is 27 bytes to 1400 bytes.

  If IXIA is used as the TWAMP Client, packet length range from 41 bytes to 1024 bytes is supported.

- In Junos OS Releases 13.2R4, 13.3R2, and 14.1 and later, the interpolated fill level of 0 percent has a drop probability of 0 percent for weighted random early detection (WRED). In earlier Junos OS releases, interpolated WRED can have a nonzero drop probability for a fill level of 0 percent, which can cause packets to be dropped even when the queue is not congested or the port is not oversubscribed.

EVPN Interface Status Commit Check

- Starting in Junos OS Release 14.1, there is a commit check enforced for disabled interfaces in EVPN type routing instances and for bridge domains that have EVPN configured.

  Prior to Junos OS Release 14.1, there was a warning displayed when using the **show routing-instance** or **show routing-instance** *instance-name* configuration command at the **[edit]** hierarchy level, which stated: **interface not defined**, but later commits did still succeed.

High Availability (HA) and Resiliency

- **Unified ISSU support for ATM MIC with SFP (MX Series)**—Starting in Junos OS Release 14.1, the ATM MIC with SFP (MIC-3D-8OC3-2OC12-ATM) supports unified ISSU with the following guidelines:
  - The PPP keepalive interval must be 10 seconds or greater. PPP requires three keepalives to fail before it brings down the session. Thirty seconds (10 seconds x 3) provides a safe margin to maintain PPP sessions across the unified ISSU in case of any traffic loss during the operation. Configure the interval with the **keepalives** statement at the **[edit interfaces at-*interface-name*]** or **[edit interfaces at-*interface-name* unit *logical-unit-number*]** hierarchy level.
  - The OAM F5 loopback cell period must be 20 seconds or greater to maintain ATM connectivity across the unified ISSU. Configure the interval with the *oam-period* statement at the **[edit interfaces at-*interface-name* unit *logical-unit-number*]** hierarchy level.

Interfaces and Chassis

- **Display revision number of Routing Engines (M Series, MX Series, and T Series)**—Beginning with Junos OS Release 14.1, you can use the **show system commit revision** command to display the revision number of the Routing Engines in a dual Routing Engines-based router.

  A commit error message is issued when overlapping subnets are configured within a logical interface.

- **Changes to DDoS protection policers for PIM and PIMv6 (MX Series with MPCs, T4000 with FPC5)**—Starting in Junos OS Release 14.1, the default values for bandwidth

and burst limits have been reduced for PIM and PIMv6 aggregate policers to prevent starvation of OSPF and other protocols in the presence of high-rate PIM activity.

Policer Limit	New Value	Old Value
Bandwidth (pps)	8000	20,000
Burst (pps)	16,000	20,000

To see the default and modified values for DDoS protection packet-type policers, issue one of the following commands:

- **show ddos-protection protocols parameters brief**—Displays all packet-type policers.
- **show ddos-protection protocols *protocol-group* parameters brief**—Displays only packet-type policers with the specified protocol group.

An asterisk (*) indicates that a value has been modified from the default.

- **Changes to distributed denial of service statement and command syntax**—Starting in Junos OS Release 14.1, the protocol group and packet type syntax has changed for the **protocols** statement at the **[edit system ddos-protection]** hierarchy level and for the various **show ddos-protection protocols** commands.

  The **filter-v4** and **filter-v6** packet types have been moved from the **unclassified** protocol group to the new **filter-action** protocol group.

  The **resolve-v4** and **resolve-v6** packet types have been removed from the **unclassified** protocol group. They are replaced by the new **mcast-v4**, **mcast-v6**, **ucast-v4**, and **ucast-v6** packet types in the new **resolve** protocol group.

  Both protocol groups also include an **aggregate** option for all unclassified packets in the group and an **other** option for unclassified packets that are not IPv4 or IPv6.

  [See protocols (DDoS) and show ddos-protection protocols.]

- **Deleting PTP clock client (MX104)**—Starting with Junos OS Release 13.2, on MX104 routers, when you toggle from a secure slave to an automatic slave or vice versa in the configuration of a Precision Timing Protocol (PTP) boundary clock, you must first delete the existing PTP clock client or slave clock settings and then *commit* the configuration. You can delete the existing PTP clock client or slave clock settings by using the **delete clock-client *ip-address* local-ip-address *local-ip-address*** statement at the **[edit protocols ptp master interface *interface-name* unicast-mode]** hierarchy level. You can then add a new clock client configuration by using the **set clock-client *ip-address* local-ip-address *local-ip-address*** statement at the **[edit protocols ptp master interface *interface-name* unicast-mode]** hierarchy level and committing the configuration. However, if you attempt to delete the existing PTP clock client and add the new clock client before committing the configuration, the PTP slave clock remains in the free-run state and does not operate in the auto-select state (to select the best clock source). This behavior is expected when PTP client or slave settings are modified.

- **Disabling distribution of connectivity fault management sessions on aggregated Ethernet interfaces (MX Series)**—Starting with Junos OS Release 14.1, connectivity

fault management (CFM) sessions operate in distributed mode and are processed on the Flexible PIC Concentrator (FPC) on aggregated Ethernet interfaces by default. Starting with Junos OS Release 14.1, to disable the distribution of CFM sessions on aggregated Ethernet interfaces and to operate in centralized mode, include the **no-aggregate-delegate-processing** statement at the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level.

[See *IEEE 802.1ag OAM Connectivity Fault Management Overview*.]

- **Preventing the filtering of packets by ARP policers (MX Series with MPCs)**—Beginning with Junos OS Release 14.1, you can configure the router to disable the processing of the specified ARP policers on the received ARP packets. Disabling ARP policers can cause denial-of-service (DoS) attacks on the system. Due to this possibility, we recommend that you exercise caution while disabling ARP policers. To prevent the processing of ARP policers on the arriving ARP packets, include the **disable-arp-policer** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet policer]** or the **[edit logical-systems *logical-system-name* interfaces *interface-name* unit *logical-unit-number* family inet policer]** hierarchy level. You can configure this statement only for interfaces with inet address families and on MX Series routers with MPCs. When you disable ARP policers per interface, the packets are continued to be policed by the distributed DoS (DDoS) ARP policer. The maximum rate of is 10000 pps per FPC.

  [See *Network Interfaces, Protocol Family and Interface Address Properties*.]

- **Disabling the control word with active CFM sessions**—Starting in Junos OS Release 14.1, if you attempt to disable the control word by configuring the **no-control-word** statement at the **[edit routing-instances *routing-instance-name* protocols l2vpn]** or **[edit protocols l2circuit neighbor *neighbor-id* interface *interface-name*]** hierarchy level for all Layer 2 VPNs and Layer 2 circuits over which you are running CFM MEPs, the existing CFM sessions are dropped. To prevent this problem, you must first deactivate the Layer 2 circuit, disable the control word, and reactivate the Layer 2 circuit on both the MEPs of a CFM session.

  [See *Network Interfaces, Ethernet OAM*.]

Routing Policy and Firewall Filters

- **New firewall filter match condition supported on MPC line cards (MX Series)**—Starting in Release 13.3R2, Junos OS supports the **gre-key** firewall filter match condition on MPC line cards on MX Series 3D Universal Edge Routers. To configure the **gre-key** firewall filter match condition, include the **gre-key** statement at the **[edit firewall family inet filter *filter* term *term* from]** hierarchy level.

Routing Protocols

- **Modification to the default BGP extended community value (M Series, MX Series, and T Series)**—Starting in Junos OS Release 14.1, the default BGP extended community value used for MVPN IPv4 VRF route import (RT-import) has been modified to the IANA-standardized value. Thus, the default behavior has changed such that the behavior of the **mvpn-iana-rt-import** statement has become the default. The **mvpn-iana-rt-import** statement is deprecated and should be removed from configurations.

- **Removal of support for provider backbone bridging (MX Series)**—Starting with Junos OS Release 14.1, the provider backbone bridging (PBB) capability is disabled and not supported on MX Series routers. The **pbb-options** statement and its substatements at the **[edit routing-instances *routing-instance-name*]** hierarchy level, and the **pbb-service-options** statement and its substatements at the **[edit routing-instances *routing-instance-name* service-groups *service-group-name*]** hierarchy level are no longer available for configuring customer and provider routing instances for PBB.

  [See *Provider Backbone Bridging*.]

- **BGP Route Advertisement**—In Junos OS Release 14.1R1, if you include the **advertise-peer-as** statement in a BGP configuration, BGP advertises routes learned from one external BGP (EBGP) peer back to another EBGP peer in the same autonomous system (AS) but not back to the originating peer. In earlier Junos OS Releases, if you include the **advertise-peer-as** statement in the configuration, BGP advertises routes learned from one EBGP peer back to another EBGP peer in the same AS and also to the originating peer.

Services Applications

- **Restrictions for maximum blocksize for NAT port block allocation**—Begining with Junos OS Release 14.1, the maximum blocksize for NAT port block allocation (PBA) is now 32,000.

Subscriber Management and Services

NOTE: **Although present in the code, the subscriber management features are not supported in Junos OS Release 14.1R1. Documentation for subscriber management features is included in the Junos OS Release 14.1 documentation set.**

- **CLI prompt to confirm clearing of all current PPPoE subscriber sessions (M Series, MX Series, and T Series)**—Starting in Junos OS Release 14.1, when you enter the **clear pppoe sessions** command and fail to include the name of an interface associated with the subscriber session that you want to gracefully terminate, the CLI prompts you to confirm that you want to clear all current PPPoE subscriber sessions. In earlier releases, the CLI does not prompt you and instead immediately terminates all the sessions.

- **Change to unicast reverse path forwarding (RPF) check and filter-based forwarding (FBF) compatibility (MX Series)**—Starting in Junos OS Release 14.1, the unicast RPF check is compatible with FBF actions. uRPF check is processed for source address checking before any FBF actions are enabled for static and dynamic interfaces. This applies to both IPv4 and IPv6 families.

- **Support for processing Cisco VSAs in RADIUS messages for service provisioning**—Starting with Junos OS Release 14.1X50, Cisco VSAs are supported for provisioning and management of services in RADIUS messages, in addition to the supported Juniper VSAs for administration of subscriber sessions. In a deployment in which a customer premises equipment (CPE) is connected over an access network to a broadband remote access gateway, the Steel-Belted Radius Carrier (SBRC)

application might be used as the authentication and accounting server using RADIUS as the protocol and the Cisco BroadHop application might be used as the Policy Control and Charging Rules Function (PCRF) server for provisioning services using RADIUS change of authorization (CoA) messages. Both the SBRC and the Cisco BroadHop servers are considered to be connected with the broadband gateway in such a topology.

By default, service accounting is disabled. If you configure service accounting using both RADIUS attributes and the CLI interface, the RADIUS setting takes precedence over the CLI setting. To enable service accounting using the CLI, include the **accounting** statement at the **[edit access profile *profile-name* service]** hierarchy level. To enable interim service accounting updates and configure the amount of time that the router waits before sending a new service accounting update, include the **update-interval *minutes*** statement at the **[edit access profile *profile-name* service accounting]** hierarchy level.

You can configure the router to collect time statistics, or both volume and time statistics, for the service accounting sessions being managed by AAA. To configure the collection of statistical details that are time-based only, include the **statistics time** statement at the **[edit access profile *profile-name* service accounting]** hierarchy level. To configure the collection of statistical details that are both volume-time-based only, include the **statistics volume-time** statement at the **[edit access profile *profile-name* service accounting]** hierarchy level.

- **Specifying the UDP port for RADIUS dynamic-request servers**—You can define the UDP port number to configure the port on which the router that functions as the RADIUS dynamic-request server must receive requests from RADIUS servers. By default, the router listens on UDP port 3799 for dynamic requests from remote RADIUS servers. You can configure the UDP port number to be used for dynamic requests for a specific access profile or for all of the access profiles on the router. To define the UDP port number, include the **dynamic-request-port *port-number*** statement at the **[edit access profile *profile-name* radius-server *server-address*]** or the **[edit access radius-server *server-address*]** hierarchy level.

- **Support for applying access profiles to DHCP local server and DHCP relay agent**—Access profiles enable you to specify subscriber access authentication and accounting parameters. After access profiles are created, you can attach them at the **[edit system services dhcp-local-server]** hierarchy level on a DHCP local server for DHCP or DHCPv6 subscribers and at the **[edit forwarding-options dhcp-relay]** hierarchy level on a DHCP relay agent for DHCP or DHCPv6 subscribers, group of subscribers, or group of interfaces.

  If you configured a global access profile at the **[edit access profile *profile-name*]** hierarchy level for all DHCP or DHCPv6 clients on a router that functions as a DHCP local server or a DHCP relay agent, the access profile configured at the **[edit system services dhcp-local-server**] or **[edit system services dhcpv-local-server dhcpv6**] hierarchy level on a DHCP local server for DHCP or DHCPv6 subscribers and at the **[edit forwarding-options dhcp-relay]** or **[edit forwarding-options dhcp-relay dhcpv6]** hierarchy level on a DHCP relay agent for DHCP or DHCPv6 subscribers take precedence over the global access profile.

  Configuring an access profile for DHCP subscribers at the DHCP relay agent level or the DHCP local server level provide you with the flexibility and effectiveness of enabling

DHCP authentication and accounting for specific subscribers instead of enabling them at a global level. If no access profile is configured at the DHCP relay agent level or the DHCP local server level, the global access profile becomes effective.

[*Release 14.1X51 Documentation PDF*]

- **Support for specifying preauthentication port and password**—You can configure a router that operates as the RADIUS client to contact a RADIUS server for authentication and preauthentication requests on two different UDP ports and using different secret passwords. Similar to configuring the port numbers for authentication and accounting requests, you can define a unique port number that the router uses to contact the RADIUS server for logical line identification (LLID) preauthentication requests. You can also define a unique password for preauthentication requests. If you do not configure a separate UDP port or secret for preauthentication purposes, the same UDP port and secret that you configure for authentication messages is used.

  To configure a unique UDP port number to be used to contact the RADIUS server for preauthentication requests, include the **preauthentication-port** ***port-number*** statement at the **[edit access radius-server** ***server-address*****]** or **[edit access profile** ***profile-name*** **radius-server** ***server-address*****]** hierarchy level.

  To configure the password to be used to contact the RADIUS preauthentication server, include the **preauthentication-secret** ***password*** statement at the [**edit access radius-server** ***server-address*****]** or **[edit access profile** ***profile-name*** **radius-server** ***server-address*****]** hierarchy level.

  The output of the **show network-access aaa radius-servers** command has been enhanced to display the preauthentication port number. The output of the **show network-access aaa radius-servers detail** command has been enhanced to display statistical information on the RADIUS messages exchanged during the preauthentication phase and the port number used for preauthentication.

User Interface and Configuration

- **Configuring regular expressions (M Series, MX Series, and T Series)**—In all supported Junos OS releases, regular expressions can no longer be configured if they require more than 64 MB of memory or more than 256 recursions for parsing.

  This change in the behavior of Junos OS is in line with the FreeBSD limit. The change was made in response to a known consumption vulnerability that allows an attacker to cause a denial-of-service (resource exhaustion) attack by using regular expressions containing adjacent repetition operators or adjacent bounded repetitions. Junos OS uses regular expressions in several places within the CLI. Exploitation of this vulnerability can cause the Routing Engine to crash, leading to a partial denial of service. Repeated exploitation can result in an extended partial outage of services provided by the routing protocol process (rpd).

- **Change in show route protocol evpn output**—In all supported Junos OS releases prior to Release 14.1, the output of the command **show route protocol evpn** does not provide any information for correlating the routes installed in the forwarding plane with routes exchanged in the signaling plane.

Starting with Junos OS Release 14.1, the command **show route protocol evpn** output provides additional correlation detail between forwarding plane and signaling plane routes.

[See show route protocol.]

VPNs

- **Group VPN ike proposal commit check (M Series, MX Series, and T Series)**—Starting in Junos OS Release 14.1, the **proposals** option for the **policy** statement under the following hierarchies is mandatory and will be checked on a commit:

  [edit security group-vpn member ike policy *policy-name*]
  [edit security group-vpn server ike policy *policy-name*]
  [edit security ike policy *policy-name*]

  Prior to Junos OS Release 14.1, the **proposals** option was not checked on a commit.

- **New output field added to the show route forwarding-table family vpls command**—Starting in Junos OS Release 14.1, the **show route forwarding-table family vpls** command output contains an extra field to show "Enabled Protocols" for a routing table instance. The following sample output of the **show route forwarding-table family vpls** command shows the **Enabled Protocols** field when broadcast, unknown unicast, and multicast (BUM) hashing is enabled by configuring the **bum-hashing** statement at the **[edit routing-instances green protocols vpls]** hierarchy level:

```
user@host> show route forwarding-table family vpls
Routing table: green.vpls
VPLS:
Enabled protocols: BUM hashing
Destination        Type RtRef Next hop           Type Index    NhRef Netif
default            perm     0                    dscd      519     1
lsi.1048832        intf     0                    indr  1048574     4
                              4.4.3.2           Push 262145      621     2
ge-3/0/0.0
00:19:e2:25:d0:01/48 user     0                 ucst      590     5 ge-2/3/9.0
0x30003/51         user     0                    comp      627     2
ge-2/3/9.0         intf     0                    ucst      590     5 ge-2/3/9.0
ge-3/1/3.0         intf     0                    ucst      619     4 ge-3/1/3.0
0x30002/51         user     0                    comp      600     2
0x30001/51         user     0                    comp      597     2
```

The following sample output of the **show route forwarding-table family vpls** command shows the **Enabled Protocols** field when broadcast, unknown unicast, and multicast (BUM) hashing is enabled by configuring the **bum-hashing** statement at the **[edit routing-instances green protocols vpls]** hierarchy level and MAC Statistics is enabled by configuring the **mac-statistics** statement at the **set routing-instances green protocols vpls** hierarchy level:

```
user@host> show route forwarding-table family vpls
Routing table: green.vpls
VPLS:
Enabled protocols: BUM hashing, MAC Stats
Destination        Type RtRef Next hop           Type Index    NhRef Netif
default            perm     0                    dscd      519     1
lsi.1048834        intf     0                    indr  1048574     4
                              4.4.3.2           Push 262145      592     2
```

```
ge-3/0/0.0
00:19:e2:25:d0:01/48 user     0                 ucst      590     5 ge-2/3/9.0
0x30003/51           user     0                  comp      630     2
ge-2/3/9.0           intf     0                 ucst      590     5 ge-2/3/9.0
ge-3/1/3.0           intf     0                 ucst      591     4 ge-3/1/3.0
0x30002/51           user     0                  comp      627     2
0x30001/51           user     0                  comp      624     2
```

Related Documentation

- New and Changed Features on page 10
- Known Behavior on page 44
- Known Issues on page 44
- Documentation Updates on page 51
- Migration, Upgrade, and Downgrade Instructions on page 53
- Product Compatibility on page 63

Known Behavior

There are no changes in known behavior in Junos OS Release 14.1R1 for the M Series, MX Series, and T Series.

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

- **High Availability (HA) and Resiliency**

High Availability (HA) and Resiliency

- The MPC5E, MPC5EQ, and MP6E cards do not support unified ISSU on an MX Series Virtual Chassis.

Related Documentation

- New and Changed Features on page 10
- Changes in Behavior and Syntax on page 36
- Known Issues on page 44
- Documentation Updates on page 51
- Migration, Upgrade, and Downgrade Instructions on page 53
- Product Compatibility on page 63

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 14.1R1 for the M Series, MX Series, and T Series.

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

- Forwarding and Sampling
- General Routing
- Interfaces and Chassis
- Internet Protocol Security (IPsec)
- Layer 2 Ethernet Services
- MPLS
- Network Address Translation (NAT)
- Platform and Infrastructure
- Routing Protocols
- Services Applications
- Software Installation and Upgrade
- User Interface and Configuration
- VPNs

Forwarding and Sampling

- We find this issue, if we set the firewall counter of IPv6's payload-protocol. Even if we confirm this counter using "show snmp mib walk jnxFWCounter ascii", we cannot see this counter. It's a cosmetic issue. So this firewall works fine. Router# run show snmp mib walk jnxFWCounter ascii jnxFWCounter."__default_arp_policer__"."__default_arp_policer__" = __default_arp_policer__ <<<<<<<<<< We cannot find counter. PR899800

General Routing

- Under particular scenarios, commit action might lead the Context-Identifier to be ignored when the OSPF protocol refreshes its database. Then the PE router will stop advertising this Context-Identifier. PR954033
- Management interface(fxp) can transmit IPv6 packets to network interfaces. PR955132
- "show interfaces et-x/y/z extensive" will display MRU now. MRU can be configured at "set interfaces et-x/y/z gigether-options mru" If MRU is not configured, then it is defaulted to MTU + 8. MRU displayed from the CLI does not include the CRC. PR958162
- When the size of apply-macro generated by op-script is equal to 1022 characters, the extensible subscriber services management daemon (essmd) subscribers might get stuck in a "terminating" state. PR966764
- Changing service set configuration continuously during scaled traffic conditions might result in stability issues. PR978032
- On T Series router with FIB Localization enabled, if reboot the Routing Engine while scaled traffic is running, the FIB-remote FPC might crash. PR979098

- In rare condition, when PPPoE subscribers log in with large amounts of configuration data, the subscriber management infrastructure daemon (smid) and authentication service process (authd) might crash, and no new subscribers could connect to the router. PR980646
- The fabric performance of MPC1, MPC2, or 16xXE MPC in 'increased-bandwidth' mode on an MX960 populated with SCBE's will be less compared to redundant mode due to XF1 ASIC scheduling bugs. PR993787

Interfaces and Chassis

- 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. PR65800
- RPD may assert on restart routing / NSR switchover or GRES switchover or FPC offline/online randomly. This is due to instability in BFD triggered local repair RLI which is enabled by default and cannot be turned off. PR926188
- Queue stats counters for AE interface will become invalid after deactivating ifl on the AE interface. PR926617
- Strange FRU Insertion trap[RE PCMCIA card 0] is generated when Routing Engine master-switching is done on box with RE-1800. PR943767
- If there is an IRB interface configured for "family inet6" in a bridge-domain on an MX Series router, the Packet Forwarding Engine might not correctly update the nexthop for an IPv6 route when the MAC address associated with the nexthop moves from an AE interface to a non-AE interface. PR958019
- In an EVPN deployment, when a CE is multihomed to multiple PEs (two or more) and BGP is cleared on any one of the multihomed PEs towards the DF-PE, then traffic loss might be observed in the network as the different multi-homed PEs react to the event and execute the Designated Forwarder (DF) election. For example, if two multi-homed PEs are connected to one CE and the BGP is cleared on the non-DF for the session with the DF, then this triggers a DF election on both the PEs and both elect themselves as the DF for the Ethernet segment with the CE, until the BGP session is established again and the ES-specific routes are exchanged again. In this case, both PEs unblock their CE-facing interfaces and can thus produce double traffic towards a remote PE. Depending on how the CE device is configured, 1) it is possible that a loop might occur in the network with respect to the intra-subnet E-VPN traffic, and loss might be observed for up to 30 seconds 2) Another side effect might also be continuous movement of the ARP routes between the MH PEs and with it the local IP EVPN routes' ownership as well, thus causing inter-subnet traffic loss towards the multi-homed CE from the remote PE. PR967376
- In an EVPN deployment when a CE is multihomed to multiple PEs (two or more) and if one of the multihomed PEs is configured for the multihoming while there is ongoing traffic between the DF and the nonmultihomed remote PE but also being sent to the non-DF (while it being configured and committed for the multihoming), then there will be traffic loss observed in the network. The reason is that as the new multihomed PE establishes state there is a nonzero finite amount of time when the CE-facing interface

is unblocked before it gets blocked for being the non-DF. Because of this, the MAC from the traffic is learned and sent over the remote PE. The remote PE will see a MAC-move from the original DF to the new PE and then back to the old DF. With this, the mac+IP routes are also cleaned up and then added back. While the routes are in flux, the inter-subnet traffic from behind the remote PE to the MH-CE will undergo a drop. PR970429

- Temperature Top and Bottom are swapped in show chassis environments output for Type3/Type4 FPCs of T-Series. PR975758
- PP0 static chap local-name is not used. PR978154
- In the multilink frame relay (mlfr) environment with "disable-tx" configuration, when the differential delay exceeds the red limit, the transmission is disabled on the bundle link. When it is restored, the link should be added back. But in this case, the link stays in the disable state and it is not rejoined to the bundle. PR978855
- type-4 ES routes not used for DF selection in multihoming case upon RPD restart. PR983569
- 1GbE SFP(EX-SFP-1FE-LX) output optical power is restored after reseating by manual removal/insert of SFP although the IF is disabled. PR984192
- SNMP OID VRRP-MIB::vrrpAssoIpAddrRowStatus returns only one IP address when the interface ifl has been configured with two virtual-addressees under two vsrrp-groups. PR987992
- CFMD might crash after configuration change of an interface in a logical system which is under OAM configuration for a l2vpn instance. PR991122

Internet Protocol Security (IPsec)

NOTE: NAT-T with IPsec is not recommended for use because there are issues with scale, DPD, and NAPT. For more information, see the following PRs PR888123, PR951616, and PR989054.

- IPsec tunnels will not come up if IKE Packets traverse through NAPT. PR888123
- IPsec tunnels are deleted with NAT-T and DPD on IPsec rekey. PR951616
- IPsec endpoint fails to decrypt packets on some of the tunnels with NAT between IPsec endpoints. PR989054

Layer 2 Ethernet Services

- When Cisco is running in an old version of PVST+, it doesn't carry VLAN ID in the end of BPDU. So Juniper Netwoks equipment fails to response Topology Change Notification ACK packet when it interoperates with Cisco equipment. After the fix, Juniper Networks equipment will read the VLAN ID information from the Ethernet header. PR984563
- jnxLacpTimeOut trap might show Neg# and incorrect# for jnxLacpifIndex and jnxLacpAggregateifIndex. PR994725

MPLS

- For point-to-multipoint LSPs configured for VPLS, the "ping mpls" command reports 100 percent packet loss even though the VPLS connection is active. PR287990
- snmpwalk/snmpgetnext or "show snmp mib walk" fail when polling MPLSLSPOCTETS, MPLSLSPPACKETS, MPLSLSPINFOOCTETS, or MPLSLSPINFOPACKETS. PR981061
- In the MPLS environment with "egress-protection" configuration, there is a direct LDP session between the primary PE and protector. One context-id is configured as the primary PE's loopback address or any LDP enabled interface address. When delete the whole apply-group or delete the ldp policy from apply-group, the routing protocol process (rpd) might crash. PR988775

Network Address Translation (NAT)

- When using **clear services nat mappings** to clear implicit dynamic mappings (created for NAPT44 with PCP at full scale) more than one time, you may see scheduler oinker messages. These messages can be safely ignored. PR923166
- Repeatedly applying the commands **clear services nat mappings** or **clear services nat flows** at maximum scale, immediately followed by scale traffic may result in stability issues or packet loss for short durations when using an MS-DPC, due to memory constraints. We recommend that you avoid such repeated usage of these clear commands at maximum scale. However, these problems do not occur when the commands are used freely at 70% load. PR934580

Platform and Infrastructure

- The Routing Engine and FPCs are connected with an internal Ethernet switch. In some rare case, the FPCs might receive a malformed packet from the Routing Engine (for example, a packet gets corrupted somewhere on it's way from the Routing Engine to the FPC), then the toxic traffic might crash the FPC. PR938578
- After rebooting the device, the interface rejects all packets. PR962782
- When two midplane link errors are present between F13 and F2 Sibs, then CLOS rerouting logic does not work properly. This can introduce RODR packet drops and result in destination errors in the plane. PR992677
- "delete" or "deactivate" of apply-group defining the entire TACACS or RADIUS configuration configured under [edit system apply-group <>] does not take effect on commit. This could lead to TACACS or RADIUS based authentication to still continue working despite removal (delete/deactivate) of configuration. PR992837

Routing Protocols

- When you configure damping globally and use the import policy to prevent damping for specific routes, and a peer sends a new route that has 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 nondefault setting. As a result, damping settings do not change appropriately when the route attributes change. PR51975
- Continuous soft core-dump might be observed due to bgp-path-selection code. RPD forks a child and the child asserts to produce a core file. The problem is with route ordering. And it is auto-corrected after collecting this soft-assert-coredump, without any impact to traffic/service. PR815146
- In certain rare circumstances, BGP NSR replication to the backup Routing Engine might not make forward progress. This was due to an issue where an internal buffer was not correctly cleared in rare circumstances when the backup Routing Engine was experiencing high CPU. PR975012
- Due to some corner cases, certain commits could cause the input and/or output BGP policies to be reexamined causing an increase in rpd CPU utilization. PR979971
- PPMD filter is not programmed properly which will result in the Routing Engine absorbing BFD packets instead of the Packet Forwarding Engine. PR985035
- In V4 RG, member site receives traffic from both serving sites for few sources upon withdraw/inject routes for 30 seconds. PR988561

Services Applications

- When you specify a standard application at the **[edit security idp idp-policy *<policy-name>* rulebase-ips rule *<rule-name>* match application]** hierarchy level, IDP does not detect the attack on the nonstandard port (for example, junos:ftp on port 85). Whether it is a custom or predefined application, the application name does not matter. IDP simply looks at the protocol and port from the application definition. Only when traffic matches the protocol and port does IDP try to match or detect against the associated attack. PR477748
- Clearing the stateful firewall subscriber analysis causes the active subscriber count to display a very huge number. The large number is seen because when a subscriber times out, the number of active subscribers is decremented. If it is set to zero using the clear command, then a decrement would give an incorrect result. There is no impact to the overall functionality, and the fix is expected to be present in 14.1R2. PR939832
- If a destination-prefix or source-prefix is used like the following example, the nat rule and term names will be used to generate an internal jpool with a form : _jpool_{rule_name}_{term_name}. If the generated jpool name exceeds 52 characters in length, it will get truncated. If the truncated jpool name overlaps with another generated jpool name, it will lead to inconsistent pool usage. PR973465
- In the L2TP scenario, when the username is more than 200 characters long, the L2TP daemon (jl2tpd) on LAC might crash. PR979047

- Stale entries occur after connecting and disconnecting 100 PPPoE Dual Stack subscribers with DTCP filters based on CID. PR979517
- If a PPPoE/PPP user disconnects in the access network without the LAC/LNS noticing it to tear down the connection (also the PPP keepalive hasn't detected yet), and a second PPP request comes from the same subscriber on the L2TP tunnel (same or different LAC/tunnel), then a second route is added to the table having the next hop "service to unknown". PR981488
- In the Layer 2 Tunneling Protocol (L2TP) environment with "failover-within-preference" configuration, there are two L2TP network servers (LNSs) with different preference. One LNS is primary and another is backup. If the primary LNS is dead, the router doesn't try to create L2TP tunnel to the backup LNS. PR990042

Software Installation and Upgrade

- By upgrade-with-configuration, the user can specify a configuration to be applied on upgrade, but the configuration file will not be loaded post upgrading. As a result, the router will bring up with old configuration. PR983291

User Interface and Configuration

- Selecting the Monitor port for any port in the Chassis Viewer page takes the user to the common Port Monitoring page instead of the corresponding Monitoring page of the selected port. PR446890
- User needs to wait until a page is completely loaded before navigating away from that page. PR567756
- The J-Web interface allows the creation of duplicate term names in the Configure > Security > Filters > IPV4 Firewall Filters page. But the duplicate entry is not shown in the grid. There is no functionality impact on the J-Web interface. PR574525
- Using the Internet Explorer 7 browser, while deleting a user from the Configure > System Properties > User Management > Users page on the J-Web interface, the system is not showing a warning message, whereas in the Firefox browser error messages are shown. PR595932
- If you access the J-Web interface using the Microsoft Internet Web browser version 7, on the BGP Configuration page (Configure > Routing > BGP), all flags might be shown in the Configured Flags list (in the Edit Global Settings window, on the Trace Options tab) even though the flags are not configured. As a workaround, use the Mozilla Firefox Web browser. PR603669
- On the J-Web interface, the next hop column in Monitor > Routing > Route Information displays only the interface address, and the corresponding IP address is missing. The title of the first column displays "static route address" instead of "Destination Address." PR684552

VPNs

- 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. PR32763
- Upon withdraw/inject bgp routes in the serving PEs for two different route-groups, member/regular sites receive traffic from both serving sites for 60 seconds. PR973623
- The S-PMSI tunnel might fail to be originated from the ingress PE after flapping the routes to customer multicast source. PR983410
- In MVPN scenario, a multihomed ingress PE might fail to advertise type-4 after losing routes to local sources. PR984946
- Group VPN member registration in MX Series router will not succeed if the same interface is used for both data traffic and server-member communication. This limitation will apply if a group VPN service-set is applied on the interface in which the member is communicating with the Group key server. PR993001

Related Documentation

- New and Changed Features on page 10
- Changes in Behavior and Syntax on page 36
- Known Behavior on page 44
- Documentation Updates on page 51
- Migration, Upgrade, and Downgrade Instructions on page 53
- Product Compatibility on page 63

Documentation Updates

This section lists the errata and changes in Junos OS Release 14.1R1 documentation for the M Series, MX Series, and T Series.

- Ethernet Interfaces Feature Guide on page 51
- Interchassis Redundancy Using Virtual Chassis Feature Guide for MX Series Routers on page 52
- Junos Address Aware Carrier Grade NAT and IPv6 Feature Guide on page 52
- Services Interfaces Configuration Guide on page 53

Ethernet Interfaces Feature Guide

- In the *Output Fields* section of the **show interfaces (10-Gigabit Ethernet)**, **show interfaces (Gigabit Ethernet)**, and **show interfaces (Fast Ethernet)** command topics of the *Ethernet Interfaces Feature Guide*, the descriptions of the **Bit errors** and **Errored blocks** fields that are displayed under the PCS Statistics section of the output are ambiguous. The following are the revised descriptions of these fields:

- **Bit errors**—The number of seconds during which at least one bit error rate (BER) occurred while the PCS receiver is operating in normal mode.
- **Errored blocks**—The number of seconds when at least one errored block occurred while the PCS receiver is operating in normal mode.

Interchassis Redundancy Using Virtual Chassis Feature Guide for MX Series Routers

- In the *Junos OS 13.2 Release Notes for M Series Multiservice Edge Routers, MX Series 3D Universal Edge Routers, and T Series Core Routers*, the *Support for MX Series Virtual Chassis (MX Series routers with MPC3E interfaces)* feature description failed to mention that you can configure a two-member MX Series Virtual Chassis on both MPC3E modules and MPC4E modules. The correct description for this feature is as follows:

  - **Support for MX Series Virtual Chassis on MX Series routers with MPC3E and MPC4E interfaces**—Extends support for configuring a two-member MX Series Virtual Chassis to MX240, MX480, and MX960 routers with any of the following modules installed:

    - MPC3E (model number MX-MPC3E-3D)
    - 32x10GE MPC4E (Model number: MPC4E-3D-32XGE-SFPP)
    - 2x100GE + 8x10GE MPC4E (Model number: MPC4E-3D-2CGE-8XGE)

    All MX Series Virtual Chassis features are supported on these modules.

    In earlier Junos OS releases, MX Series routers did not support MX Series Virtual Chassis configuration on MPC3E and MPC4E modules.

    [See Junos OS High Availability Library for Routing Devices and Junos OS for MX Series 3D Universal Edge Routers.]

Junos Address Aware Carrier Grade NAT and IPv6 Feature Guide

- The **address-allocation** statement topic fails to state the following additional information regarding addresses allocation on MS-MICs and MS-MPCs:

  Regardless of whether the round-robin method of allocation is addresses is enabled by using the **address-allocation round-robin** statement, round-robin allocation is enabled by default on MS-MICs and MS-MPCs.

- The **address-allocation** statement topic fails to state the following additional information regarding addresses allocation on MS-MICs and MS-MPCs:

  Regardless of whether the round-robin method of allocation is addresses is enabled by using the **address-allocation round-robin** statement, round-robin allocation is enabled by default on MS-MICs and MS-MPCs.

Services Interfaces Configuration Guide

- The following additional information applies to the sample configuration described in the *Example: Flow-Tap Configuration* topic of the *Flow Monitoring* chapter.

  NOTE: The described example applies only to M Series and T Series routers, except M160 and TX Matrix routers. For MX Series routers, because the flow-tap application resides in the Packet Forwarding Engine rather than a service PIC or Dense Port Concentrator (DPC), the Packet Forwarding Engine must send the packet to a tunnel logical (vt-) interface to encapsulate the intercepted packet. In such a scenario, you need to allocate a tunnel interface and assign it to the dynamic flow capture process for FlowTapLite to use.

Related Documentation

- New and Changed Features on page 10
- Changes in Behavior and Syntax on page 36
- Known Behavior on page 44
- Known Issues on page 44
- Migration, Upgrade, and Downgrade Instructions on page 53
- Product Compatibility on page 63

Migration, Upgrade, and Downgrade Instructions

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for the M Series, MX Series, and T Series. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

Basic Procedure for Upgrading to Release 14.1

In order to upgrade to Junos OS 10.0 or later, you must be running Junos OS 9.0S2, 9.1S1, 9.2R4, 9.3R3, 9.4R3, 9.5R1, or later minor versions, or you must specify the **no-validate** option on the **request system software install** command.

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

NOTE: With Junos OS Release 9.0 and later, the compact flash disk memory requirement for Junos OS is 1 GB. For M7i and M10i routers with only 256 MB memory, see the Customer Support Center JTAC Technical Bulletin PSN-2007-10-001 at **https://www.juniper.net/alerts/viewalert.jsp?txtAlertNumber=PSN-2007-10-001&actionBtn=Search**

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

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

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

The download and installation process for Junos OS Release 14.1 is different from previous Junos OS releases.

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

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

2. Select the name of the Junos platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the **Release** drop-down list to the right of the Download Software page.
4. Select the **Software** tab.
5. In the **Install Package** section of the **Software** tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new **jinstall** package on the 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-14.1R11-domestic-signed.tgz
```

All other customers, use the following command:

```
user@host> request system software add validate reboot
source/jinstall-14.1R11-export-signed.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 14.1 jinstall package, you cannot issue the request system software rollback command to return to the previously installed software. Instead you must issue the request system software add validate command and specify the jinstall package that corresponds to the previously installed software.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release.

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

Upgrading a Router with Redundant Routing Engines

If the router has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation as follows:

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine and save the configuration change to both Routing Engines.
2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.

3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.
4. Install the new software on the original master Routing Engine that is now active as the backup Routing Engine.

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

Upgrading Juniper Network Routers Running Draft-Rosen Multicast VPN to Junos OS Release 10.1

In releases prior to Junos OS Release 10.1, the draft-rosen multicast VPN feature implements the unicast **lo0.x** address configured within that instance as the source address used to establish PIM neighbors and create the multicast tunnel. In this mode, the multicast VPN loopback address is used for reverse path forwarding (RPF) route resolution to create the reverse path tree (RPT), or multicast tunnel. The multicast VPN loopback address is also used as the source address in outgoing PIM control messages.

In Junos OS Release 10.1 and later, you can use the router's main instance loopback (**lo0.0**) address (rather than the multicast VPN loopback address) to establish the PIM state for the multicast VPN. We strongly recommend that you perform the following procedure when upgrading to Junos OS Release 10.1 if your draft-rosen multicast VPN network includes both Juniper Network routers and other vendors' routers functioning as provider edge (PE) routers. Doing so preserves multicast VPN connectivity throughout the upgrade process.

Because Junos OS Release 10.1 supports using the router's main instance loopback (**lo0.0**) address, it is no longer necessary for the multicast VPN loopback address to match the main instance loopback adddress **lo0.0** to maintain interoperability.

NOTE: **You might want to maintain a multicast VPN instance lo0.x address to use for protocol peering (such as IBGP sessions), or as a stable router identifier, or to support the PIM bootstrap server function within the VPN instance.**

Complete the following steps when upgrading routers in your draft-rosen multicast VPN network to Junos OS Release 10.1 if you want to configure the routers's main instance loopback address for draft-rosen multicast VPN:

1. Upgrade all M7i and M10i routers to Junos OS Release 10.1 before you configure the loopback address for draft-rosen Multicast VPN.

NOTE: **Do not configure the new feature until all the M7i and M10i routers in the network have been upgraded to Junos OS Release 10.1.**

2. After you have upgraded all routers, configure each router's main instance loopback address as the source address for multicast interfaces. Include the **default-vpn-source interface-name *loopback-interface-name*]** statement at the **[edit protocols pim]** hierarchy level.

3. After you have configured the router's main loopback address on each PE router, delete the multicast VPN loopback address (**lo0.x**) from all routers.

   We also recommend that you remove the multicast VPN loopback address from all PE routers from other vendors. In Junos OS releases prior to 10.1, to ensure interoperability with other vendors' routers in a draft-rosen multicast VPN network, you had to perform additional configuration. Remove that configuration from both the Juniper Networks routers and the other vendors' routers. This configuration should be on Juniper Networks routers and on the other vendors' routers where you configured the lo0.mvpn address in each VRF instance as the same address as the main loopback (lo0.0) address.

   This configuration is not required when you upgrade to Junos OS Release 10.1 and use the main loopback address as the source address for multicast interfaces.

   

   NOTE: **To maintain a loopback address for a specific instance, configure a loopback address value that does not match the main instance address (lo0.0).**

For more information about configuring the draft-rosen Multicast VPN feature, see the Multicast Protocols Feature Guide for Routing Devices.

Upgrading the Software for a Routing Matrix

A routing matrix can be either a TX Matrix router as the switch-card chassis (SCC) or a TX Matrix Plus router as the switch-fabric chassis (SFC). By default, when you upgrade software for a TX Matrix router or a TX Matrix Plus router, the new image is loaded onto the TX Matrix or TX Matrix Plus router (specified in the Junos OS CLI by using the **scc** or **sfc** option) and distributed to all line-card chassis (LCCs) in the routing matrix (specified in the Junos OS CLI by using the **lcc** option). To avoid network disruption during the upgrade, ensure the following conditions before beginning the upgrade process:

- A minimum of free disk space and DRAM on each Routing Engine. The software upgrade will fail on any Routing Engine without the required amount of free disk space and DRAM. To determine the amount of disk space currently available on all Routing Engines of the routing matrix, use the CLI **show system storage** command. To determine the amount of DRAM currently available on all the Routing Engines in the routing matrix, use the CLI **show chassis routing-engine** command.
- The master Routing Engines of the TX Matrix or TX Matrix Plus router (SCC or SFC) and all LCCs connected to the SCC or SFC are all re0 or are all re1.
- The backup Routing Engines of the TX Matrix or TX Matrix Plus router (SCC or SFC) and all LCCs connected to the SCC or SFC are all re1 or are all re0.
- All master Routing Engines in all routers run the same version of software. This is necessary for the routing matrix to operate.
- All master and backup Routing Engines run the same version of software before beginning the upgrade procedure. Different versions of the Junos OS can have incompatible message formats especially if you turn on GRES. Because the steps in

the process include changing mastership, running the same version of software is recommended.

- For a routing matrix with a TX Matrix router, the same Routing Engine model is used within a TX Matrix router (SCC) and within a T640 router (LCC) of a routing matrix. For example, a routing matrix with an SCC using two RE-A-2000s and an LCC using two RE-1600s is supported. However, an SCC or an LCC with two different Routing Engine models is not supported. We suggest that all Routing Engines be the same model throughout all routers in the routing matrix. To determine the Routing Engine type, use the CLI **show chassis hardware | match routing** command.
- For a routing matrix with a TX Matrix Plus router, the SFC contains two model RE-DUO-C2600-16G Routing Engines, and each LCC contains two model RE-DUO-C1800-8G or RE-DUO-C1800-16G Routing Engines.

BEST PRACTICE: **Make sure that all master Routing Engines are re0 and all backup Routing Engines are re1 (or vice versa). For the purposes of this document, the master Routing Engine is re0 and the backup Routing Engine is re1.**

To upgrade the software for a routing matrix, perform the following steps:

1. Disable graceful Routing Engine switchover (GRES) on the master Routing Engine (re0) and save the configuration change to both Routing Engines.
2. Install the new Junos OS release on the backup Routing Engine (re1) while keeping the currently running software version on the master Routing Engine (re0).
3. Load the new Junos OS on the backup Routing Engine. After making sure that the new software version is running correctly on the backup Routing Engine (re1), switch mastership back to the original master Routing Engine (re0) to activate the new software.
4. Install the new software on the new backup Routing Engine (re0).

For the detailed procedure, see the Routing Matrix with a TX Matrix Router Deployment Guide or the Routing Matrix with a TX Matrix Plus Router Deployment Guide.

Upgrading Using Unified ISSU

Unified in-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic. Unified in-service software upgrade is only supported by dual Routing Engine platforms. In addition, graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) must be enabled. For additional information about using unified in-service software upgrade, see the High Availability Feature Guide for Routing Devices.

Upgrading from Junos OS Release 9.2 or Earlier on a Router Enabled for Both PIM and NSR

Junos OS Release 9.3 introduced NSR support for PIM for IPv4 traffic. However, the following PIM features are not currently supported with NSR. The commit operation fails if the configuration includes both NSR and one or more of these features:

- Anycast RP
- Draft-Rosen multicast VPNs (MVPNs)
- Local RP
- Next-generation MVPNs with PIM provider tunnels
- PIM join load balancing

Junos OS Release 9.3 introduced a new configuration statement that disables NSR for PIM only, so that you can activate incompatible PIM features and continue to use NSR for the other protocols on the router: the **nonstop-routing disable** statement at the **[edit protocols pim]** hierarchy level. (Note that this statement disables NSR for all PIM features, not only incompatible features.)

If neither NSR nor PIM is enabled on the router to be upgraded or if one of the unsupported PIM features is enabled but NSR is not enabled, no additional steps are necessary and you can use the standard upgrade procedure described in other sections of these instructions. If NSR is enabled and no NSR-incompatible PIM features are enabled, use the standard reboot or ISSU procedures described in the other sections of these instructions.

Because the **nonstop-routing disable** statement was not available in Junos OS Release 9.2 and earlier, if both NSR and an incompatible PIM feature are enabled on a router to be upgraded from Junos OS Release 9.2 or earlier to a later release, you must disable PIM before the upgrade and reenable it after the router is running the upgraded Junos OS and you have entered the **nonstop-routing disable** statement. If your router is running Junos OS Release 9.3 or later, you can upgrade to a later release without disabling NSR or PIM—simply use the standard reboot or ISSU procedures described in the other sections of these instructions.

To disable and reenable PIM:

1. On the router running Junos OS Release 9.2 or earlier, enter configuration mode and disable PIM:

   ```
   [edit]

   user@host# deactivate protocols pim
   user@host# commit
   ```

2. Upgrade to Junos OS Release 9.3 or later software using the instructions appropriate for the router type. You can either use the standard procedure with reboot or use ISSU.
3. After the router reboots and is running the upgraded Junos OS, enter configuration mode, disable PIM NSR with the **nonstop-routing disable** statement, and then reenable PIM:

```
[edit]

user@host# set protocols pim nonstop-routing disable
user@host# activate protocols pim
user@host# commit
```

Downgrading from Release 14.1

To downgrade from Release 14.1 to another supported release, follow the procedure for upgrading, but replace the 14.1 **jinstall** package with one that corresponds to the appropriate release.

NOTE: You cannot downgrade more than three releases. For example, if your routing platform is running Junos OS Release 11.4, you can downgrade the software to Release 10.4 directly, but not to Release 10.3 or earlier; as a workaround, you can first downgrade to Release 10.4 and then downgrade to Release 10.3.

For more information, see the *Installation and Upgrade Guide*.

Changes Planned for Future Releases

- **Introduction of the all keyword to prevent accidental execution of certain clear commands**—The **all** keyword is planned to be introduced in Junos OS Relase 14.2 (as an optional keyword) and in Junos OS Release 15.2 (as a mandatory keyword) for certain **clear** commands that are used for clearing protocol and neighbor sessions. This makes users explicitly select the **all** keyword to clear all protocol or session information. Thus, it prevents accidental clearing or resetting of protocols or neighbor sessions, which might disrupt network operations.

  The **all** keyword is planned to be introduced for the following **clear** commands:

  - **clear arp**
  - **clear bgp neighbor**
  - **clear bfd adaptation**
  - **clear bfd session**
  - **clear igmp membership**
  - **clear isis adjacency**
  - **clear isis database**
  - **clear ldp neighbor**
  - **clear ldp session**
  - **clear mld membership**
  - **clear mpls lsp**
  - **clear msdp cache**
  - **clear multicast forwarding-cache**

- **clear (ospf | ospf3) database**
- **clear (ospf | ospf3) neighbor**
- **clear pim join**
- **clear pim join-distribution**
- **clear pim register**
- **clear rsvp sessions**

In Junos OS Release 14.2 and 15.1—the **all** keyword would be *optional*. Therefore, when you type any of these **clear** commands followed by the **?** in the CLI, the **all** keyword would be listed as an option after the **<[Enter]>** keyword. You can execute the **clear** command directly or with the **all** keyword to clear all information. For example, when you type **clear mpls lsp ?**, you'll see:

```
user@host> clear mpls lsp ?

Possible completions:
<[Enter]>            Execute this command
all                  Reset 'all' the nontransit or egress LSPs
                     originating on this router       <<<<<<<<<<<<
autobandwidth        Clear LSP autobandwidth counters
logical-system       Name of logical system, or 'all'
name                 Regular expression for LSP names to match
optimize             Perform nonpreemptive optimization computation now
...
```

Both **clear mpls lsp** or **clear mpls lsp all** would function identically in these releases.

In Junos OS Release 15.2 and later—the **all** keyword would be *mandatory*. Therefore, when you type a **clear** command followed by the **?** in the CLI, the **<[Enter]>** option to execute the command directly (without specifying any options) would not be available.

For example, when you type **clear mpls lsp ?**, you would see **all** listed as an option but not **<[Enter]>** to execute the command directly. Therefore, you would have to type **clear mpls lsp all** and then press **<[Enter]>** if you want to clear information about all the non transit or egress LSPs originating on the router.

```
user@host> clear mpls lsp ?

Possible completions:
all                  Reset 'all' the nontransit or egress LSPs
                     originating on this router       <<<<<<<<<<<<
autobandwidth        Clear LSP autobandwidth counters
logical-system       Name of logical system, or 'all'
name                 Regular expression for LSP names to match
optimize             Perform nonpreemptive optimization computation now
...
```

Related Documentation

- New and Changed Features on page 10
- Changes in Behavior and Syntax on page 36
- Known Behavior on page 44
- Known Issues on page 44

- Documentation Updates on page 51
- Product Compatibility on page 63

Product Compatibility

- Hardware Compatibility on page 63

Hardware Compatibility

To obtain information about the components that are supported on the devices, and special compatibility guidelines with the release, see the Hardware Guide and the Interface Module Reference for the product.

To determine the features supported on M Series, MX Series, and T Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at: http://pathfinder.juniper.net/feature-explorer/

Related Documentation

- New and Changed Features on page 10
- Changes in Behavior and Syntax on page 36
- Known Behavior on page 44
- Known Issues on page 44
- Documentation Updates on page 51
- Migration, Upgrade, and Downgrade Instructions on page 53

Junos OS Release Notes for PTX Series Packet Transport Routers

These release notes accompany Junos OS Release 14.1R1 for the PTX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

You can also find these release notes on the Juniper Networks Junos OS Documentation webpage, located at http://www.juniper.net/techpubs/software/junos/.

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 14.1R1 for the PTX Series.

Hardware

- **New FPC with eight Packet Forwarding Engines (PTX5000)**—Starting in Junos OS Release 14.1, a new FPC (FPC2-PTX-P1A), with eight Packet Forwarding Engines and two PIC slots, is supported on the PTX5000. The FPC is capable of forwarding at 960 Gbps speed, and it supports 300W of PIC power per PIC slot. The new FPC supports the following PICs:
  - P2-100GE-CFP2 (4x100G CFP2 PIC)
  - P1-PTX-24-10GE-SFPP (24x10G LAN PIC)
  - P1-PTX-24-10G-W-SFPP (24x10G LAN/WAN PIC)
  - P1-PTX-2-100G-C-WDM-C (2x100G LH DWDM PIC)
- **New 4-port 100-Gigabit Ethernet PIC (PTX5000)**—Beginning with Junos OS Release 14.1, a new 4-port 100-Gigabit Ethernet PIC with CFP2 (P2-100GE-CFP2) is supported on the FPC FPC2-PTX-P1A in a PTX5000. The PIC supports L4 optics.

- **New SIB to support high density FPC (PTX5000)**—Starting in Junos OS Release 14.1, a new high-density SIB (SIB2-I-PTX5000) provides switch fabric capacity of 960 Gbps speed per FPC slot for the FPC FPC2-PTX-P1A in a PTX5000.
- **New high-capacity DC PSM and PDU (PTX5000)**—Starting in Junos OS Release 14.1, the following DC power supply module (PSM) and DC power distribution unit (PDU) are added to provide power to a new, high-density FPC—FPC2-PTX-P1A—and other components in a PTX5000:

  · PTX High Capacity-60A DC PDU (PDU2-PTX-DC)

  · PTX High Capacity-60A DC PSM (PSM2-PTX-DC)
- **Fabric capacity on PTX5000**—Starting with Junos OS Release 14.1, the PTX5000 supports nine Switch Interface Boards (SIBs). Each FPC2-PTX-P1A FPC supports 1Tb per slot capacity, thereby resulting in a fabric bandwidth of 16 terabits per second (Tbps), full-duplex (8 Tbps of any-to-any, nonblocking, half-duplex) switching. The chassis with SIB-I-PTX5008 provides an 8+1 active redundancy that supports linerate for all the eight FPC slots.

  [See Fabric Fault Handling Overview on PTX5000 Packet Transport Router]
- **Enhanced midplane (PTX5000)**—Starting in Junos OS Release 14.1, the PTX5000 supports a new enhanced midplane. The PTX5000BASE2 model is a chassis with an enhanced midplane that requires high capacity 60-A DC PDUs and PSMs. The enhanced midplane is identified as **Midplane-8Se** in the output from the **show chassis hardware** operational-mode CLI command.

Interfaces and Chassis

- **Support for physical interface damping (PTX Series)**—Beginning with Junos OS Release 14.1, interface damping is supported on *physical interfaces* to address periodic flaps with long up and down durations (in seconds) as opposed to instantaneous multiple flaps with very short up and down durations (in milliseconds) addressed by the Interface hold timers. When the interface is placed in the suppressed state, the interface link state is set to down. Interface event damping uses an exponential back-off algorithm to suppress interface up and down event reporting to the upper-level protocols. To configure interface damping, include the **damping** statement at the **[edit interfaces *interface-name*]** hierarchy level. You use the **show interfaces extensive** command to view the interface damping values and link state.
- **Adaptive load balancing (ALB) for aggregated Ethernet bundles (PTX Series)**—ALB evenly distributes data flows across aggregated Ethernet member links. Network administrators use this feature to manage uneven or overloaded data flows on member links. ALB supports up to 32 member links and up to 50 aggregated Ethernet bundles. The algorithm determines which link to use by considering the scanned packet or bit rate associated with each hash value in conjunction with the mapping of hash values to a given link. ALB is applied to IPv4, IPv6, and MPLS packet headers. ALB is disabled by default.

  

  NOTE: ALB is not applied to multicast traffic.

To configure ALB, include the **adaptive** statement at the **[edit interfaces *ae-interface* aggregated-ether-options load-balance]** hierarchy level. Under the adaptive statement, you can set the following ALB options: tolerance percentage, scan-interval, and pps.

[See Configuring Aggregated Ethernet Interfaces on PTX Series Packet Transport Routers.]

- **SFPP-10G-CT50-ZR (PTX Series)**—The SPFF-10G-CT50-ZR tunable transceiver provides a duplex LC connector and supports the 10GBASE-Z optical interface specification and monitoring. The transceiver is not specified as part of the 10-Gigabit Ethernet standard and is instead built according to Juniper Networks specifications. Only WAN-PHY and LAN-PHY modes are supported. To configure the wavelength on the transceiver, use the **wavelength** statement at the **[edit interfaces *interface-name* optics-options]** hierarchy level. The following interface modules support the SPFF-10G-CT50-ZR transceiver:

  PTX Series:

  - 10-Gigabit Ethernet LAN/WAN OTN PIC with SFP+ (model number: P1-PTX-24-10G-W-SFPP)—Supported in Junos OS Release 13.2R3, 13.3R2, 14.1, and later

  For more information about interface modules, see the "Cables and Connectors" section in the *Interface Module Reference* for your router.

  [See 10-Gigabit Ethernet 10GBASE Optical Interface Specifications and wavelength]

- **SFPP-10G-ZR-OTN-XT (PTX Series)**—The SFPP-10G-ZR-OTN-XT dual-rate extended temperature transceiver provides a duplex LC connector and supports the 10GBASE-Z optical interface specification and monitoring. The transceiver is not specified as part of the 10-Gigabit Ethernet standard and is instead built according to ITU-T and Juniper Networks specifications. The following interface modules support the SFPP-10G-ZR-OTN-XT transceiver:

  PTX Series:

  - 10-Gigabit Ethernet PIC with SFP+ (model number: P1-PTX-24-10GE-SFPP)—Supported in Junos OS Release 12.3R5, 13.2R3, 13.3, and later
  - 10-Gigabit Ethernet LAN/WAN OTN PIC with SFP+ (model number: P1-PTX-24-10G-W-SFPP)—Supported in Junos OS Release 12.3R5, 13.2R3, 13.3, and later

  For more information about interface modules, see the "Cables and Connectors" section in the *Interface Module Reference* for your router.

  [See 10-Gigabit Ethernet 10GBASE Optical Interface Specifications.]

- **New Flexible PIC Concentrator (FPC) model number FPC-SFF-PTX-T (PTX3000)**—Starting in Junos OS Release 14.1, a new FPC is supported on the PTX3000. The FPC-SFF-PTX-T does not interoperate with other Type 5 FPCs in the same chassis. The FPC-SFF-PTX-T model has a 10ms RTT buffer capacity and does not support IPv6 or IP multicast features.

[See PTX3000 FPCs Supported.]

- **Support for high-density FPC (PTX5000)**—Starting with Junos OS Release 14.1, a new high-density FPC, FPCE (model number: FPC2-PTX-P1A), is supported on the PTX5000. This FPC has eight Packet Forwarding Engines and a forwarding capacity of 9600 million packets per second (Mpps).

  Table 1 on page 67 provides information regarding the Type 5 PICs that are supported on the FPC2-PTX-P1A FPC:

Table 1: Type 5 PICs Supported on FPC2-PTX-P1A

Type 5 PIC	PIC Model Number
10-Gigabit Ethernet PIC with SFP+	P1-PTX-24-10GE-SFPP
10-Gigabit Ethernet LAN/WAN OTN PIC with SFP+	P1-PTX-24-10G-W-SFPP
100-Gigabit DWDM OTN PIC	P1-PTX-2-100G-WDM
100-Gigabit Ethernet PIC with CFP2	P2-100GE-CFP2

To meet the increased power requirements of the high-density FPC, the following new power distribution unit (PDU) and power supply module (PSM) are supported on the PTX5000:

- PTX High Capacity 60A DC PDU (PDU2-PTX-DC)
- PTX High Capacity 60A DC PSM (PSM2-PTX-DC)

NOTE: **The PTX High Capacity 60A DC PDU can support a maximum of eight PSMs.**

[See *PTX5000 FPCs Supported*.]

MPLS

- **Require BFD-triggered Packet Forwarding Engine local repair (PTX Series)**—Starting in Junos OS Release 14.1, this feature enables you to configure BFD and MPLS ping for fast-failure detection without relying on fast physical level detection. With links between routers, when a route goes down, the local Packet Forwarding Engine does a local repair and traffic is quickly re-routed around the broken link. The RPD is then informed of the down link and does a global repair and pushes down the updated route information to all other FPCs.

  [See PTX Series Packet Transport Routers.]

- **Link protection for MLDP**—Beginning in Junos OS Release 14.1, link protection for MLDP is supported to enable fast reroute of traffic carried over LDP LSPs in case of a link failure. LDP point-to-multipoint LSPs can be used to send traffic from a single root or

ingress node to a number of leaf nodes or egress nodes traversing one or more transit nodes. When one of the links of the point-to-multipoint tree fails, the subtrees may get detached until the IGP reconverges and MLDP initiates label mapping using the best path from the downstream to the new upstream router. To protect the traffic in the event of a link failure, you can configure an explicit tunnel so that traffic can be rerouted using the tunnel. Junos OS supports make-before-break (MBB) capabilities to ensure minimum packet loss when attempting to signal a new LSP path before tearing down the old LSP path. This feature also adds targeted LDP support for MLDP link protection.

[See Example: Configuring LDP Link Protection.]

- **Entropy label and FAT label support (PTX Series)**—Starting in Release 14.1, the Junos OS supports entropy labels and Flow Aware Transport for Psuedowires (FAT) labels. Entropy label and FAT label when configured on the label-switching routers (LSRs) and label edge routers (LEs) perform load-balancing of MPLS packets across equal-cost multipath (ECMP) paths or link aggregation groups (LAG) without the need for deep packet inspection of the payload.

  In Junos OS Release 14.1, entropy labels can be used for RSVP-signaled label-switched paths (LSPs) and point-to-point LDP-signaled LSPs. FAT flow labels can be used for LDP-signaled forwarding equivalence class (FEC 128 and FEC 129) pseudowires for virtual private LAN service (VPLS) and virtual private wire service (VPWS) networks.

  [See Configuring the Entropy Label for LSPs and FAT Flow Labels Overview.]

Network Management and Monitoring

- **SNMP notifying target for removed notify target configuration (PTX Series)**—Beginning with Junos OS Release 14.1, when a trap target is deleted from Juniper Networks devices, either a syslog event or a syslog trap is generated as per the user configuration. The existing SNMP trap **jnxSyslogTrap** is sent to all target network management systems (NMSs) specified in the SNMP agent including the target NMS, which is being deleted. By default, in the event of target deletion, only a syslog event is generated. To trigger a trap on deletion of a trap target, configure a syslog event policy, which sends the syslog as a trap to the network management systems.

Routing Protocols

- **Selecting backup LFA for IS-IS routing protocol (PTX Series)**—Starting with Junos OS Release 14.1, the default loop-free alternate (LFA) selection algorithm or criteria can be overridden with an LFA policy. These policies are configured for each destination (IPv4 and IPv6) and a primary next-hop interface. These backup policies enforce LFA selection based on admin-group, srlg, neighbor, neighbor-tag, bandwidth, protection-type, and metric attributes of the backup path. During backup shortest-path-first (SPF) computation, each attribute (both node and link) of the backup path, stored per backup-next hop, is accumulated by IGP. For the routes created internally by IGP, the attribute set of every backup path is evaluated against the policy configured per destination per prefix primary next-hop interface. The first or the best backup path is selected and installed as the backup next hop in the routing table. To configure the backup selection policy, include the **backup-selection** configuration statement at the **[edit routing-options]** hierarchy level. The **show backup-selection** command displays the configured policies for a given interface and destination. The display can be filtered against a particular destination, prefix, interface, or logical systems.

Related Documentation

- Changes in Behavior and Syntax on page 69
- Known Behavior on page 70
- Known Issues on page 70
- Documentation Updates on page 71
- Migration, Upgrade, and Downgrade Instructions on page 71
- Product Compatibility on page 74

Changes in Behavior and Syntax

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 14.1R1 for the PTX Series.

- VPNs on page 70

VPNs

- **Support for chained composite next hops for Layer 3 VPN transit traffic (PTX Series)**—Starting in Junos OS Release 14.1, on PTX Series Packet Transport Routers only, chained composite next hops for Layer 3 VPN transit traffic are enabled by default. You no longer need to configure the **transit l3pvn** statement at the **[edit routing-options forwarding-table chained-composite-next-hop]** hierarchy level. You should continue to configure this statement on MX Series 3D Universal Edge Routers to enable chained composite next hops for Layer 3 VPN transit traffic. Chained composite next hops facilitate the handling of large volumes of transit traffic in the core of large networks.

  [See *Chained Composite Next Hops for Transit Devices*.]

Related Documentation

- New and Changed Features on page 64
- Known Behavior on page 70
- Known Issues on page 70
- Documentation Updates on page 71
- Migration, Upgrade, and Downgrade Instructions on page 71
- Product Compatibility on page 74

Known Behavior

There are no changes in known behavior in Junos OS Release 14.1R1 for the PTX Series.

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

Related Documentation

- New and Changed Features on page 64
- Changes in Behavior and Syntax on page 69
- Known Issues on page 70
- Documentation Updates on page 71
- Migration, Upgrade, and Downgrade Instructions on page 71
- Product Compatibility on page 74

Known Issues

There are no known issues in hardware and software in Junos OS Release 14.1R1 for the PTX Series.

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

Related Documentation

- New and Changed Features on page 64
- Changes in Behavior and Syntax on page 69

Documentation Updates

There are no outstanding issues with the published documentation for Junos OS Release 14.1R1 for the PTX Series.

Related Documentation

- New and Changed Features on page 64
- Changes in Behavior and Syntax on page 69
- Known Behavior on page 70
- Known Issues on page 70
- Migration, Upgrade, and Downgrade Instructions on page 71
- Product Compatibility on page 74

Migration, Upgrade, and Downgrade Instructions

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS for the PTX Series. Upgrading or downgrading Junos OS can take several hours, depending on the size and configuration of the network.

Upgrading Using Unified ISSU

Unified in-service software upgrade (ISSU) enables you to upgrade between two different Junos OS releases with no disruption on the control plane and with minimal disruption of traffic. Unified in-service software upgrade is only supported by dual Routing Engine platforms. In addition, graceful Routing Engine switchover (GRES) and nonstop active routing (NSR) must be enabled. For additional information about using unified in-service software upgrade, see the High Availability Feature Guide for Routing Devices.

NOTE: **Unified ISSU on the PTX5000 does not support upgrades from Junos OS Release 13.3 to Junos OS Release 14.1. Upgrading from Junos OS Release 13.3 to Junos OS Release 14.1 will break the unified ISSU process.**

Upgrading a Router with Redundant Routing Engines

If the router has two Routing Engines, perform a Junos OS installation on each Routing Engine separately to avoid disrupting network operation as follows:

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

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

Basic Procedure for Upgrading to Release 14.1R1

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

NOTE: Back up the file system and the currently active Junos OS configuration before upgrading Junos OS. This allows you to recover to a known, stable environment if the upgrade is unsuccessful. Issue the following command:

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

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

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.

The download and installation process for Junos OS Release 14.1 is different from previous Junos OS releases.

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

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

2. Select the name of the Junos OS platform for the software that you want to download.
3. Select the release number (the number of the software version that you want to download) from the **Release** drop-down list to the right of the Download Software page.
4. Select the **Software** tab.
5. In the **Install Package** section of the **Software** tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new **jinstall** package on the router.

    NOTE: After you install a Junos OS Release 14.1 jinstall package, you cannot issue the request system software rollback command to return to the previously installed software. Instead you must issue the request system software add validate command and specify the jinstall package that corresponds to the previously installed software.

    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.

    Customers in the United States and Canada, use the following command:

    ```
    user@host> request system software add validate reboot
    source/jinstall-14.1R11-domestic-signed.tgz
    ```

All other customers, use the following command:

```
user@host> request system software add validate reboot
source/jinstall-14.1R11-export-signed.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 14.1 **jinstall** package, you cannot issue the **request system software rollback** command to return to the previously installed software. Instead you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

Related Documentation

- New and Changed Features on page 64
- Changes in Behavior and Syntax on page 69
- Known Behavior on page 70
- Known Issues on page 70
- Documentation Updates on page 71
- Product Compatibility on page 74

Product Compatibility

- Hardware Compatibility on page 75

Hardware Compatibility

To obtain information about the components that are supported on the devices, and special compatibility guidelines with the release, see the Hardware Guide and the Interface Module Reference for the product.

To determine the features supported on PTX Series devices in this release, use the Juniper Networks Feature Explorer, a Web-based application that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. Find Feature Explorer at: http://pathfinder.juniper.net/feature-explorer/

Related Documentation

- New and Changed Features on page 64
- Changes in Behavior and Syntax on page 69
- Known Behavior on page 70
- Known Issues on page 70
- Documentation Updates on page 71
- Migration, Upgrade, and Downgrade Instructions on page 71

Finding More Information

For the latest, most complete information about known and resolved issues with Junos OS, see the Juniper Networks Problem Report Search application at: http://prsearch.juniper.net .

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos OS feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: http://pathfinder.juniper.net/feature-explorer/.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at: http://www.juniper.net/techpubs/content-applications/content-explorer/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/ . If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need postsales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/customers/support/downloads/710059.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.
- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: http://kb.juniper.net/InfoCenter/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool located at https://tools.juniper.net/SerialNumberEntitlementSearch/.

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/ .
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, visit us at http://www.juniper.net/support/requesting-support.html .

If you are reporting a hardware or software problem, issue the following command from the CLI before contacting support:

```
user@host> request support information | save filename
```

To provide a core file to Juniper Networks for analysis, compress the file with the **gzip** utility, rename the file to include your company name, and copy it to **ftp.juniper.net/pub/incoming**. Then send the filename, along with software version information (the output of the **show version** command) and the configuration, to **support@juniper.net**. For documentation issues, fill out the bug report form located at https://www.juniper.net/cgi-bin/docbugreport/.

Revision History

24 July 2014—Revision 6, Junos OS Release 14.1R1– EX Series, M Series, MX Series, PTX Series, and T Series.

18 July 2014—Revision 5, Junos OS Release 14.1R1– EX Series, M Series, MX Series, PTX Series, and T Series.

15 July 2014—Revision 4, Junos OS Release 14.1R1– EX Series, M Series, MX Series, PTX Series, and T Series.

26 June 2014—Revision 3, Junos OS Release 14.1R1– EX Series, M Series, MX Series, PTX Series, and T Series.

19 June 2014—Revision 2, Junos OS Release 14.1R1– EX Series, M Series, MX Series, PTX Series, and T Series.

12 June 2014—Revision 1, Junos OS Release 14.1R1– EX Series, M Series, MX Series, PTX Series, and T Series.