INSIDE THIS RELEASE

- Supported on EX Series, MX Series, PTX Series, QFX Series, T Series, and Junos Fusion

NEW HARDWARE FEATURES

- New line cards for EX9200 switches
- New Routing Engine RE-PTX-X8-64G (PTX5000)

NEW SOFTWARE FEATURES

- Junos Fusion Enterprise
  - Configuration to keep an aggregated Ethernet link in an MC-LAG up for a peer with limited LACP capability (EX9200)
  - Configuration consistency check for multichassis link aggregation groups (EX9200)
- Support for Layer 2 VPNs (EX9200)
- Support for suppressing the default classifier (MX Series)
- Active-active multihoming for EVPN (MX Series with MPCs and MICs only)
- High availability for IPsec on MS-MPCs
- Clock Synchronization feature support on non-Ethernet MICs
- Support to monitor physical Ethernet links, detect link degradation, and trigger fast-reroute to minimize packet loss (MX Series)
- Feature to improve MC-LAG Layer 2 and Layer 3 convergence (MX Series)
- LACP hold-up timer configuration support on LAG interfaces
- Asynchronous notification on MIC-BOC3OC12-4OC48-SFP and MIC-1OC192-HO-VC-XFP (MX Series)
- Configuration for multiple up MEPs for interfaces belonging to a single VPLS service or a bridge domain (MX Series with MPC)
- JET for Junos provides a modern programmatic interface for developers of third-party applications
- Protection against incorrect label injection across ASBRs (MX Series)
- Leaking MPLS routes to nondefault routing instances (MX Series with MPC/MIC interfaces)
- Improved scaling for multicast OIFs (MX Series)
- New load-balancing options using source or destination IP address only (MX Series)
- New route-filter-list and source-address-filter-list configuration statements (MX Series)
- Support for inline video monitoring on MPC5 and MPC6 (MX Series routers)
- MVPN source-active upstream multicast hop selection and redundant source improvements (MX Series)
- MPLS-TP enhancements for on-demand connectivity verification (PTX Series)
- Support for shaping of the traffic exiting a physical interface (PTX Series)
Release Notes: Junos® OS Release 16.1R1 for the EX Series, MX Series, PTX Series, QFX Series, T Series, and Junos Fusion
Junos OS Release 16.1R1

1 September 2016

Contents

Introduction ................................................................. 7
Junos OS Release Notes for EX Series Switches .............................. 8
New and Changed Features ............................................. 8
  Hardware ................................................................. 9
  Authentication, Authorization, and Accounting ...................... 9
  Interfaces and Chassis ................................................ 10
  Management ............................................................ 11
  Multicast .............................................................. 11
  Network Management and Monitoring ................................ 12
  Port Security .......................................................... 12
  Routing Policy and Firewall Filters .................................. 13
  Software-Defined Networking ....................................... 14
  User Interface and Configuration ................................... 14
  VPNs .................................................................. 14
Changes in Behavior and Syntax .......................................... 15
  General Routing ......................................................... 15
  Security ................................................................. 15
  User Interface and Configuration ................................... 16
Known Behavior .............................................................. 16
Layer 2 Features ............................................................ 16
Known Issues ................................................................ 17
  Authentication, Authorization, and Accounting .................. 17
  High Availability and Resiliency ..................................... 17
  Interface and Chassis .................................................. 18
  IP Address Management .............................................. 18
  Multicast .............................................................. 18
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Analytics</td>
<td>18</td>
</tr>
<tr>
<td>Port Security</td>
<td>18</td>
</tr>
<tr>
<td>Software Installation and Upgrade</td>
<td>18</td>
</tr>
<tr>
<td>Documentation Updates</td>
<td>19</td>
</tr>
<tr>
<td>NETCONF XML Management Protocol Developer Guide</td>
<td>19</td>
</tr>
<tr>
<td>Migration, Upgrade, and Downgrade Instructions</td>
<td>19</td>
</tr>
<tr>
<td>Upgrade and Downgrade Support Policy for Junos OS Releases</td>
<td>19</td>
</tr>
<tr>
<td>Product Compatibility</td>
<td>20</td>
</tr>
<tr>
<td>Hardware Compatibility</td>
<td>20</td>
</tr>
<tr>
<td>Junos OS Release Notes for Junos Fusion Enterprise</td>
<td>21</td>
</tr>
<tr>
<td>New and Changed Features</td>
<td>21</td>
</tr>
<tr>
<td>Junos Fusion Enterprise</td>
<td>22</td>
</tr>
<tr>
<td>Changes in Behavior and Syntax</td>
<td>23</td>
</tr>
<tr>
<td>General Routing</td>
<td>23</td>
</tr>
<tr>
<td>Known Behavior</td>
<td>24</td>
</tr>
<tr>
<td>Junos Fusion</td>
<td>24</td>
</tr>
<tr>
<td>Known Issues</td>
<td>24</td>
</tr>
<tr>
<td>Interfaces and Chassis</td>
<td>25</td>
</tr>
<tr>
<td>Layer 2 Features</td>
<td>25</td>
</tr>
<tr>
<td>Network Management and Monitoring</td>
<td>26</td>
</tr>
<tr>
<td>Platform and Infrastructure</td>
<td>26</td>
</tr>
<tr>
<td>Documentation Updates</td>
<td>26</td>
</tr>
<tr>
<td>Migration, Upgrade, and Downgrade Instructions</td>
<td>27</td>
</tr>
<tr>
<td>Basic Procedure for Upgrading Junos OS on an Aggregation Device</td>
<td>27</td>
</tr>
<tr>
<td>Upgrading an Aggregation Device with Redundant Routing Engines</td>
<td>29</td>
</tr>
<tr>
<td>Preparing the Switch for Satellite Device Conversion</td>
<td>29</td>
</tr>
<tr>
<td>Converting a Satellite Device to a Standalone Switch</td>
<td>30</td>
</tr>
<tr>
<td>Upgrade and Downgrade Support Policy for Junos OS Releases</td>
<td>32</td>
</tr>
<tr>
<td>Downgrading from Release 16.1</td>
<td>32</td>
</tr>
<tr>
<td>Product Compatibility</td>
<td>33</td>
</tr>
<tr>
<td>Hardware and Software Compatibility</td>
<td>33</td>
</tr>
<tr>
<td>Junos OS Release Notes for Junos Fusion Provider Edge</td>
<td>34</td>
</tr>
<tr>
<td>New and Changed Features</td>
<td>34</td>
</tr>
<tr>
<td>Hardware</td>
<td>34</td>
</tr>
<tr>
<td>Multicast</td>
<td>34</td>
</tr>
<tr>
<td>Changes in Behavior and Syntax</td>
<td>36</td>
</tr>
<tr>
<td>Known Behavior</td>
<td>36</td>
</tr>
<tr>
<td>Junos Fusion</td>
<td>37</td>
</tr>
<tr>
<td>Known Issues</td>
<td>37</td>
</tr>
<tr>
<td>Junos Fusion</td>
<td>37</td>
</tr>
<tr>
<td>Satellite Software</td>
<td>37</td>
</tr>
<tr>
<td>Resolved Issues</td>
<td>38</td>
</tr>
<tr>
<td>Documentation Updates</td>
<td>38</td>
</tr>
<tr>
<td>Migration, Upgrade, and Downgrade Instructions</td>
<td>39</td>
</tr>
<tr>
<td>Basic Procedure for Upgrading an Aggregation Device</td>
<td>39</td>
</tr>
<tr>
<td>Upgrading an Aggregation Device with Redundant Routing Engines</td>
<td>41</td>
</tr>
<tr>
<td>Preparing the Switch for Satellite Device Conversion</td>
<td>42</td>
</tr>
<tr>
<td>Autoconverting a Switch into a Satellite Device</td>
<td>43</td>
</tr>
<tr>
<td>Manually Converting a Switch into a Satellite Device</td>
<td>45</td>
</tr>
</tbody>
</table>
Configuring a Switch into a Satellite Device Before Connecting It to a
Junos Fusion Topology ........................................... 47
Configuring Satellite Device Upgrade Groups .................. 48
Converting a Satellite Device to a Standalone Device ........ 49
Upgrade and Downgrade Support Policy for Junos OS Releases .... 51
Downgrading from Release 16.1 ................................. 52
Product Compatibility .............................................. 52
Hardware Compatibility .......................................... 52
Junos OS Release Notes for MX Series 3D Universal Edge Routers and T Series
Core Routers ....................................................... 53
New and Changed Features ........................................ 53
Hardware ............................................................. 54
Authentication, Authorization, and Accounting .................. 56
Class of Service (CoS) ............................................. 56
EVPNs ................................................................. 57
General Routing ..................................................... 58
High Availability and Resiliency .................................... 59
Interfaces and Chassis .............................................. 60
IPv4 ................................................................. 68
Junos OS XML API and Scripting .................................. 68
Layer 2 Features ................................................... 68
Management ......................................................... 69
MPLS ................................................................. 70
Multicast ............................................................. 75
Network Management and Monitoring .............................. 76
Operation Administration and Management ...................... 78
Routing Policy and Firewall Filters ................................. 81
Routing Protocols ................................................... 82
Security ............................................................... 85
Services Applications ............................................... 86
Software Installation and Upgrade .................................. 89
Software Defined Networking ..................................... 91
Subscriber Management and Services ............................. 92
System Logging ..................................................... 103
System Management ................................................ 104
Timing and Synchronization ....................................... 104
User Interface and Configuration .................................... 104
Virtual Chassis ....................................................... 105
VPNs ................................................................. 105
Changes in Behavior and Syntax .................................... 107
General Routing ..................................................... 107
Interfaces and Chassis .............................................. 108
Junos FIPS .......................................................... 108
Junos OS XML API and Scripting ................................. 109
Layer 2 Features ................................................... 109
MPLS ................................................................. 110
Network Management and Monitoring ............................. 110
Routing Policy and Firewall Filters ................................ 111
Routing Protocols ................................................... 111
Security .......................................................... 112
Services Applications ........................................ 114
Software Installation and Upgrade ......................... 115
Subscriber Management and Services (MX Series) .... 115
System Logging .................................................. 120
System Management ........................................... 120
User Interface and Configuration ............................ 120
Known Behavior .................................................. 121
Bridging and Learning ........................................ 121
General Routing ................................................ 121
MPLS .............................................................. 122
Routing Protocols .............................................. 122
Software Installation and Upgrade ......................... 122
Subscriber Management and Services ................. 122
System Logging .................................................. 123
VPNs ............................................................... 123
Known Issues .................................................... 124
Forwarding and Sampling .................................... 125
General Routing ................................................ 125
Interfaces and Chassis ........................................ 126
Layer 2 Features ............................................... 127
MPLS .............................................................. 127
Platform and Infrastructure .................................. 127
Provider Edge Satellite Software ......................... 128
Routing Protocols .............................................. 128
Services Applications ....................................... 128
Software Installation and Upgrade ......................... 129
VPNs ............................................................... 129
Resolved Issues ............................................... 129
Resolved Issues: 16.1R1 ....................................... 129
Documentation Updates ..................................... 132
NETCONF XML Management Protocol Developer Guide .... 132
Security Services Administration Guide .................. 132
SNMP MIBs and traps reference ........................... 133
Syslog Reference Guide ..................................... 133
Standards Reference ......................................... 133
Subscriber Management Provisioning Guide .......... 133
Migration, Upgrade, and Downgrade Instructions ..... 134
Basic Procedure for Upgrading to Release 16.1 ......... 134
Upgrading from Junos OS (FreeBSD 6.1) to Junos OS (FreeBSD 10.x) ........................................ 136
Upgrading from Junos OS (FreeBSD 6.1) to Junos OS (FreeBSD 6.1) ........................................ 137
Upgrading from Junos OS (FreeBSD 6.1) to Junos OS (FreeBSD 6.1) ........................................ 137
Upgrade and Downgrade Support Policy for Junos OS Releases ........................................... 139
Upgrading a Router with Redundant Routing Engines ........................................... 139
Upgrading Juniper Network Routers Running Draft-Rosen Multicast VPN to Junos OS Release 10.1 ........................................... 140
Downgrading from Release 16.1 ............................ 141
Product Compatibility ........................................... 142
Hardware Compatibility .................................... 142
Introduction

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

These release notes accompany Junos OS Release 16.1R1 for the EX Series, MX Series, PTX Series, QFX Series, T Series and Junos Fusion. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

NOTE: The following MX features are not supported in Junos OS Release 16.1R1:

- CLNS
- ISSU
- J-Web
- PTP
- Subscriber Management and Services
- Virtual Chassis
- VXLAN
Junos OS Release Notes for EX Series Switches

These release notes accompany Junos OS Release 16.1R1 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 on page 8
- Changes in Behavior and Syntax on page 15
- Known Behavior on page 16
- Known Issues on page 17
- Documentation Updates on page 19
- Migration, Upgrade, and Downgrade Instructions on page 19
- Product Compatibility on page 20

New and Changed Features

This section describes the new features in Junos OS Release 16.1R1 for the EX Series switches.

NOTE: The following EX Series switches are supported in Release 16.1R1: EX4300, EX4600, and EX9200.

NOTE: A new J-Web distribution model was introduced in Junos OS Release 14.1X53-D10, and that same model is supported in Release 16.1R1 and later. The model provides two packages:

- Platform package—Installed as part of Junos OS; provides basic functionalities of J-Web.
- Application package—Optionally installable package; provides complete functionalities of J-Web.

In Junos OS Release 16.1R1, J-Web is supported on the EX4300 and EX4600 Series switches in both standalone and Virtual Chassis setup.


- Hardware on page 9
- Authentication, Authorization, and Accounting on page 9
- Interfaces and Chassis on page 10
- Management on page 11
• Multicast on page 11
• Network Management and Monitoring on page 12
• Port Security on page 12
• Routing Policy and Firewall Filters on page 13
• Software-Defined Networking on page 14
• User Interface and Configuration on page 14
• VPNs on page 14

Hardware

• New line cards for EX9200 switches—Starting with Junos OS Release 16.1R1, EX9200 switches support the following new line cards:
  
  EX9200-12QS line card: It is a line card with 12 Gigabit Ethernet rate-selectable ports, each of which can house transceivers. These ports can operate at 10-Gbps, 40-Gbps, and 100-Gbps speeds. [See EX9200-12QS Line Card.]

  EX9200-40XS line card: It is a line card with 40 10-Gigabit Ethernet ports with Media Access Control Security (MACsec) capability, each of which can house 10-gigabit small form-factor plus pluggable (SFP+) transceivers. [See EX9200-40XS Line Card.]

Authentication, Authorization, and Accounting

• Additional attributes for RADIUS accounting (EX4300)—Starting with Junos OS Release 16.1R1, additional RADIUS accounting attributes are supported on EX4300 switches. RADIUS accounting attributes are included in Accounting Request messages sent from a network access server (NAS) to the RADIUS accounting server. These RADIUS accounting attributes contain user accounting information that is used for keeping network statistics and for general network monitoring. The following additional attributes are supported: Client-System-Name, Framed-MTU, Session-Timeout, Acct-Authentic, NAS-Port-ID, and Filter-ID. There is no configuration required for enabling these attributes.

  [See Understanding 802.1X and RADIUS Accounting on EX Series Switches.]

• Liveness detection for captive portal (EX4300)—Starting with Junos OS Release 16.1R1, you can configure a keep-alive timer to extend a captive portal authentication session after the MAC table aging timer expires. The keep-alive timer starts when the MAC address of the authenticated host ages out of the Ethernet switching table. If traffic is received within the keep-alive period, the timer stops and the authenticated session remains active. If there is no traffic within the keep-alive period, the authenticated session ends, and the host must re-authenticate.

  [See Understanding Authentication Session Timeout.]
**Interfaces and Chassis**

- **Configuration support to keep an aggregated Ethernet link in an MC-LAG up for a peer that has limited LACP capability (EX9200)**—Starting with Junos OS Release 16.1R1, you can configure an aggregated Ethernet link or an interface in an MC-LAG topology to remain up even when the peer link or peer interface has limited Link Access Control Protocol (LACP) capability.

  To enable this feature, configure the `force-up` statement at the `[edit interfaces interface-name ether-options 802.3ad lacp]` hierarchy level.

  [See Forcing MC-LAG Links or Interfaces with Limited LACP Capability to Be Up.]

- **Configuration consistency check for multichassis link aggregation groups (EX9200)**—Starting with Junos OS Release 16.1R1, use configuration consistency checks, which are enabled by default, to find configuration-parameter inconsistencies between multichassis link aggregation group (MC-LAG) peers. Severe inconsistencies prevent MC-LAG interfaces from coming up; the interfaces come up after you correct those inconsistencies. Moderate inconsistencies generate error messages, and you can optionally fix those inconsistencies. At each commit, the configuration on each MC-LAG peer is checked. Use `show multichassis configuration-consistency list-of-parameters` to view which parameters are checked and which parameters must be configured identically or uniquely across MC-LAG peers. Use `show multichassis configuration-consistency redundancy-group-id redundancy-group-id (global | icl | mc-ae-id mc-ae-id)` to see the consistency status for a given mc-ae ID. See Understanding Multichassis Link Aggregation Group Configuration Consistency Check for more information.

- **Configuration synchronization for multichassis link aggregation groups (EX9200)**—Starting with Junos OS Release 16.1R1, multichassis link aggregation group (MC-LAG) configuration synchronization enables you to easily propagate, synchronize, and commit configurations from one MC-LAG peer to another. Log in to either peer to manage both, and use configuration groups to simplify the configuration process. You can create one configuration group each for the local peer and the remote peer, and a global configuration common to both peers.

  Create conditional groups to specify when peer configurations are synchronized. Enable `peers-synchronize` at the `[edit system commit]` hierarchy to synchronize configurations and commits across peers by default. NETCONF over SSH provides a secure connection between peers; Secure Copy Protocol (SCP) copies configurations securely between them.

- **A limited encryption Junos OS image, Junos Limited, created for customers in Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia (EX9200)**—Starting with Junos OS Release 16.1R1, customers in the Eurasian Customs Union (comprising Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) must use the limited encryption Junos OS image, Junos Limited, instead of the Junos Worldwide image, on EX9200 switches. The Junos Limited image does not have data-plane encryption and is intended only for countries in the Eurasian Customs Union, because these countries have import restrictions on software that has data-plane encryption. Unlike the Junos Worldwide image, the Junos Limited image supports control-plane encryption through the protocols SSH and SSL, thus enabling secure management of the system.
NOTE: Customers in Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia must use the limited encryption Junos Limited image. Customers in all other countries must use the Junos image, introduced in Release 15.1R1 to replace the Junos Domestic image.

Management

- **YANG module that defines Junos OS operational commands (EX9200)**—Starting with Junos OS Release 16.1, Juniper Networks provides the juniper-command YANG module, which represents the operational command hierarchy and collective group of modules that define the remote procedure calls (RPCs) for Junos OS operational mode commands. You can download Juniper Networks YANG modules from the website, or you can generate the modules by using the `show system schema format yang module juniper-command` operational command on the local device. The `juniper-command` module is bound to the namespace URI http://yang.juniper.net/yang/1.1/jrpc and uses the prefix `jrpc`.

  [See Understanding the Juniper Networks YANG Modules for Operational Commands.]

- **YANG module that defines CLI formatting for RPC output (EX9200)**—Starting with Junos OS Release 16.1, Juniper Networks provides the junos-extension-odl YANG module. The module contains definitions for Junos OS Output Definition Language (ODL) statements, which determine the CLI formatting for RPC output when you execute the operational command corresponding to that RPC in the CLI or when you request the RPC output in text format. You can use statements in the `junos-extension-odl` module in custom RPCs to convert the XML output into a more logical and human-readable representation of the data. The `junos-extension-odl` module is bound to the namespace URI http://yang.juniper.net/yang/1.1/jodl and uses the prefix `junos-odl`.

  [See Understanding Junos OS YANG Extensions for Formatting RPC Output.]

Multicast

- **MLD snooping versions 1 and 2 (EX4300)**—Starting with Junos OS Release 16.1R1, EX4300 switches support Multicast Listener Discovery (MLD) snooping version 1 (MLDv1) and version 2 (MLDv2). MLD snooping constrains the flooding of IPv6 multicast traffic on VLANs. When MLD snooping is enabled on a VLAN, an EX4300 switch examines MLD messages between hosts and multicast routers and learns which hosts are interested in receiving traffic for a multicast group. On the basis of what it learns, the switch forwards multicast traffic only to those interfaces in the VLAN that are connected to interested receivers instead of flooding the traffic to all interfaces.

- **IPv6 PIM support (EX4300)**—Starting with Junos OS Release 16.1R1, EX4300 switches support Protocol Independent Multicast (PIM) for IPv6. The EX4300 switches support the following IPv6 PIM modes:
  - Sparse mode
  - Dense mode
Sparse-dense mode
Source-specific mode (SSM)

PIM sparse mode supports the following rendezvous point (RP) functionality:

- Static RP addresses
- Bootstrap routers
- Automatic RP announcement and discovery
- Embedded RPs
- Anycast RP

[See PIM Overview.]

Network Management and Monitoring

- **Sampling VXLAN traffic (EX9200)**—Starting with Junos OS Release 16.1R1, on EX9200 switches, you can use sFlow technology to sample 128 bytes of a VXLAN packet starting from the outer IP header. When configuring sFlow technology, you must specify an interface on which VXLAN packets enter or exit.

  - Ingress packets sampled before encapsulation—At this stage, sampled packets do not have an outer IP header. Outer Layer 2, Layer 3, and VXLAN network identifier (VNI) information are added to the packets as an sFlow extended header.

  - Ingress packets sampled before de-encapsulation—At this stage, sampled packets have an outer IP header. An sFlow extended header is added for an inner header offset.

  - Egress packets sampled after encapsulation—At this stage, sampled packets have an outer IP header. An sFlow extended header is added for an inner header offset.

  - Egress packets sampled after de-encapsulation—At this stage, sampled packets do not have an outer IP header. Outer Layer 2, Layer 3, and VNI information are added to the packets as an sFlow extended header.

- **Support for IPv6 for sFlow Monitoring (EX9200)**—Starting with Junos OS Release 16.1R1, on EX9200 switches, sFlow technology supports configuration of IPv6 addresses in addition to the existing IPv4 address support.

Port Security

- **Media Access Control Security (MACsec) support (EX9200 switches)**—Starting with Junos OS Release 16.1R1, MACsec is supported on all SFP and SFP+ interfaces on the EX9200-40XS line card when it is installed in an EX9200 switch. MACsec is an industry-standard security technology that provides secure communication for all traffic on point-to-point Ethernet links. MACsec is capable of identifying and preventing most security threats, and can be used in combination with other security protocols to provide end-to-end network security. MACsec can be enabled only on domestic versions of Junos OS software. MACsec is standardized in IEEE 802.1AE.

[See Understanding Media Access Control Security (MACsec).]
IPv6 Router Advertisement (RA) Guard (EX4300)—Starting with Junos OS Release 16.1 for EX Series switches, IPv6 RA guard is supported on EX4300 switches. RA guard protects networks against rogue RA messages generated either maliciously or unintentionally by unauthorized or improperly configured routers connecting to the network segment. RA guard works by validating RA messages based on whether they meet certain criteria, which is configured on the switch as a policy. RA guard inspects the RA message and compares the information contained in the message attributes to the policy. Depending on the policy, RA guard either drops or forwards the RA messages that match the conditions.

[See Understanding IPv6 Router Advertisement Guard].

Routing Policy and Firewall Filters

Filter-based forwarding for IPv6 traffic (EX4300 switches and EX4300 Virtual Chassis)—Starting with Junos OS Release 16.1R1, standalone EX4300 switches and EX4300 Virtual Chassis support the use of firewall filters in conjunction with virtual routing instances, enabling you to specify different routes for IPv6 traffic to traverse through the network. To set up this feature, called filter-based forwarding, you specify a firewall filter and match criteria and then specify the virtual routing instance to send packets to.

You can use filter-based forwarding to route IPv6 traffic through a firewall or security device before the traffic continues on its path. You can also use filter-based forwarding to give IPv6 traffic preferential treatment or to improve load balancing of switch traffic.

Filtering and policing VXLAN traffic (EX9200)—Starting with Junos OS Release 16.1R1, on EX9200 switches, you can filter and police VXLAN traffic in the following ways:

- Per-VXLAN network identifier (VNI) filtering and policing—You can create a firewall filter that matches the VNI of a VXLAN segment. To rate-limit traffic for the VXLAN segment, you can specify policer as the action in the firewall filter. To rate-limit traffic exiting the VXLAN segment, you must apply the filter to the input traffic for the VXLAN. To rate-limit traffic entering the VXLAN segment, you must apply the filter to the output traffic for the VXLAN.

- Per-virtual tunneling endpoint (VTEP) filtering and policing—To perform per-VTEP filtering, you create a firewall filter with one or more match conditions. In addition, you can create a dynamic profile for each dynamically created VTEP interface to filter input or output traffic. You can also create a default profile for interfaces that are not included in a dynamic profile.

For the packets that match the per-VTEP filter, you can rate-limit the traffic for a dynamically created VTEP interface by specifying policer as the action in the firewall filter.

- Filtering and policing based on outer header—You can create a firewall filter that matches the outer IP and UDP header contents of a VXLAN packet. When configuring this firewall filter, you must specify family inet and apply the filter to an interface on which VXLAN packets enter or exit. For the packets that match the filter, you can rate-limit traffic for the interface by specifying policer as the action in the firewall filter.
Software-Defined Networking

- **Support for ping and traceroute (EX9200) in troubleshooting overlay networks**—Starting with Junos OS Release 16.1, EX9200 switches support overlay ping and traceroute as troubleshooting tools for overlay networks such as Virtual Extensible LANs (VXLANs). For ping and traceroute mechanisms to work in overlay networks, the ping and traceroute packets, also referred to collectively as the Operations, Administration, and Maintenance (OAM) packets, must be encapsulated with the same tunnel headers (outer headers) as the data packets forwarded over the overlay segment. The OAM packets then follow the same path as the data packets for the overlay segment. If any connectivity issues arise in the overlay segment, an OAM packet corresponding to a flow experiences the same connectivity issues as a data packet for that flow. OAM packets can collect detailed information specific to an overlay segment, and as a result, connectivity issues in the overlay network can be better detected.

User Interface and Configuration

- **Support for JSON format for configuration data (EX4300, EX4600, EX9200)**—Starting with Junos OS Release 16.1, you can configure devices running Junos OS using configuration data in JavaScript Object Notation (JSON) format in addition to the existing text, Junos XML, and Junos OS `set` command formats. You can load configuration data in JSON format in the Junos OS CLI by using the `load (merge | override | update) json` command or from within a NETCONF or Junos XML protocol session by using the `<load-configuration format="json">` operation. You can load JSON configuration data either from an existing file or as a data stream. Configuration data that is provided as a data stream must be enclosed in a `<configuration-json>` element.

[See load, Defining the Format of Configuration Data to Upload in a Junos XML Protocol Session, and Mapping Junos OS Configuration Statements to JSON.]

VPNs

- **Support for Layer 2 VPNs (EX9200)**—Starting with Junos OS Release 16.1R1, EX9200 switches support Layer 2 VPNs, allowing you to securely connect geographically diverse sites across an MPLS network. Implementing a Layer 2 VPN on the switch is similar to using other Layer 2 technologies, such as Asynchronous Transfer Mode (ATM) or Frame Relay. However, with Layer 2 VPNs, traffic is forwarded by the customer’s customer edge (CE) switch to the service provider’s provider edge (PE) switch in Layer 2 format. It is carried by MPLS over the service provider’s network and then converted back to Layer 2 format at the receiving site. Layer 2 VPNs provide complete separation between the service provider network and the customer network. This means that provider edge (PE) devices and customer edge (CE) devices do not exchange routing information, giving the customer full control over routing.

[See Layer 2 VPNs Feature Guide for EX9200 Switches.]
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 16.1R1 for the EX Series.

- General Routing on page 15
- Security on page 15
- User Interface and Configuration on page 16

General Routing

- **Enhancement to request support information command**—Starting with Junos OS Release 16.1R1, the `request support information` command is enhanced to capture the following additional details:
  - `file list detail/var/rundb/`—Displays the size of the configuration databases.
  - `show system configuration database usage`—Displays the actual usage of the configuration databases.

  **NOTE:** This information will be displayed only if the `show system configuration database usage` command is supported in the release.

- `file list detail /config/`—Contains the db_ext file and shows the size of it to indicate whether extend_size is enabled or disabled.

- **New option introduced under show | display xml | display**—Starting with Junos OS 16.1R1, you can use the `show | display xml | display | mark-changed` statement to view the `mark-changed` status of the nodes. This is useful for debugging purpose.

- **Modified output of the clear services sessions | display xml command (MX Series)**—In Junos OS Release 16.1, the output of the `clear services sessions | display xml` command is modified to include the `<sess-marked-for-deletion>` tag instead of the `<sess-removed>` tag. In releases before Junos OS Release 14.1X55-D30, the output of this command includes the `<sess-removed>` tag. The replacement of the `<sess-removed>` tag with the `<sess-marked-for-deletion>` tag establishes consistency with the output of the `clear services sessions` command that includes the field Sessions marked for deletion.

Security

- **Changes to DDoS protection protocol group and packet type support (EX 9200)**—Starting with Junos OS Release 16.1, the following changes have been made to the `protocols` statement at the `[edit system ddos-protection]` hierarchy level and to the output of the `show ddos-protection protocols` command:
• Removed the firewall-host protocol group.
• Removed the unclassified packet type from the mcast-snoop protocol group.
• Added the unclassified packet type to the tcp-flags protocol group.

User Interface and Configuration

• New default implementation for serialization for JSON configuration data (EX Series)—Starting with Junos OS Release 16.1, the default implementation for serialization for configuration data emitted in JavaScript Object Notation (JSON) has changed. The new default is as defined in Internet drafts draft-ietf-netmod-yang-json-09, JSON Encoding of Data Modeled with YANG, and draft-ietf-netmod-yang-metadata-06, Defining and Using Metadata with YANG.

[See Mapping Junos OS Configuration Statements to JSON.]

• output-file-name option for show system schema command is deprecated (EX Series)—Starting with Junos OS Release 16.1, the output-file-name option for the show system schema operational command is deprecated. To direct the output to a file, use the output-directory option and specify the directory. By default, the filename for the output file uses the module name as the filename base and the format as the filename extension. If you also include the module-name option in the command, the specified module name is used for both the name of the generated module and for the filename base for the output file.

[See show system schema.]
• On EX Series switches that support Enhanced Layer 2 Software (ELS), when an interface is removed from a private VLAN (PVID) and then added back, the corresponding MAC entry might not be deleted from the Ethernet table. PR1036265

• On EX4300 switches, starting with Junos OS Release 15.1R3, a pfex_junos core file might be created when you add or delete a native VLAN configuration with flexible-vlan-tagging. PR1089483

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 16.1R1 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.

Authentication, Authorization, and Accounting

• On EX4300 switches, when 802.1X single-supplicant authentication is initiated, multiple EAP Request Id Frame Sent packets might be sent. PR1163966

• Changing the 802.1X (dot1x) supplicant mode from single-secure to multiple on interfaces of an EX9200-40XS line card might generate FPC core files. PR1198463

Firewall Filters

• Sending line-rate traffic on 10G interfaces of an EX9200-40XS line card that has an ingress router firewall filter configured with actions log and syslog might generate FPC kernel core files. PR1191397

Interfaces and Chassis

• On EX4600 switches, a long ICMP delay might occur when you attempt to ping a directly connected integrated routing and bridging (IRB) interface. PR966905

• On EX4300 switches, after disabling MC-LAG member interfaces, more than 3 seconds of traffic loss might occur. PR1164228

• If an Inter-Chassis Control Protocol (ICCP) interface on an EX9200 switch in an MC-LAG Active-Active topology is disabled and then re-enabled, traffic might be dropped for more than 2 seconds. PR1173923

• On an EX9200-12QS line card, interfaces with the default speed of 10G are not brought down even when the remote end of a connection is misconfigured as 40G. PR1175918

• Restarting an EX9200-40XS card with MC-LAG ICL, ICCP, and MC-AE interfaces configured on different interfaces of the same EX9200-40XS card might cause the system to shut down. PR1183135

• On an EX4300 switch or EX4300 Virtual Chassis that has a generic routing encapsulation (GRE) tunnel configured on an integrated routing and bridging interface
(IRB), the associated GRE statistical counters might not be updated after the GRE interface is deactivated and then reactivated. PR1183521

- On EX4300 Virtual Chassis, Layer 2 multicast might not work properly when both Layer 2 and Layer 3 entries are present for the same group on two different integrated routing and bridging (IRB) interfaces. PR1183531

**Network Analytics**

- Despite the EX4300 switch's being configured with the network analytics feature, the analytics daemon might not run. As a result, the network analytics feature might be unable to collect traffic and queue statistics and generate reports. PR1184720

**Port Security**

- On an EX9200-6QS line card, storm control might not work for multicast traffic. PR1191611

- On EX4300 switches, the routing table entry for an integrated routing and bridging (IRB) interface on which a connection with a DHCPv6 server is configured might be removed if the snooping device in the topology is configured with ND inspection. PR1201628

- On an EX9200-40XS line card, if you toggle the MACSec encryption option multiple times, encryption and protected MACSec statistics might be updated incorrectly. As a workaround, restart the line card. PR1185659

**Software Installation and Upgrade**

- During a nonstop software upgrade (NSSU) on an EX4300 Virtual Chassis, a traffic loop or loss might occur if the Junos OS software version that you are upgrading and the Junos OS software version that you are upgrading to use different internal message formats. PR1123764

- On an EX4300 Virtual Chassis, when you perform an NSSU, there might be up to five seconds of traffic loss for multicast traffic. PR1125155

- When performing a unified ISSU (FRU upgrade) on EX9200-40T, EX9200-40F, EX9200-40F-M, EX9200-32XS, EX9200-2C-8XS, and EX9200-4QS line cards, an issue occurs with the buffer size in the line cards. As a result, the unified ISSU cannot be performed on EX9200 switches with these line cards. PR1175240

- After a unified ISSU upgrade from Junos OS Release 15.1R3 to Junos OS Release 16.1 on EX4600 switches, LLDP neighbor discovery might fail. PR1187729

- While performing a unified ISSU upgrade of an EX9200 switch, BGPv6, OPSFv6, RIPv2, and multicast traffic might be dropped for approximately 30 seconds. PR1195439
Documentation Updates

This section lists the errata and changes in Junos OS Release 16.1R1 for the EX Series switches documentation.


**NETCONF XML Management Protocol Developer Guide**

The **NETCONF XML Management Protocol Developer Guide** incorrectly states that you can load custom YANG modules and action scripts on devices running Junos OS to augment the operational command hierarchy with non-native YANG RPCs. Junos OS does not support loading custom RPCs on devices running Junos OS.

Related Documentation

- New and Changed Features on page 8
- Changes in Behavior and Syntax on page 15
- Known Behavior on page 16
- Documentation Updates on page 19
- Migration, Upgrade, and Downgrade Instructions on page 19
- Product Compatibility on page 20

Migration, Upgrade, and Downgrade Instructions

This section contains the upgrade and downgrade support policy 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 about software installation and upgrade, see the Installation and Upgrade Guide.

- Upgrade and Downgrade Support Policy for Junos OS Releases on page 19

**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.

---

Copyright © 2016, Juniper Networks, Inc.
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 earlier or later, 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.

Related Documentation
- New and Changed Features on page 8
- Changes in Behavior and Syntax on page 15
- Known Behavior on page 16
- Known Issues on page 17
- Documentation Updates on page 19
- Product Compatibility on page 20

Product Compatibility
- Hardware Compatibility on page 20

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

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 8
- Changes in Behavior and Syntax on page 15
- Known Behavior on page 16
- Known Issues on page 17
- Documentation Updates on page 19
- Migration, Upgrade, and Downgrade Instructions on page 19
Junos OS Release Notes for Junos Fusion Enterprise

These release notes accompany Junos OS Release 16.1R1 for Junos Fusion Enterprise. Junos Fusion Enterprise is a Junos Fusion that uses EX9200 switches in the aggregation device role. These release notes describe new and changed features, limitations, and known problems in the hardware and software.

NOTE: For a complete list of all hardware and software requirements for a Junos Fusion Enterprise, including which Juniper Networks devices can function as satellite devices, see Understanding Junos Fusion Enterprise Software and Hardware Requirements in the Junos Fusion Enterprise Feature Guide.

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 on page 21
• Changes in Behavior and Syntax on page 23
• Known Behavior on page 24
• Known Issues on page 24
• Documentation Updates on page 26
• Migration, Upgrade, and Downgrade Instructions on page 27
• Product Compatibility on page 33

New and Changed Features

This section describes the new features in Junos OS Release 16.1R1 for Junos Fusion Enterprise.

NOTE: For more information about the Junos Fusion Enterprise features, see the Junos Fusion Enterprise Feature Guide.

• Junos Fusion Enterprise
Junos Fusion Enterprise

• **Junos Fusion Enterprise support**—Starting with Junos OS Release 16.1R1, Junos Fusion Enterprise—a Junos Fusion that uses EX9200 switches in the aggregation device role—is supported to bring the Junos Fusion technology to enterprise switching networks.

Junos Fusion Enterprise allows enterprise switching networks to combine numerous switches into a single, port-dense device that simplifies network management because it is managed from a single point—the EX9200 switch or switches acting in the aggregation device role—and simplifies network topologies because the Junos Fusion Enterprise is viewed as a single device by the larger network. Junos Fusion Enterprise supports the 802.1BR standard.

[See Junos Fusion Enterprise Overview.]

• **Dual aggregation device support for Junos Fusion (Junos Fusion Enterprise)**—Starting in Junos OS Release 16.1R1, dual aggregation device topologies are supported in a Junos Fusion. A Junos Fusion Enterprise dual aggregation topology provides traffic load-balancing and redundancy to the Junos Fusion.

Junos Fusion Enterprise supports multiple aggregation devices using multichassis link aggregation groups (MC-LAGs) and the Inter-Chassis Control Protocol (ICCP).

[See Junos Fusion Enterprise Components.]

• **Satellite device clustering support for Junos Fusion (Junos Fusion Enterprise)**—Starting in Junos OS Release 16.1R1, satellite device clustering in a Junos Fusion is supported. Satellite device clustering allows you to connect up to 10 satellite devices into a single cluster, and connect the satellite device cluster to the aggregation device as a single group instead of as individual satellite devices.

Satellite device clustering is particularly useful in scenarios where optical cabling options between buildings are limited and in scenarios where you want to preserve optical interfaces for other purposes. If you have, for instance, two buildings that have limited optical interfaces between each other and you want to put an aggregation device in one building and two to ten satellite devices in the other building, you can group the ten satellite devices into a cluster and connect the cluster to the aggregation device with a single cable.

[See Understanding Satellite Device Clustering in a Junos Fusion.]

• **PoE for Junos Fusion (Junos Fusion Enterprise)**—Starting in Junos OS Release 16.1R1, PoE is supported on Junos Fusion Enterprise.

PoE enables electric power, along with data, to be passed over a copper Ethernet LAN cable. Powered devices—such as VoIP telephones, wireless access points, video cameras, and point-of-sale devices—that support PoE can receive power safely from the same access ports that are used to connect personal computers to the network. This reduces the amount of wiring in a network, and also eliminates the need to position a powered device near an AC power outlet, making network design more flexible and efficient.

In a Junos Fusion Enterprise, PoE is used to carry electric power from an extended port on a satellite device to a connected device. An extended port is any network-facing

---

Copyright © 2016, Juniper Networks, Inc.
port on a satellite device in a Junos Fusion Enterprise. All extended ports that support PoE on satellite devices in a Junos Fusion Enterprise support the IEEE 802.3at PoE+ standard.

Junos Fusion Enterprise is able to support PoE when the satellite device provides PoE-capable interfaces.

[See Understanding Power over Ethernet in a Junos Fusion Enterprise.]

- **LLDP-MED with VoIP integration (Junos Fusion Enterprise)**—Starting in Junos OS Release 16.1R1, Link Layer Discovery Protocol–Media Endpoint Discovery (LLDP-MED) with VoIP integration is available for Junos Fusion Enterprise.

  LLDP-MED with VoIP integration is an extension of LLDP that is used to support device discovery of VoIP telephones and to create location databases for these telephone locations.

  [See Understanding LLDP and LLDP-MED on a Junos Fusion Enterprise.]

**Related Documentation**

- Changes in Behavior and Syntax on page 23
- Known Behavior on page 24
- Known Issues on page 24
- Documentation Updates on page 26
- Migration, Upgrade, and Downgrade Instructions on page 27
- Product Compatibility on page 33

**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 in Junos OS Release 16.1R1 for Junos Fusion Enterprise.

- General Routing on page 23

**General Routing**

- **Enhancement to request support information command**—Starting in Junos OS Release 16.1R1, the `request support information` command is enhanced to capture the following additional details:
  
  - `file list detail/var/rundb/`—Displays the size of the configuration databases.
  - `show system configuration database usage`—Displays the actual usage of the configuration databases.

  **NOTE:** This information will be displayed only if the `show system configuration database usage` command is supported in the release.
- **file list detail /config/**—Contains the db_ext file and shows the size of it to indicate whether extend_size is enabled or disabled.

- **New option introduced under show | display xml | display**—Starting in Junos OS 16.1R1, you can use the `show | display xml | display | mark-changed` statement to view the "mark-changed" status of the nodes. This is useful for debugging purpose.

### Related Documentation
- New and Changed Features on page 21
- Known Behavior on page 24
- Known Issues on page 24
- Documentation Updates on page 26
- Migration, Upgrade, and Downgrade Instructions on page 27
- Product Compatibility on page 33

### Known Behavior

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 16.1R1 for Junos Fusion Enterprise.

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

- Junos Fusion on page 24

### Junos Fusion

- On Junos Fusion Enterprise, PoE Simple Network Management Protocol (SNMP) traps are not supported. PR1112613

### Related Documentation
- New and Changed Features on page 21
- Changes in Behavior and Syntax on page 23
- Known Issues on page 24
- Documentation Updates on page 26
- Migration, Upgrade, and Downgrade Instructions on page 27
- Product Compatibility on page 33

### Known Issues

This section lists the known issues in hardware and software in Junos OS Release 16.1R1 for Junos Fusion Enterprise.
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 on page 25
- Layer 2 Features on page 25
- Network Management and Monitoring on page 26
- Platform and Infrastructure on page 26

**Interfaces and Chassis**

- On a Junos Fusion Enterprise using a dual aggregation device topology, an interchassis link (ICL) configured on an aggregated ethernet interface cannot pass traffic between aggregation devices. **PR1090470**

- On Junos Fusion Enterprise, PoE telemetries do not work. **PR1112953**

- On a Junos Fusion Enterprise, PoE configuration changes might not be reflected on satellite devices that are not in the online state at the time of the configuration change. **PR1154486**

- On a Junos Fusion Enterprise that has rebooted a satellite device in a satellite device cluster, traffic can be lost for several seconds after the satellite device returns to an operational state. **PR1168820**

- On a Junos Fusion Enterprise using a dual aggregation device topology, control traffic generated by the aggregation device - with the exception of Address Resolution Protocol (ARP) traffic - is sometimes not forwarded to the extended ports on the satellite devices. This issue does not impact data path traffic flows. **PR1174373**

- On a Junos Fusion Enterprise that has been reconfigured from a dual aggregation device topology to a single aggregation device topology, some satellite devices may not return online and remain in the Present state in the show chassis satellite output indefinitely after the reconfiguration. As a workaround, enter the restart satellite-discovery-provisioning-process command to reboot the satellite discovery provisioning process and return the satellite devices online. **PR1182542**

**Layer 2 Features**

- On a Junos Fusion Enterprise, Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED) fast start does not work. **PR1171899**

- On a Junos Fusion Enterprise, LLDP might stop working if it is re-enabled after being manually disabled. **PR1188254**

- On a Junos Fusion Enterprise that has simultaneously deleted or deactivated LLDP and LLDP-MED, LLDP packets continue to be forwarded. As a workaround, deactivate or delete LLDP-MED and commit the configuration before deactivating and deleting LLDP. **PR1136395**
Network Management and Monitoring

- On a Junos Fusion Enterprise, the SNMP trap that should be sent for a satellite device reboot event is not sent. PR1182895

Platform and Infrastructure

- On a Junos Fusion Enterprise, PoE firmware upgrades for EX4300 series switches acting as satellite devices are not supported. PR1151622

- On a Junos Fusion Enterprise that has an EX9200-6QS line card installed in the aggregation device, restarting the EX9200-6QS line card might lead to an FPC staying in the ready state instead of returning online. As a workaround, reboot the aggregation device. PR1173958

- On a Junos Fusion Enterprise that is using a 40-Gbps QSFP+ direct-attach copper (DAC) cable to interconnect an EX4300 switch running Junos into a satellite device cluster, the EX4300 switch running Junos may not convert into a satellite device and is not recognized by the satellite devices in the satellite device cluster until link autonegotiation is disabled using the set interfaces ether-options no-auto-negotiation statement.

  As a workaround, interconnect the satellite device using a standard 40-Gbps QSFP+ cable to convert the switch into a satellite device. If desired, interconnect the satellite devices using the 40-Gbps QSFP+ direct-attach copper (DAC) cable after the EX4300 switch is converted into a satellite device. PR1198942

- In a JUNOS Fusion Enterprise that has enabled PoE for all extended ports, the show poe interface command output displays the PoE administrative status as Enabled for non-PoE-capable interfaces. PR1150955

Related Documentation

- New and Changed Features on page 21
- Changes in Behavior and Syntax on page 23
- Known Behavior on page 24
- Documentation Updates on page 26
- Migration, Upgrade, and Downgrade Instructions on page 27
- Product Compatibility on page 33

Documentation Updates

There are no errata or changes in Junos OS Release 16.1R1 for Junos Fusion Enterprise documentation.

Related Documentation

- New and Changed Features on page 21
- Changes in Behavior and Syntax on page 23
- Known Behavior on page 24
- Known Issues on page 24
Migration, Upgrade, and Downgrade Instructions

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

- Basic Procedure for Upgrading Junos OS on an Aggregation Device on page 27
- Upgrading an Aggregation Device with Redundant Routing Engines on page 29
- Preparing the Switch for Satellite Device Conversion on page 29
- Converting a Satellite Device to a Standalone Switch on page 30
- Upgrade and Downgrade Support Policy for Junos OS Releases on page 32
- Downgrading from Release 16.1 on page 32

Basic Procedure for Upgrading Junos OS on an Aggregation Device

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

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

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

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

The download and installation process for Junos OS Release 16.1R1 is different from previous Junos OS releases.
1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:
   
   http://www.juniper.net/support/downloads/

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

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

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

5. Select the Software tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

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

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

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

```sh
user@host> request system software add validate reboot
source/junos-install-ex92xx-x86-64-16.1R1.11-domestic-signed.tgz
```

All other customers, use the following commands.

```sh
user@host> request system software add validate reboot
source/junos-install-ex92xx-x86-64-16.1R1.11-domestic-limited.tgz
```

Replace source with one of the following values:

- `/pathname` — For a software package that is installed from a local directory on the router.

- For software packages that are downloaded and installed from a remote location:
  
  - `ftp://hostname/pathname`
  
  - `http://hostname/pathname`
  
  - `scp://hostname/pathname` (available only for Canada and U.S. version)

The validate option validates the software package against the current configuration as a prerequisite to adding the software package to ensure that the router reboots successfully. This is the default behavior when the software package being added is a different release.
Adding the `reboot` command reboots the router after the upgrade is validated and installed. When the reboot is complete, the router displays the login prompt. The loading process can take 5 to 10 minutes.

Rebooting occurs only if the upgrade is successful.

**NOTE:** After you install a Junos OS Release 16.1R1 junos-install 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 junos-install package that corresponds to the previously installed software.

### Upgrading an Aggregation Device with Redundant Routing Engines

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

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

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

### Preparing the Switch for Satellite Device Conversion

There are multiple methods to upgrade or downgrade satellite software in your Junos Fusion Enterprise. See [Configuring or Expanding a Junos Fusion Enterprise](#).

For satellite device hardware and software requirements, see [Understanding Junos Fusion Enterprise Software and Hardware Requirements](#).

A satellite device must be running Junos OS Release 14.1X53-D35 or later before it can be converted into a satellite device, in any context.

Use the following command to install Junos OS Release 14.1X53-D35 onto a switch before converting it into a satellite device:

```bash
user@host> request system software add validate reboot source/jinstall-ex-4300-14.1X53-D35.3-domestic-signed.tgz
```

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

1. Log in to the device using the console port.
2. Clear the device:
[edit]
user@satellite-device# request system zeroize

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

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

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

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

   user@satellite-device> request virtual-chassis vc-port delete pic-slot 1 port port-number
   For example, to convert all four built-in 40-Gbps QSFP+ interfaces on an EX4300-24P switch into network ports:

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

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

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

**Converting a Satellite Device to a Standalone Switch**

In the event that you need to convert a satellite device to a standalone device, you will need to install a new Junos OS software package on the satellite device and remove it from the Junos Fusion topology.
The following steps explain how to download software, remove the satellite device from the Junos Fusion, and install the Junos OS software image on the satellite device so that the device can operate as a standalone device.

1. Using a Web browser, navigate to the Junos OS software download URL on the Juniper Networks webpage:
   
   http://www.juniper.net/support/downloads

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

3. Select By Technology > Junos Platform > Junos Fusion from the pull-down menu and select the switch platform series and model for your satellite device.

4. Select the Junos OS Release 14.1X53-D35 software image for your platform.

5. Review and accept the End User License Agreement.

6. Download the software to a local host.
   
   Copy the software to the routing platform or to your internal software distribution site.

7. Remove the satellite device from the automatic satellite conversion configuration.
   
   If automatic satellite conversion is enabled for the satellite device's member number, remove the member number from the automatic satellite conversion configuration. The satellite device's member number is the same as the FPC slot ID. You can check the automatic satellite conversion configuration by entering the show command at the [edit chassis satellite-management auto-satellite-conversion] hierarchy level.

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

   For example, to remove member number 101 from the Junos Fusion:

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

8. Commit the configuration.
   
   To commit the configuration to both Routing Engines:

   [edit]
   user@aggregation-device# commit synchronize

   Otherwise, commit the configuration to a single Routing Engine:

   [edit]
   user@aggregation-device# commit

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

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

   For example, to install a software package stored in the /var/tmp directory on the aggregation device onto an EX4300 switch acting as the satellite device using FPC slot 102: 

   [edit]
   user@aggregation-device> request chassis satellite install /var/tmp/102 package-filename

   where package-filename is the name of the software package file on the FPC slot.
[edit]
user@aggregation-device> request chassis satellite install
/var/tmp/jinstall-ex-4300-14.1X53-D35.3-domestic-signed.tgz fpc-slot 102

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

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

11. When you are prompted to log back in to your device, unplug the device from the Junos Fusion topology. See Removing a Transceiver from a QFX Series Device or Removing a Transceiver from a Switch, as needed. Your device has been removed from the Junos Fusion.

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

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

Downgrading from Release 16.1

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

To downgrade from Release 16.1 to another supported release, follow the procedure for upgrading, but replace the 16.1 junos-install 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.

Product Compatibility

- Hardware and Software Compatibility on page 33

Hardware and Software Compatibility

For a complete list of all hardware and software requirements for a Junos Fusion Enterprise, including which Juniper Networks devices function as satellite devices, see Understanding Junos Fusion Enterprise Software and Hardware Requirements in the Junos Fusion Enterprise Feature Guide.

Related Documentation

- New and Changed Features on page 21
- Changes in Behavior and Syntax on page 23
- Known Behavior on page 24
- Known Issues on page 24
- Documentation Updates on page 26
- Migration, Upgrade, and Downgrade Instructions on page 27
Junos OS Release Notes for Junos Fusion Provider Edge

These release notes accompany Junos OS Release 16.1R1 for the Junos Fusion Provider Edge. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

• New and Changed Features on page 34
• Changes in Behavior and Syntax on page 36
• Known Behavior on page 36
• Known Issues on page 37
• Resolved Issues on page 38
• Documentation Updates on page 38
• Migration, Upgrade, and Downgrade Instructions on page 39
• Product Compatibility on page 52

New and Changed Features

This section describes the new features in Junos OS Release 16.1R1 for Junos Fusion Provider Edge.

• Hardware on page 34
• Multicast on page 34

Hardware

• Additional MPC support—Starting with Junos OS Release 16.1R1, the following Modular Port Concentrators (MPCs) are supported on the MX Series routers:
  • MPC7E
  • MPC8E
  • MPC9E

Multicast

• Egress Multicast Replication—Starting with Junos OS Release 16.1, you can enable egress multicast replication to optimize multicast traffic in a Junos Fusion. In egress multicast replication, multicast traffic is replicated on satellite devices, rather than on the aggregation device. If you have a large number of multicast receivers or high multicast bandwidth traffic, enabling egress multicast replication reduces the traffic on cascade port interfaces and reduces the load on the aggregation device. This can reduce the latency and jitter in packet delivery, decrease the number of problems associated with oversubscription, and prevent a traffic storm caused by flooding of unknown unicast packets to all interfaces.
This feature is disabled by default. To enable egress multicast replication, use the `local-replication` statement in the `the [edit forwarding-options satellite]` hierarchy level. When you enable this feature, local replication is enabled on all satellite devices that are connected to the aggregation device. You cannot enable local replication for just a few selected satellite devices, specific bridge domains, or specific route prefixes.

Egress multicast replication does not take effect with the following features (Junos Fusion replicates multicast traffic on the aggregation device and other multicast traffic will continue to be replicated on satellite devices):

- Multicast support on pure layer 3 extended ports
- MLD snooping on an IPv6 network

Egress multicast replication is incompatible with the following features (the feature will not work together with egress multicast replication and you must choose either to enable egress multicast replication or to use the feature):

- VLAN tag manipulations, such as VLAN tag translations, VLAN tag stacking, and VLAN per port policies. This can result in dropped packets caused by unexpected VLAN tags.
- Multicast support for the extended ports on the edge side of Pseudowire connections in VPLS networks.
- Multicast support for the extended ports on the edge side of EVPN.
- Multicast VPN deployments.
- MPLS/BGP VPN deployments.
- Features that perform egress actions on individual extended ports, such as egress local-port mirroring.

Use the following new operational commands to display information related to this feature:

- `show bridge flood next-hops satellite`
- `show bridge flood next-hops satellite nexthop-id nexthop-identifier`
- `show bridge flood satellite`
- `show bridge flood satellite bridge-domain-name domain-name`
- `show bridge satellite device`
- `show multicast ecid-mapping satellite`
- `show multicast next-hops satellite`
- `show multicast snooping next-hops satellite nexthop-id nexthop-identifier`
- `show multicast snooping route satellite`
- `show multicast snooping route satellite bridge-domain-name domain-name`
- `show multicast snooping route satellite group group-id`
• show multicast statistics satellite
• show multicast summary satellite

Related Documentation
• Changes in Behavior and Syntax on page 36
  • Known Behavior on page 36
  • Known Issues on page 37
  • Resolved Issues on page 38
  • Documentation Updates on page 38
  • Migration, Upgrade, and Downgrade Instructions on page 39
  • Product Compatibility on page 52

Changes in Behavior and Syntax

There are no changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands in Junos OS Release 16.1R1 for Junos Fusion Provider Edge.

Known Behavior

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 16.1R1 for Junos Fusion Provider Edge.

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

• Junos Fusion on page 37
Junos Fusion

- On a Junos Fusion Provider Edge topology, if you enable MC-LAG over an IRB interface and perform a graceful Routing Engine switchover, the system might experience traffic loss of up to 60 percent of the traffic for 90 seconds and a drop in the ARP count. PR1080192

Related Documentation

- New and Changed Features on page 34
- Changes in Behavior and Syntax on page 36
- Known Issues on page 37
- Resolved Issues on page 38
- Documentation Updates on page 38
- Migration, Upgrade, and Downgrade Instructions on page 39
- Product Compatibility on page 52

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 16.1R1 for Junos Fusion Provider Edge.

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

- Junos Fusion on page 37
- Satellite Software on page 37

Junos Fusion

- On a Junos Fusion Provider Edge topology, if you configure an outgoing firewall or policer to drop packets prior to transmission, the logical interfaces of satellite device extended ports that appear in the output of the `show interfaces extensive` command might include packets in the statistics counter that have been dropped but not forwarded. PR1078304

- On a Junos Fusion Provider Edge topology running multicast, if you disable and reenable a satellite device, the PIM upstream interface state might not be updated correctly. PR1091449

Satellite Software

- On a Junos Fusion Provider Edge topology, you might not be able to disable auto-negotiation on fiber-based Gigabit Ethernet ports in a QFX5100 switch acting as a satellite device. PR1183112

Related Documentation

- New and Changed Features on page 34
- Changes in Behavior and Syntax on page 36
Resolved Issues

There are no fixed issues in the Junos OS Release 16.1R1 for Junos Fusion Provider Edge.

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

Documentation Updates

There are no errata or changes in Junos OS Release 16.1R1 for Junos Fusion Provider Edge documentation.

Related Documentation

- Known Behavior on page 36
- Resolved Issues on page 38
- Documentation Updates on page 38
- Migration, Upgrade, and Downgrade Instructions on page 39
- Product Compatibility on page 52
Migration, Upgrade, and Downgrade Instructions

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

- Basic Procedure for Upgrading an Aggregation Device on page 39
- Upgrading an Aggregation Device with Redundant Routing Engines on page 41
- Preparing the Switch for Satellite Device Conversion on page 42
- Autoconverting a Switch into a Satellite Device on page 43
- Manually Converting a Switch into a Satellite Device on page 45
- Configuring a Switch into a Satellite Device Before Connecting It to a Junos Fusion Topology on page 47
- Configuring Satellite Device Upgrade Groups on page 48
- Converting a Satellite Device to a Standalone Device on page 49
- Upgrade and Downgrade Support Policy for Junos OS Releases on page 51
- Downgrading from Release 16.1 on page 52

Basic Procedure for Upgrading an Aggregation Device

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

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

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

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the `juniper.conf` and `ssh` files), might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. See the Junos OS Administration Library for Routing Devices.
The download and installation process for Junos OS Release 16.1R1 is different from previous Junos OS releases.

1. Using a Web browser, navigate to the Download Software URL on the Juniper Networks webpage:
   http://www.juniper.net/support/downloads/

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

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

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

5. Select the Software tab.

6. Select the software package for the release.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

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

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

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

- For 64-bit software:
  ```
  user@host> request system software add validate reboot
  source/jinstall64-16.1[R]REV.SPIN-domestic-signed.tgz
  ```

   **NOTE:** We highly recommend using 64-bit Junos OS software when implementing Junos Fusion.

- For 32-bit software:
  ```
  user@host> request system software add validate reboot
  source/jinstall-16.1[R]REV.SPIN-domestic-signed.tgz
  ```

All other customers, use the following commands.

- For 64-bit software:
  ```
  user@host> request system software add validate reboot
  source/jinstall-16.1[R]REV.SPIN-domestic-signed.tgz
  ```

   **NOTE:** We highly recommend using 64-bit Junos OS software when implementing Junos Fusion.
For 32-bit software:

```
user@host> request system software add validate reboot
source/jinstall-16.1[BR]REV.SPIN-export-signed.tgz
```

Replace `source` with one of the following values:

- `/pathname`—For a software package that is installed from a local directory on the router.
- For software packages that are downloaded and installed from a remote location:
  - `ftp://hostname/pathname`
  - `http://hostname/pathname`
  - `scp://hostname/pathname` (available only for 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 16.1[BR]REV 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.

---

### Upgrading an Aggregation Device with Redundant Routing Engines

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

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

Satellite devices in a Junos Fusion topology use a satellite software package that is different from the standard Junos OS software package. Before you can install the satellite software package on a satellite device, you first need to upgrade the target satellite device to an interim Junos OS software version that can be converted to satellite software. Table 1 on page 42 shows a support matrix that maps Junos OS software used in aggregation devices to the compatible preconverted switch software and satellite device software.

Table 1: Aggregation Device Junos OS Software Compatibility with Satellite Software

<table>
<thead>
<tr>
<th>Aggregation Device Version</th>
<th>Switch Version (preconversion)</th>
<th>Satellite Device Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Junos OS Release 14.2R3</td>
<td>Junos OS Release 14.1X53-D16 or later</td>
<td>1.0R1</td>
</tr>
<tr>
<td>Junos OS Release 14.2R4</td>
<td>Junos OS Release 14.1X53-D25 or later</td>
<td>1.0R1-S2</td>
</tr>
<tr>
<td>Junos OS Release 14.2R5</td>
<td>Junos OS Release 14.1X53-D30 or later</td>
<td>1.0R2</td>
</tr>
<tr>
<td>Junos OS Release 14.2R6</td>
<td>Junos OS Release 14.1X53-D30 or later</td>
<td>1.0R3</td>
</tr>
<tr>
<td>Junos OS Release 16.1R1</td>
<td>Junos OS Release 14.1X53-D30 or later</td>
<td>1.0R3</td>
</tr>
</tbody>
</table>

Customers with EX4300 switches, use the following command:

```
user@host> request system software add validate reboot
source/jinstall-ex-4300-14.1X53-D30.3-domestic-signed.tgz
```

Customers with QFX5100 switches, use the following command:

```
user@host> request system software add validate reboot
source/jinstall-qfx-5-14.1X53-D30.3-domestic-signed.tgz
```

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

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

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

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

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

If you lose your connection to the device, log in using the console port.
3. (EX4300 switches only) After the reboot is complete, convert the built-in 40-Gbps QSFP+ interfaces from Virtual Chassis ports (VCPs) into network ports:

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

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

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

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

After this initial preparation, you can use one of three methods to convert your switches into satellite devices—autoconversion, manual conversion, and preconfiguration.

**Autoconverting a Switch into a Satellite Device**

Use this procedure to automatically configure a switch into a satellite device when it is cabled into the aggregation device.

You can use the autoconversion procedure to add one or more satellite devices to your Junos Fusion topology. The autoconversion procedure is especially useful when you are adding multiple satellite devices to Junos Fusion, because it allows you to easily configure the entire topology before or after cabling the satellite devices to the aggregation devices.

Before you begin:

- Ensure that your aggregation device is running Junos OS Release 14.2R5 or later, and that the satellite devices are running Junos OS Release 14.1X53-D30 or later.

To autoconvert a switch into a satellite device:

1. Cable a link between the aggregation device and the satellite device, if desired.

   **NOTE:** You can cable the aggregation device to the satellite device at any point in this procedure.

   When the aggregation device is cabled to the satellite device during this procedure, the process for converting a switch into a satellite device to finalize this process occurs immediately.

   If the aggregation device is not cabled to the satellite device, the process for converting a switch into a satellite device to finalize this process starts when the satellite device is cabled to the aggregation device.

2. Log in to the aggregation device.

3. Configure the cascade ports.
For example, to configure interface xe-0/0/1 on the aggregation device into a cascade port:

```
[edit]
user@aggregation-device# set interfaces xe-0/0/1 cascade-port
```

4. Associate an FPC slot ID with each satellite device.

Examples:

- To configure the FPC slot ID of the satellite device that is connected to xe-0/0/1 to 101:
  
  ```
  [edit]
  user@aggregation-device# set chassis satellite-management fpc 101 cascade-ports xe-0/0/1
  ```

- To map FPC slot ID 101 to the satellite device using the serial number ABCDEFGHIJKL:
  
  ```
  [edit]
  user@aggregation-device# set chassis satellite-management fpc 101 serial-number ABCDEFGHIJKL
  ```

- To map FPC slot ID to the satellite device using MAC address 12:34:56:AB:CD:EF:
  
  ```
  [edit]
  user@aggregation-device# set chassis satellite-management fpc 110 system-id 12:34:56:AB:CD:EF
  ```

5. (Recommended) Configure an alias name for the satellite device:

```
[edit]
user@aggregation-device# set chassis satellite-management fpc slot-id alias alias-name
```

where `slot-id` is the FPC slot ID of the satellite device defined in the previous step, and `alias-name` is the alias.

For example, to configure the satellite device numbered 101 as qfx5100-48s-1:

```
[edit]
user@aggregation-device# set chassis satellite-management fpc 101 alias qfx5100-48s-1
```

6. Configure an FPC slot ID into a software upgrade group.

For example, to add a satellite device with FPC number 101 to an existing software group named group1, or create a software upgrade group named group1 and add a satellite device with FPC slot 101 to the group:

```
[edit]
user@aggregation-device# set chassis satellite-management upgrade-group group1 satellite 101
```

If you are creating a new software upgrade group in this step, you also need to associate the group with a satellite software image. You can skip this final step if the software upgrade group has been created and an association already exists.

Before associating a satellite software image with a satellite software group, the configuration with the satellite software upgrade group must be committed:

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

After committing the configuration, associate a satellite software image named `satellite-1.0R3-signed.tgz` to the upgrade group named group1:

```
user@aggregation-device# request system software add /var/tmp/satellite-1.0R3-signed.tgz upgrade-group group1
```
7. Enable automatic satellite conversion:

```
[edit]
user@aggregation-device# set chassis satellite-management auto-satellite-conversion satellite slot-id
```

For example, to automatically convert FPC 101 into a satellite device:

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

8. Commit the configuration:

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

If you want to commit the configuration to both Routing Engines:

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

The satellite software upgrade on the satellite device begins after this final step is completed, or after you cable the satellite device to a cascade port using automatic satellite conversion if you have not already cabled the satellite device to the aggregation device.

After the satellite software update, the switch operates as a satellite device in the Junos Fusion topology

---

**Manually Converting a Switch into a Satellite Device**

Use this procedure to manually convert a switch into a satellite device after cabling it into the Junos Fusion topology.

This procedure should be used to convert a switch that is not currently acting as a satellite device into a satellite device. A switch might not be recognized as a satellite device for several reasons, including that the device was not previously autoconverted into a satellite device or that the switch had previously been reverted from a satellite device to a standalone switch.

**Before you begin:**

- Ensure that your aggregation device is running Junos OS Release 14.2R5 or later, and that the switches that will become satellite devices are running Junos OS Release 14.1X53-D30 or later.

To manually convert a switch into a satellite device:

1. Cable a link between the aggregation device and the satellite device.
2. Log in to the aggregation device.
3. Configure the link on the aggregation device into a cascade port, if you have not done so already.

For example, to configure interface xe-0/0/1 on the aggregation device into a cascade port:

```
[edit]
user@aggregation-device# set interfaces xe-0/0/1 cascade-port
```
4. Associate an FPC slot ID with the satellite device.

Examples:

- To configure the FPC slot ID of the satellite device that is connected to xe-0/0/1 to 101:
  ```
  [edit]
  user@aggregation-device# set chassis satellite-management fpc 101 cascade-ports xe-0/0/1
  ```

- To map FPC slot ID 101 to the satellite device using the serial number ABCDEFGHIJKL:
  ```
  [edit]
  user@aggregation-device# set chassis satellite-management fpc 101 serial-number ABCDEFGHIJKL
  ```

- To map FPC slot ID to the satellite device using MAC address 12:34:56:AB:CD:EF:
  ```
  [edit]
  user@aggregation-device# set chassis satellite-management fpc 110 system-id 12:34:56:AB:CD:EF
  ```

5. Configure the interface on the aggregation device into a software upgrade group.

For example, to add a satellite device with FPC number 101 to an existing software group named group1, or create a software upgrade group named group1 and add a satellite device configured with FPC number 101 to the group:

```
[edit]
user@aggregation-device# set chassis satellite-management upgrade-group group1 satellite 101
```

If you are creating a new software upgrade group in this step, you also need to associate the group with a satellite software image. You can skip this final step if the software upgrade group has been created and an association already exists.

Before associating a satellite software image with a satellite software group, the configuration with the satellite software upgrade group must be committed:

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

After committing the configuration, associate a satellite software image named satellite-1.0R3-signed.tgz to the upgrade group named group1:

```
user@aggregation-device# request system software add /var/tmp/satellite-1.0R3-signed.tgz upgrade-group group1
```

6. Commit the configuration:

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

If you want to commit the configuration to both Routing Engines:

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

7. Manually configure the switch into a satellite device:

```
user@aggregation-device# request chassis satellite interface interface-name device-mode satellite
```

For example, to manually configure the switch that is connecting the satellite device to interface xe-0/0/1 on the aggregation device into a satellite device:

```
user@aggregation-device# request chassis satellite interface xe-0/0/1 device-mode satellite
```
The satellite software upgrade on the satellite device begins after this final step is completed.

After the satellite software update, the switch operates as a satellite device in the Junos Fusion topology

Configuring a Switch into a Satellite Device Before Connecting It to a Junos Fusion Topology

Use this procedure to install the satellite software onto a switch before interconnecting it into a Junos Fusion topology as a satellite device. Installing the satellite software on a switch before interconnecting it to a Junos Fusion topology allows you to more immediately deploy the switch as a satellite device by avoiding the downtime associated with the satellite software installation procedure for Junos Fusion.

Before you begin:

- Ensure that your switch that will become a satellite device is running Junos OS Release 14.1X53-D30 or later.
- Ensure that you have copied the satellite software onto the device that will become a satellite device.

**NOTE:** Ensure there is sufficient space available in the /var/tmp directory to be able to copy the software to the switch (especially for EX4300 switches). If there is not enough memory available, issue the request system storage cleanup command on the device before attempting to perform the conversion.

In SNOS Release 1.0R3, a satellite-ppc-1.0R3.2-signed.tgz package is included specifically for converting Junos OS to satellite on EX4300 to address a EX4300 switch space issue. The satellite-ppc package is to be used only for configuring a switch into a satellite device before connecting it to a Junos Fusion topology.

1. You can manually install the satellite software onto a switch by entering the following command:

   ```
   user@satellite-device> request chassis device-mode satellite URL-to-satellite-software
   ```

   For instance, to install the satellite software package `satellite-1.0R3.2-signed.tgz` stored in the `/var/tmp/` directory on the switch:

   ```
   user@satellite-device> request chassis device-mode satellite /var/tmp/satellite-1.0R3.2-signed.tgz
   ```

   - To install satellite software onto a QFX5100 switch, use the `satellite-1.0R3.2-signed.tgz` satellite software package.

   - To install satellite software onto a EX4300 switch, use the `satellite-ppc-1.0R3.2-signed.tgz` satellite software package.

2. The device will reboot to complete the satellite software installation.
After the satellite software is installed, follow this procedure to connect the switch into a Junos Fusion topology:

1. Log in to the aggregation device.
2. Configure the link on the aggregation device into a cascade port, if you have not done so already.

   For example, to configure interface xe-0/0/1 on the aggregation device into a cascade port:

   ```
   [edit]
   user@aggregation-device# set interfaces xe-0/0/1 cascade-port
   ```

3. Configure the satellite switch into a satellite software upgrade group that is using the same version of satellite software that was manually installed onto the switch.

   This step is advisable, but not always required. Completing this step ensures that the satellite software on your device is upgraded to the version of satellite software associated with the satellite software upgrade group when the satellite device connects to the aggregation device.

4. Commit the configuration.

   To commit the configuration to both Routing Engines:

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

   To commit the configuration to a single Routing Engine:

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

5. Cable a link between the aggregation device and the satellite device.

### Configuring Satellite Device Upgrade Groups

To simplify the upgrade process for multiple satellite devices, you can create a software upgrade group at the aggregation device, assign satellite devices to the group, and install the satellite software on a groupwide basis.

To create a software upgrade group and assign satellite devices to the group, include the `satellite` statement at the `[edit chassis satellite-management upgrade-groups upgrade-group-name]` hierarchy level.

To configure a software upgrade group and assign satellite devices to the group:

1. Log in to the aggregation device.
2. Create the software upgrade group, and add the satellite devices to the group.

   ```
   [edit]
   user@aggregation-device# set chassis satellite-management upgrade-groups
   upgrade-group-name satellite satellite-member-number-or-range
   ```

   `upgrade-group-name` is the name of the upgrade group, and the `satellite-member-number-or-range` is the member numbers of the satellite devices that are being added to the upgrade group. If you enter an existing upgrade group name as
the `upgrade-group-name`, you add new satellite devices to the existing software upgrade group.

For example, to create a software upgrade group named `group1` that includes all satellite devices numbered 101 through 120, configure the following:

```
[edit]
user@aggregation-device# set chassis satellite-management upgrade-groups group1 satellite 101-120
```

To install, remove, or roll back a satellite software version on an upgrade group, issue the following operational mode commands:

- `request system software add upgrade-group group-name`—Install the satellite software on all members of the specified upgrade group.
- `request system software delete upgrade-group group-name`—Remove the satellite software association from the specified upgrade group.
- `request system software rollback upgrade-group group-name`—Associate an upgrade group with a previous version of satellite software.

Customers installing satellite software on EX4300 and QFX5100 switches referenced in a software upgrade group, use the following command:

```
user@aggregation-device> request system software add upgrade-group group-name source/satellite-1.0R3.2-signed.tgz
```

A copy of the satellite software is saved on the aggregation device. When you add a satellite device to an upgrade group that is not running the same satellite software version, the new satellite device is automatically updated to the version of satellite software that is associated with the upgrade group.

You can issue the `show chassis satellite software` command to see which software images are stored on the aggregation device and which upgrade groups are associated with the software images.

**Converting a Satellite Device to a Standalone Device**

In the event that you need to convert a satellite device to a standalone device, you will need to install a new Junos OS software package on the satellite device and remove it from the Junos Fusion topology.

**NOTE:** If the satellite device is a QFX5100 switch, you need to install a PXE version of Junos OS. The PXE version of Junos OS is the software that includes `pxe` in the Junos OS package name when it is downloaded from the Software Center—for example, the PXE image for Junos OS Release 14.1X53-D30 is named `install-media-pxe-qfx-5-14.1X53-D30.3.tgz`. If the satellite device is an EX4300 switch, you install a standard `jinstall-ex-4300` version of Junos OS.
The following steps explain how to download software, remove the satellite device from Junos Fusion, and install the Junos OS software image on the satellite device so that the device can operate as a standalone device.

1. Using a Web browser, navigate to the Junos OS software download URL on the Juniper Networks webpage:
   
   http://www.juniper.net/support/downloads

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

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

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

5. Review and accept the End User License Agreement.

6. Download the software to a local host.

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

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

   If automatic satellite conversion is enabled for the satellite device's member number, remove the member number from the automatic satellite conversion configuration. The satellite device's member number is the same as the FPC slot ID. You can check the automatic satellite conversion configuration by entering the show command at the [edit chassis satellite-management auto-satellite-conversion] hierarchy level.

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

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

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

9. Commit the configuration.

   To commit the configuration to both Routing Engines:

   [edit]
   
   user@aggregation-device# commit synchronize

   Otherwise, commit the configuration to a single Routing Engine:

   [edit]
   
   user@aggregation-device# commit

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

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

   For example, to install a PXE software package stored in the /var/tmp directory on the aggregation device onto a QFX5100 switch acting as the satellite device using FPC slot 101:
For example, to install a software package stored in the `/var/tmp` directory on the aggregation device onto an EX4300 switch acting as the satellite device using FPC slot 101:

```
user@aggregation-device> request chassis satellite install /var/tmp/install-media-pxe-qfx-5-14.1X53-D30.3.tgz fpc-slot 101
```

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

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

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

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

---

**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](http://www.juniper.net/support/eol/junos.html)
Downgrading from Release 16.1

To downgrade from Release 16.1 to another supported release, follow the procedure for upgrading, but replace the 16.1 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.

Related Documentation
- New and Changed Features on page 34
- Changes in Behavior and Syntax on page 36
- Known Behavior on page 36
- Known Issues on page 37
- Resolved Issues on page 38
- Documentation Updates on page 38
- Product Compatibility on page 52

Product Compatibility
- Hardware Compatibility on page 52

Hardware Compatibility

To obtain information about the components that are supported on the devices, and special compatibility guidelines with the release, see the Hardware Guides for the devices used in your Junos Fusion Provider Edge topology.

To determine the features supported on Junos Fusion devices, 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 34
- Changes in Behavior and Syntax on page 36
- Known Behavior on page 36
- Known Issues on page 37
- Resolved Issues on page 38
- Documentation Updates on page 38
Junos OS Release Notes for MX Series 3D Universal Edge Routers and T Series Core Routers

These release notes accompany Junos OS Release 16.1R1 for the 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/.

The following MX features are not supported in Junos OS Release 16.1R1:

- CLNS
- ISSU
- J-Web
- PTP
- Subscriber Management and Services
- Virtual Chassis
- VXLAN

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 16.1R1 for the MX Series and T Series.

- Hardware on page 54
- Authentication, Authorization, and Accounting on page 56
- Class of Service (CoS) on page 56
- EVPNs on page 57
- General Routing on page 58
- High Availability and Resiliency on page 59
- Interfaces and Chassis on page 60
IPv4 on page 68
Junos OS XML API and Scripting on page 68
Layer 2 Features on page 68
Management on page 69
MPLS on page 70
Multicast on page 75
Network Management and Monitoring on page 76
Operation Administration and Management on page 78
Routing Policy and Firewall Filters on page 81
Routing Protocols on page 82
Security on page 85
Services Applications on page 86
Software Installation and Upgrade on page 89
Software Defined Networking on page 91
Subscriber Management and Services on page 92
System Logging on page 103
System Management on page 104
Timing and Synchronization on page 104
User Interface and Configuration on page 104
Virtual Chassis on page 105
VPNs on page 105

Hardware

New Routing Engine RE-S-X6-64G (MX240, MX480, and MX960)---Starting in Junos OS Release 16.1, the Routing Engine RE-S-X6-64G is supported on MX240, MX480, and MX960 routers. This Routing Engine has an increased computing capability and scalability to support the rapid rise in the data plane capacity. The Routing Engine is based on a modular, virtualized architecture and leverages the hardware-assisted virtualization capabilities.

The Routing Engine has a 64-bit CPU and supports a 64-bit kernel and 64-bit applications. With its multicore capabilities, the Routing Engine supports symmetric multiprocessing in the Junos OS kernel and hosted applications.

NOTE: The Routing Engine RE-S-X6-64G is supported only on SCBE2, and it is not compatible with the SCB or the SCBE.

New Routing Engine REMX2K-X8-64G (MX2010, MX2020)---Starting in Junos OS Release 16.1, the Routing Engine REMX2K-X8-64G is supported on MX2010 and MX2020 routers. This Routing Engine has an increased computing capability and scalability to support the rapid rise in the data plane capacity. The Routing Engine is based on a
modular virtualized architecture and leverages the hardware-assisted virtualization capabilities.

The Routing Engine has a 64-bit CPU and supports a 64-bit kernel and 64-bit applications. With its multicore capabilities, the Routing Engine supports symmetric multiprocessing in the Junos OS kernel and hosted applications.

- **New MPC variants that support higher scale and bandwidth (MX Series)**—Starting with Junos OS Release 16.1, MPC7E (Multi-Rate), MPC7E 10G, MPC8E, and MPC9E are supported on MX Series routers. Table 2 on page 55 lists the platforms that support these MPCs.

### Table 2: Supported Platforms

<table>
<thead>
<tr>
<th>MPC</th>
<th>Supported Platforms</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPC7E (Multi-Rate)</td>
<td>MX240, MX480, MX960, MX2010, and MX2020</td>
</tr>
<tr>
<td>MPC7E 10G</td>
<td>MX240, MX480, MX960, MX2010, and MX2020</td>
</tr>
<tr>
<td>MPC8E</td>
<td>MX2010 and MX2020</td>
</tr>
<tr>
<td>MPC9E</td>
<td>MX2010 and MX2020</td>
</tr>
</tbody>
</table>

See [MIC/MPC Compatibility](#) for supported MICs on these MPCs.

---

**NOTE:** MPC7E (Multi-Rate) MPC is also supported in Junos OS Release 15.1F4. MPC7E 10G, MPC8E, and MPC9E MPCs are also supported in Junos OS Release 15.1F5. To use these MPCs in these releases, you must install Junos Continuity software. See [Junos Continuity Software](#) for more details.
Authentication, Authorization, and Accounting

- Logging out idle root users from C shell or CLI console session (MX Series)—Starting with Junos OS Release 16.1, idle users (including root users) are logged out of their C shell or CLI console session after the expiry of the configured maximum idle timeout period.

Class of Service (CoS)

- Support for suppressing the default classifier (MX Series)—Beginning with Junos OS Release 16.1R1, you can disable the application of the default classifier on an interface or a routing instance to preserve the incoming classifier. This is done by applying the no-default option at the [edit class-of-service routing-instances routing-instance-name classifiers] hierarchy level. This is useful, for example, in a bridge domain, where the default classifier for the interface overrides the configured classifier for the domain.

  [See Applying Behavior Aggregate Classifiers to Logical Interfaces.]

- Support for queuing features on built-in ports to provide customized traffic shaping services (MX80, MX104)—Starting with Junos OS Release 16.1, support for hierarchical class-of-service (HCoS) features such as per-unit scheduling and hierarchical scheduling is extended to the built-in (fixed) ports on MX80 and MX104 routers. The MX104 has four built-in ports: xe-2/0/0, xe-2/0/1, xe-2/0/2, and xe-2/0/3. The MX80 also has four built-in ports: xe-0/0/0, xe-0/0/1, xe-0/0/2, and xe-0/0/3. You can enable scheduling and shaping on a logical interface and provide customized traffic shaping services for the logical interface, and this configuration is independent of any configuration on other logical interfaces on a given physical interface. You can configure per-unit scheduling by including the per-unit-scheduler statement at the [edit interfaces interface-name] hierarchy level. To configure hierarchical scheduling, include the hierarchical-scheduler statement at the [edit interfaces interface-name] hierarchy level.

- Timestamping of class-of-service (CoS) queues for a configured Flexible PIC Concentrator (MX Series)—Starting in Junos OS Release 16.1, you can configure the Packet Forwarding Engine to collect the timestamp for all inbound and outbound queue counters for all subscribers that are configured on the Flexible PIC Concentrator (FPC) and, when requested, also return statistics corresponding to data traffic on the router.

  To configure the timestamp for an FPC, include the packet-timestamp enable statement at the [edit chassis fpc slot-number traffic-manager] hierarchy level.

  [See Enabling a Timestamp for Ingress and Egress Queue Packets]

- Support for packet-marking schemes on a per-customer basis (MX Series)—Traditionally, packet marking in the Junos OS uses the forwarding class and loss priority determined from a BA classifier or multifield classifier. This approach does not allow rewrite rules to be directly assigned for each customer because of the limited number of combinations of forwarding class and loss priority.

  Beginning with Junos OS Release 16.1R1, a new packet-marking scheme, called policy map, enables you to define rewrite rules on a per-customer basis. Policy maps are
defined at the [edit class-of-service policy-map] hierarchy level and can be assigned to a customer through a firewall action, an ingress interface, or a routing policy. [See Assigning Rewrite Rules on a Per-Customer Basis Using Policy Maps Overview.]

- **Enhanced ingress queuing support for built-in ports (MX80, MX104)**—Starting with Junos OS Release 16.1, support for ingress queuing is extended to the built-in (fixed) ports on MX80 and MX104 routers. The MX104 has the following four built-in ports: xe-2/0/0, xe-2/0/1, xe-2/0/2, and xe-2/0/3. The MX80 also has four built-in ports: xe-0/0/0, xe-0/0/1, xe-0/0/2, and xe-0/0/3. In this release, for the MX80 and MX104, the maximum number of ports that can support ingress queuing is increased from 10 to 12. You can distribute the 12 ingress queuing ports among MIC ports and built-in ports. Therefore, you can select a combination of ports (including MIC ports and built-in ports) for ingress queuing. To enable ingress queuing, specify ingress-and-egress as the value of the mode statement at the [edit chassis fpc fpc-slot-number pic pic-slot-number traffic-manager] hierarchy level.

**NOTE:** The systemwide hierarchical queuing bandwidth remains the same and is shared by built-in ports and MIC ports. Enabling ingress queuing on built-in ports results in a Packet Forwarding Engine restart, and requires a two-step commit operation.

In releases before Junos OS Release 16.1, ingress queuing is supported only on MIC ports and not on built-in ports, and the maximum number of ports that support ingress queuing is 10.

- **Hierarchical CoS support for GRE tunnel interface output queues (MX Series routers with MPC5E)**—Starting with Junos OS Release 16.1R1, you can manage output queuing of traffic entering GRE tunnel interfaces hosted on MPC5E line cards in MX Series routers. Support for the output-traffic-control-profile configuration statement, which applies an output traffic scheduling and shaping profile to the interface, is extended to GRE tunnel physical and logical interfaces. Support for the output-traffic-control-profile-remaining configuration statement, which applies an output traffic scheduling and shaping profile for remaining traffic to the interface, is extended to GRE tunnel physical interfaces.

**NOTE:** Interface sets (sets of interfaces used to configure hierarchical CoS schedulers on supported Ethernet interfaces) are not supported on GRE tunnel interfaces.

[See Configuring Traffic Control Profiles for Shared Scheduling and Shaping.]

**EVPN**

- **EVPN with VXLAN data plane encapsulation (MX Series)**—Starting in Junos OS Release 16.1, MX Series routers can use EVPN with VXLAN encapsulation to provide Layer 2 connectivity for end stations within a Virtualized Network (VN) created by the Contrail virtualization software. The end stations consist of virtual hosts connected to
the virtualized server, and non-virtualized bare metal servers connected to top-of-rack platforms. MX Series routers also function as default gateways for the inter-VN traffic among end stations that belong to different VNs. EVPN is used as a Layer 2 overlay solution to provide Layer 2 connections over the IP underlay for the endpoints within a VN whenever Layer 2 connectivity is required by an end station.

- **Active-active multihoming support for EVPN**s (MX Series with MPCs and MICs only)—Starting with Junos OS Release 15.1F6 and 16.1R1, the Ethernet VPN (EVPN) solution on MX Series routers with MPC and MIC interfaces is extended to provide multihoming functionality in the active-active redundancy mode of operation. This feature enables load balancing of Layer 2 unicast traffic across all the multihomed links on and toward a customer edge device.

  The EVPN active-active multihoming feature provides link-level and node-level redundancy along with effective utilization of resources.

  To enable EVPN active-active multihoming, include the `all-active` statement at the `[edit interfaces esi]` hierarchy level.

  ![EVPN Multihoming Overview](image)
  ![Example: Configuring EVPN Active-Active Multihoming](image)

**General Routing**

- **Support for fabric management on MPC7E-MRATE and MPC7E-10G MPCs (MX240, MX480, and MX960 routers)**—Fabric management is implemented on MPC7E-MRATE and MPC7E-10G MPCs and is supported in Junos OS Release 16.1R1. The MX960 router supports a maximum of six fabric planes (two per MX-SCBE2), and the MX240, and MX480 routers support a maximum of eight fabric planes (four per MX-SCBE2).

  ![NOTE: The MPC7E-MRATE, and MPC7E-10G MPCs are supported only on MX-SCBE2.](image)

  ![NOTE: Fabric management is supported on the MPC7E-MRATE and MPC7E-10G MPCs in Junos OS Releases,15.F4, 15.1F5 with respective JAM packages, and in 15.1F6.](image)

- **Support for virtualization on RE-S-X6-64G (MX240, MX480, MX960, MX2010, and MX2020)**—The Routing Engine RE-S-X6-64G supports virtualization for the following platforms:
  - MX240, MX480, and MX960—Junos OS Release 15.1F3 and later
  - MX2010 and MX2020—Junos OS Release 15.1F5 and later

  Virtualization enables the router to support multiple instances of Junos OS and other operating systems on the same Routing Engine. However, for Junos OS Release 15.1F3, one instance of Junos OS, which runs as a guest operating system, is launched by default. The user needs to log in to this instance for operations and management. For more information see, `RE-MX-X6, RE-MX-X8, and RE-PTX-X8 with VM Host Support`.
With virtualization of the Routing Engine, Junos OS supports new request and show commands associated with host and hypervisor processes. The commands are related to:

- Reboot, halt, and power management for the host
- Software upgrade for the host
- Disk snapshot for the host

### High Availability and Resiliency

#### Support for unified in-service software upgrade (MX Series)
Starting in Release 16.1, Junos OS extends support for unified in-service software upgrade (unified ISSU) for the following MICs:

- **Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP** (MIC-3D-4OC3-1OC12-CE)
- **Channelized E1/T1 Circuit Emulation MIC** (MIC-3D-16CHE1-T1-CE)
- **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)

Unified ISSU is a process to upgrade the system software with minimal disruption of transit traffic and no disruption of the control plane. You can use unified ISSU only to upgrade to a later version of the system software. When unified ISSU completes, the new system software state is identical to that of the system software when the system upgrade is performed through a cold boot.

**NOTE:** This feature is documented but not supported in Junos OS Release 16.1R1.

#### High availability for IPsec on MS-MPCs
Starting in Junos OS Release 16.1, you can use the new one-to-one statement at the [edit interfaces interface-name load-balancing-options high-availability-options] hierarchy level to configure one-to-one redundancy (1:1) between a pair of interfaces. If the active interface fails, the backup interface takes over. The one-to-one statement configures synchronization between the two interfaces, which creates support for IPsec connections over the redundant interfaces.

#### Support for unified in-service software upgrade on MX Series routers with MPC5E and MPC6E
Starting with Release 15.1F2 and 16.1R1, Junos OS supports unified in-service software upgrade (unified ISSU) on MX Series routers with MPC5E (MPC5E-40G10G, MPC5E-100G10G), MPC5EQ (MPC5EQ-40G10G, MPC5EQ-100G10G), and MPC6E (MX2K-MPC6E). Also, in this release, Junos OS extends support for unified ISSU on the following MICs that are supported on MPC6E:

- **10-Gigabit Ethernet MIC with SFP+ (24 Ports)**
- **10-Gigabit Ethernet DWDM OTN MIC** (non-OTN mode only)
• 100-Gigabit Ethernet MIC with CFP2 (non-OTN mode only)

• 100-Gigabit Ethernet MIC with CXP (4 Ports)

Unified ISSU is a process to upgrade the system software with minimal disruption of transit traffic and no disruption of the control plane. You can use unified ISSU only to upgrade to a later version of the system software. When unified ISSU completes, the new system software state is identical to that of the system software when the system upgrade is performed through a cold boot.

• Configure BFD over LAG using AE interface addresses (MX Series)—Beginning with Junos OS Release 16.1, you can configure BFD over child links of an AE or LAG bundle using AE interface addresses also, thereby conserving routable IP addresses. In earlier Junos releases, you could configure BFD over LAG using loopback addresses only. To configure BFD over LAG using AE interface addresses or loopback addresses, include the bfd-liveness-detection statement at the [edit interfaces aex aggregated-ether-options bfd-liveness-detection] hierarchy level. Disable duplicate address detection before configuring this feature for the IPv6 address family.

[See Understanding Independent Micro BFD Sessions for LAG.]

Interfaces and Chassis

• Maximum generation rate for ICMP and ICMPv6 messages is configurable (MX Series)—Starting in Junos OS Release 16.1, you can configure the maximum rate at which ICMP and ICMPv6 messages that are not ttl-expired are generated by using the icmp rate limit and icmp6 rate limit configuration statements at the [edit chassis] hierarchy level.

• Clock Synchronization feature support on non-Ethernet MICs—Starting in Release 16.1R1, Junos OS extends clock synchronization support for the MIC-3D-1OC192-XFP on the MX104 router. This feature enables the selection of the best timing source based upon the Synchronization Status Message (SSM).

• Support for GPS external clock interface on the MX2020 Control Board (MX2020)—Starting with Junos OS Release 16.1, you can configure the external clock interface on the MX2020 Control Board to select the global positioning system (GPS) clock source as an input clock source to the centralized timing circuit. You can also configure the external clock interface to select either the chassis clock source or a recovered line clock source with GPS timing signals of 1 MHz, 5 MHz, or 10 MHz with 1 pulse per second (PPS) as the output clock source.

• Support for inline Two-Way Active Measurement Protocol (TWAMP) server on MPC5E (MX240, MX480, MX960, MX2010, and MX2020)—You can now configure an inline TWAMP server as part of the inline services (si-) interface processing for MPC5E interfaces. TWAMP is an open protocol for measuring network performance between any two devices that support TWAMP. To configure the TWAMP server, specify the logical interface on the service PIC that provides the TWAMP service by including the twamp-server statement at the [edit interfaces si-fpc/pic/port unit logical-unit-number family inet] hierarchy level. You can also specify the TWAMP server properties by including the server statement at the [edit services rpm twamp] hierarchy level.
• Support to monitor physical Ethernet (10G, 40G, and 100G) links, detect link degradation, and trigger fast-reroute to minimize packet loss (MX Series Routers with MPC3, MPCE, and MPC4E)—Starting with Junos OS Release 16.1R1, you can monitor the physical link degrade (indicated by bit error rate BER levels) and take corrective actions when [BER] levels drop in the range of $10^{-13}$ to $10^{-5}$.

Layer 2 and Layer 3 protocols support the monitoring of a physical link degrade and so does the Ethernet link through the Link Fault System (LFS). However, for both these monitoring mechanisms, the BER range of $10^{-13}$ to $10^{-5}$ is very low. Due to its low BER level, the physical link degrade goes undetected, causing disruption and packet loss on an Ethernet link.

Following new configurations have been introduced at the [edit interfaces interface-name] hierarchy level to support this feature in Junos OS:

- To monitor physical link degrade on Ethernet interfaces, configure the link-degrade-monitor statement.
- To configure the BER threshold value at which the corrective action should be triggered or cleared from an interface, use the link-degrade-monitor thresholds (setvalue | clearvalue) statement. The value is the BER threshold value in a scientific notation. You can configure this value in the 1E-n format, where 1 is the mantissa (remains constant) and n is the exponent. For example, a threshold value of 1E-3 refers to the BER threshold value of $1 \times 10^{-3}$.

The supported exponent range is 1 through 16 and the default value is

- To configure the link degrade interval value, use the link-degrade-monitor thresholds interval value statement. The interval value configured, determines the number of consecutive link degrade events that are considered before taking any corrective action. The supported value range for the interval is 1 through 256, and the default interval is 10.

- To configure link degrade warning thresholds, use the link-degrade-monitor thresholds (warning-set value | warning-clear value) statement. The value is again specified in the 1E-n format and the supported value range for n is 1 through 16. With this configuration, every time the BER threshold value is reached, a system message is logged to indicate that a link degrade has occurred (warning-set) or the link degrade has been cleared (warning-clear) on an interface.

- To configure the link degrade action that is taken on reaching the configured BER threshold levels, use the link-degrade action media-based statement. A media-based action brings down the physical interface at the local end of the interface, and stops BER monitoring on the interface (though link fail is active at the local end and the recovery fail is active on the remote end of the degraded link) until an autorecovery mechanism is triggered.

- To configure the link degrade recovery options, use the link-degrade recovery (auto interval value | manual) statement. The recovery mechanism triggers the recovery of a degraded link.

auto recovery is used with the media-based action when there are no Layer 2 or Layer 3 protocols configured on the interface. With the auto recovery option, you must
configure the interval in seconds, after which the system triggers the auto recovery mechanism on a degraded link. The default interval is 1800 seconds.

The manual recovery option is configured with media-based action configuration when Layer 2 and Layer 3 protocols are configured on an interface. To trigger manual recovery, use the request interface link-degrade-recovery interface-name statement.

- **Support for ITU-T Y.1731 ETH-LM, ETH-SLM, and ETH-DM on aggregated Ethernet interfaces (MX Series routers with MPCs)**—Starting in Junos OS Release 16.1, you can configure ITU-T Y.1731 standard-compliant Ethernet loss measurement (ETH-LM), Ethernet synthetic loss measurement (ETH-SLM), and Ethernet delay measurement (ETH-DM) capabilities on aggregated Ethernet (AE) interfaces. These performance monitoring functionalities are supported on MX Series routers with MPCs, where the same level of support for the Ethernet services OAM mechanisms as the level of support on non-aggregated Ethernet interfaces is available on AE interfaces. ETH-DM is supported on MPC3E and MPC4E modules with only software timestamping. ETH-SLM is supported on MPC3E and MPC4E modules.

- **Optical transceiver support for MX104**—Starting with Release 16.1R1, Junos OS extends support for the following optical transceivers on MX104 routers:
  - SFP-1FE-FX-Manufactured by Fiberxon—supports Gigabit Ethernet MIC with SFP (MIC-3D-20GE-SFP), Gigabit Ethernet MIC with SFP (E) (MIC-3D-20GE-SFP-E), and Gigabit Ethernet with SFP (EH) (MIC-3D-20GE-SFP-EH)
  - SFP-1FE-FX-Manufactured by Avago—supports Gigabit Ethernet MIC with SFP (E) (MIC-3D-20GE-SFP-E) and Gigabit Ethernet with SFP (EH) (MIC-3D-20GE-SFP-EH), but does not support Gigabit Ethernet MIC with SFP (MIC-3D-20GE-SFP)
  - SFP-1GE-FE-E-T
  - SFP-1GE-LH
  - SFP-1GE-LX
  - SFP-1GE-SX-ET
  - SFP-GE10KT13R14
  - SFP-GE10KT14R13
  - SFP-GE40KM
  - SFP-GE40KT13R15
  - SFP-GE40KT15R13
  - SFP-GE80KCW1470-ET
  - SFP-GE80KCW1550-ET
  - SFP-GE80KCW1610-ET
  - SFP-T-ET
  - SFP-LX-ET
  - SFPP-10GE-ER
  - SFPP-10GE-ZR
• Increased tunnel bandwidth for inline tunnel services (MX240, MX480, MX960, MX2010, and MX2020 routers)—Starting with Junos OS Release 16.1R1, the tunnel bandwidth is increased for MPC7E-10G, MPC7E-MRATE, MX2K-MPC8E, and MX2K-MPC9E. The maximum bandwidth per tunnel is 120 Gbps for MPC7E-10G, MPC7E-MRATE, and MX2K-MPC8E, and 200 Gbps for MX2K-MPC9E. The `bandwidth` command for tunnel services is enhanced to configure the tunnel bandwidth from 1 Gbps through 400 Gbps, with increments of 1 Gbps.

• Support for Ethernet OAM on MPC7E-MRATE, MPC7E-10G, MX2K-MPC8E, and MX2K-MPC9E (MX240, MX480, MX960, MX2010, and MX2020 routers)—Starting in Release 16.1R1, Junos OS extends MPLS support for MPC7E-MRATE, MPC7E-10G, MX2K-MPC8E, and MX2K-MPC9E.

• Support for Ethernet OAM on MPC7E-MRATE, MPC7E-10G, MX2K-MPC8E, and MX2K-MPC9E (MX240, MX480, MX960, MX2010, and MX2020 routers)—Starting in Release 16.1R1, Junos OS extends Ethernet OAM support for MPC7E-MRATE, MPC7E-10G, MX2K-MPC8E, and MX2K-MPC9E.

• Support for scaling on MPC7E-MRATE, MPC7E-10G, MX2K-MPC8E, and MX2K-MPC9E (MX240, MX480, MX960, MX2010, and MX2020 routers)—Starting in Junos OS Release 16.1R1, MPC7E-MRATE, MPC7E-10G, MX2K-MPC8E, and MX2K-MPC9E are supported on MX Series routers. These MPcs support scaling and performance values that are equivalent to the scaling and performance values supported by MPcs such as MPC6E, MPC5E, MPC2E-3D-NG/NG-Q, and MPC2E-3D-NG/NG-Q.

• Support for hyper mode feature on MPC7E-MRATE, MPC7E-10G, MX2K-MPC8E, and MX2K-MPC9E (MX240, MX480, MX960, MX2010, and MX2020)—The hyper mode feature is supported on MPC7E-MRATE, MPC7E-10G, MX2K-MPC8E, and MX2K-MPC9E. The hyper mode feature enhances the performance and throughput of a router by increasing the data packet processing rate and optimizes the lifetime of a data packet.

To configure the hyper mode feature, use the `hyper-mode` statement at the [edit forwarding-options] hierarchy level.

• Support for flexible queuing on MPC7E-MRATE, MPC7E-10G, MX2K-MPC8E, and MX2K-MPC9E (MX240, MX480, MX960, MX2010, and MX2020)—The flexible queuing feature is supported on non-hierarchical quality-of-service (non-HQoS) MPcs MPC7E-MRATE, MPC7E-10G, MX2K-MPC8E, and MX2K-MPC9E. By default, the non-HQoS MPcs do not support flexible queuing. You can enable flexible queuing on these MPcs by including the `flexible-queuing-mode` statement at the [edit chassis fpc] hierarchy level. When flexible queuing is enabled, non-HQoS MPcs support a limited queuing capability of 32,000 queues per slot, including ingress and egress.

• Configuration support to improve convergence (MX Series)—Starting with Junos OS Release 16.1R1, you can configure multichassis link aggregation (MC-LAG) interfaces to improve Layer 2 and Layer 3 convergence time to subsecond values when a multichassis aggregated Ethernet link goes down or comes up in a bridge domain.

To use this feature, ensure that the interchassis link (ICL) is configured on an aggregated Ethernet interface. For Layer 2 convergence, configure the `enhanced-convergence` statement at the [edit interfaces aeX aggregated-ether-options mc-ae] hierarchy level.
For Layer 3, configure the `enhanced-convergence` statement at the `[edit interfaces irb unit unit-number]` hierarchy level for an integrated routing and bridging (IRB) Interface.

**NOTE:**
- If the `enhanced-convergence` feature is configured on an multichassis aggregated Ethernet interface of a bridge domain that has an IRB interface, the IRB interface must also be configured for the convergence feature.
- All multichassis aggregated Ethernet interfaces that are part of a bridge domain must be configured for enhanced convergence in order to utilize this feature on any of them.
- On enabling or disabling the enhanced convergence feature, all services get deleted and re-created.

[See Configuring Active-Active Bridging and VRRP over IRB in Multichassis Link Aggregation on MX Series Routers, Configuring Multichassis Link Aggregation on MX Series Routers.]

- **LACP hold-up timer configuration support on LAG interfaces**—Starting with Junos OS Release 16.1R1, you can configure a Link Aggregation Control Protocol (LACP) hold-up timer value for link aggregation group (LAG) interfaces.

You configure the hold-up timer to prevent excessive flapping of a child (member) link of a LAG interface due to transport layer issues. With transport layer issues, it is possible for a link to be physically up and still cause LACP state-machine flapping. LACP state-machine flapping can adversely affect traffic on the LAG interface. To prevent this, a hold-up timer value is configured. LACP monitors the PDUs received on the child link for the configured time value, but does not allow the member link to transition from the expired or defaulted state to current state. This configuration thus prevents excessive flapping of the member link.

To configure the LACP hold-up timer for LAG interfaces, use the `hold-time up timer-value` statement at the `[edit interfaces ae aeX aggregated-ether-options lacp]` hierarchy level.
• Initialization delay timer feature support on LAG interfaces (MX Series)—Starting with Junos OS Release 16.1R1, you can configure an initialization delay timer value on link aggregation group (LAG) interfaces.

When a stand-by multichassis aggregated Ethernet (MC-AE) interface reboots to come up in active-active MC-AE mode, the Link Aggregation Control Protocol (LACP) protocol comes up faster than the Layer 3 protocols. As soon as LACP comes up, the interface is UP and starts receiving traffic from the neighboring interfaces. In absence of the routing information, the traffic received on the interface is dropped, causing traffic loss.

The initialization delay timer, when configured, delays the MC-AE node from coming UP for a specified amount of time. This gives the Layer 3 protocols time to converge on the interface and prevent traffic loss.

To configure the initialization delay timer on an MC-AE interface, use the `init-delay-timer` statement at the `[edit interfaces ae-interface-name aggregated-ether-options mc-ae]` hierarchy level.

• Support for ARP cache protection to prevent DOS attacks (MX Series and T Series)—Starting in Junos OS Release 16.1, you can configure an ARP cache limit for resolved and unresolved next-hop entries in the cache. This limits the maximum number of next hops that can be created. The benefit of configuring ARP cache limit is to protect the device from DOS attacks. You can configure the cache limit globally at the system level or for a particular interface. To configure the cache limit at the system level, include the `arp-system-cache-limit` statement at the `[edit system]` hierarchy level. To configure the cache limit at an interface level, include the `arp-max-cache` statement at the `[edit interfaces interface-name unit interface-unit-number family inet]` hierarchy level. To configure the maximum number of unresolved next-hop entries to hold for an interface, set the `arp-new-hold-limit` statement at the `[edit interfaces interface-name unit interface-unit-number family inet]` hierarchy level. To view ARP cache statistics at the system level, run the `show system statistics arp` command. To view the ARP cache statistics for an interface, run the `show interfaces interface-name` command.

• Synchronous Ethernet support on MPC7E-MRATE, MPC7E-10G, MX2K-MPC8E, and MX2K-MPC9E (MX240, MX480, MX960, MX2010, and MX2020)—Starting with Junos OS Release 16.1R1, Synchronous Ethernet with Ethernet Synchronization Message Channel is supported on MPC7E-MRATE, MPC7E-10G, MX2K-MPC8E, and MX2K-MPC9E.

• Disabling fabric grant bypass mode for better performance (MX2010 and MX2020)—Fabric grant bypass mode is enabled, by default, for all MPCs on MX2010 and MX2020 routers. Disabling fabric grant bypass mode controls congestion and thus improves system behavior and performance on MX2010 and MX2020 routers. Starting with Junos OS Release 16.1, you can disable fabric grant bypass mode on MX2010 and MX2020 routers by including the `disable-grant-bypass` configuration statement at the `[edit chassis fabric]` hierarchy level.
NOTE: After disabling fabric grant bypass mode on the MX2010 and MX2020, you must reboot the router for the changes to take effect. MPC1 (MX-MPC1-3D), MPC2 (MX-MPC2-3D), and the 16-port 10-Gigabit Ethernet MPC (MPC-3D-16XGE-SFP) do not power on after you disable fabric grant bypass mode and reboot the router.

• Support for asynchronous notification on MIC-8OC3OC12-4OC48-SFP and MIC-1OC192-HO-VC-XFP (MX240, MX480, MX960, MX2010, and MX2020 routers)—Starting in Junos OS Release 16.1R1, the asynchronous-notification command is supported at the [edit interfaces interface-name sonet-options] hierarchy level for the MICs MIC-8OC3OC12-4OC48-SFP and MIC-1OC192-HO-VC-XFP.

In a network comprising SONET and Ethernet interfaces connected through a TCC circuit, if an interface goes down, you can use the asynchronous-notification command to disable the physical interface on the remote end, thereby notifying the loss of signal (LOS) and loss of connection.

• Routing Engine failover detection (MX240, MX480, MX960, MX2010, and MX2020)—Starting with Junos OS Release 16.1, you use the on-re-to-fpc-stale configuration statement at the [edit chassis redundancy failover] hierarchy level to instruct the backup Routing Engine to take the mastership if the em0 interface fails on the master Routing Engine.

• Upgrading MPC8E bandwidth from 960 Gbps to 1600 Gbps (MX2010 and MX2020)—Starting in Junos OS Release 16.1R1, you can upgrade MPC8E to provide an increased bandwidth of 1600 Gbps (1.6 Tbps), by using an add-on license. After you purchase the license and perform the upgrade, MPC8E provides a bandwidth of 1.6 Tbps, which is equivalent to that of MPC9E. However, the MPC continues to be identified as MPC8E.

NOTE: After you upgrade MPC8E to provide a bandwidth of 1.6 Tbps, the power consumption by MPC8E increases and is equivalent to the power that MPC9E consumes.

You upgrade the bandwidth by using the set chassis fpc slot bandwidth 1.6T command. You can disable this feature by using the delete chassis fpc slot bandwidth 1.6T command.

[See MPC8E on MX Series Routers Overview.]

• Configuration support for multiple up MEps for interfaces belonging to a single VPLS service or a bridge domain (MX Series with MPC)—Starting with Junos OS Release 16.1R1, you can configure multiple up maintenance association endpoints (MEP) for a single combination of maintenance association ID and maintenance domain ID for interfaces belonging to a particular VPLS service or a bridge domain.

To configure multiple up MEps, specify mep mep-id statement at the [edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name}
**maintenance association ma-name** hierarchy level, when the MEP direction is configured as direction up.

- **Enhancement to ambient-temperature statement (MX Series)**—Starting in Junos OS Release 16.1R1, the default ambient temperature is set at 40°C on MX480, MX960, MX2010, and MX2020 3D Universal Edge Routers. You can override ambient temperature by setting the temperature at 55°C or 25°C.

```
[edit]
user@router# set chassis ambient-temperature ?
Possible completions:
25C 25 degree celsius
40C 40 degree celsius
55C 55 degree celsius
[edit]
```

When a router restarts, the system adjusts the power allocation or the provisioned power for the line cards on the basis of the configured ambient temperature. If enough power is not available, a minor chassis alarm is raised. However, the chassis continues to run with the configured ambient temperature. You can configure a new higher ambient temperature only after you make more power available by adding new power supply modules or by taking a few line cards offline. By using the provisioned power that is saved by configuring a lower ambient temperature, you can bring more hardware components online.

- **Support for fabric black-hole detection and recovery in TX Matrix Plus routers**—TX Matrix Plus routers can detect and recover from fabric faults that are not caused by hardware failure but might be a result of a fabric black-hole condition.

To recover from a fabric black-hole condition, the routing matrix uses the following options:

- SIB reboot
- FPC reboot
- Destination reprogramming
- Related faults recovery

You can disable the automatic recovery feature by using the **auto-recovery-disable** statement at the **[edit chassis fabric degraded]** hierarchy level. You can configure the FPCs to go offline when a traffic black-hole condition is detected in the routing matrix by using the **fpc-offline-on-blackholing** statement at the **[edit chassis fabric degraded]** hierarchy level.

You can configure the FPCs to restart when a traffic black-hole condition is detected in the routing matrix by using the **fpc-restart** statement at the **[edit chassis fabric degraded]** hierarchy level.

[See **auto-recovery-disable** and **fpc-offline-on-blackholing**.]
IPv4

- **IPv4 address conservation method for hosting providers (MX Series)**—Starting with Junos OS Release 14.2R4, Release 15.1R1, Release 16.1R1, and later releases, you can configure a static route on an integrated routing and bridging (IRB) interface with or without pinning to a specific underlying interface, thereby conserving the usage of IP address space.

When a customer needs servers to be assigned within a block of IP addresses, several IP addresses are consumed. These include the network and broadcast IP addresses, the addresses for the router gateway that the servers are connected to, and the addresses of the individual servers. When this effect is multiplied across thousands of hosting providers, IP address space is underutilized.

This issue can be resolved by configuring the router interface with an address from the reserved IPv4 prefix for shared address space (RFC 6598) and by using static routes pointed at that interface. Internet Assigned Numbers Authority (IANA) has recorded the allocation of an IPv4 /10 for use as shared address space. The shared address space address range is 100.64.0.0/10.

This way, the router interface is allocated an IP address from the shared address space, so it is not consuming publicly routable address space, and connectivity is handled with static routes on the interface. The interface in the server is configured with a publicly routable address, but the router interfaces are not. Network and broadcast addresses are consumed out of the shared address space rather than the publicly routable address space.

**Junos OS XML API and Scripting**

- **Support for Python language for commit, event, op, and SNMP scripts (MX Series and T Series)**—Starting in Junos OS Release 16.1, you can author commit, event, op, and SNMP scripts in Python on devices that include the Python extensions package in the software image. Creating automation scripts in Python enables you to take advantage of Python features and libraries as well as leverage Junos PyEZ APIs supported in Junos PyEZ Release 1.3.1 and earlier releases to perform operational and configuration tasks on devices running Junos OS. To enable execution of Python automation scripts, which the root user must own, configure the language python statement at the [edit system scripts] hierarchy level, and configure the filename for the Python script under the hierarchy level appropriate to that script type. Supported Python versions include Python 2.7.x.

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

**Layer 2 Features**

- **Support for MAC pinning to prevent loops (MX Series)**—A MAC move occurs when a MAC address frequently appears on a different physical interface than the one it was learned on. Frequent MAC moves indicate the presence of loops in Layer 2 bridges and in VPLS networks. To avoid loops, you can enable the MAC pinning feature on an interface.
Starting in Junos OS Release 16.1, support for MAC pinning is provided to prevent loops in Layer 2 bridges and in VPLS networks.

When you enable MAC pinning on an interface in a bridge domain or VPLS domain, a MAC address learned over that interface cannot be relearned on any other interface in the same bridge domain or VPLS domain until the MAC address either ages out on the first interface or is cleared from the MAC table. If a packet with the same MAC address arrives at any other interface in the same bridge domain, then the packet is discarded. This action, effectively, controls MAC moves and prevents the creation of loops in Layer 2 bridges and VPLS domains.

**NOTE:** If you do not specify the timeout interval for the MAC addresses by configuring the `mac-table-aging-time` statement, the MAC addresses learned over the MAC pinning interface are pinned to the interface until the default timeout period expires.

- **Enhanced convergence time required for IRB ARP resolution (MX Series)**—Starting with Junos OS Release 16.1, the convergence of IRB ARP resolution when the underlying L2 IFL association with the MAC changes due to link failure or MAC move improves when both enhanced-convergence and enhanced-ip chassis is configured. The `show arp` and `show ipv6 neighbor` command does not display the underlying IFL information if the destination interface is IRB.

- **Support for Layer 2 port mirroring to a remote collector over a GRE Interface (MX Series)**—Starting with Junos OS Release 16.1, Layer 2 port mirroring to a remote collector over a GRE Interface is supported.

**Management**

- **YANG module that defines CLI formatting for RPC output (MX Series and T Series)**—Starting with Junos OS Release 16.1, Juniper Networks provides the `junos-extension-odl` YANG module. The module contains definitions for Junos OS Output Definition Language (ODL) statements, which determine the CLI formatting for RPC output when you execute the operational command corresponding to that RPC in the CLI or when you request the RPC output in text format. You can use statements in the `junos-extension-odl` module in custom RPCs to convert the XML output into a more logical and human-readable representation of the data. The `junos-extension-odl` module is bound to the namespace URI `http://yang.juniper.net/yang/1.1/jodl` and uses the prefix `junos-odl`.

  [See Understanding Junos OS YANG Extensions for Formatting RPC Output.]

- **YANG module that defines Junos OS operational commands (MX Series and T Series)**—Starting with Junos OS Release 16.1, Juniper Networks provides the `juniper-command` YANG module, which represents the operational command hierarchy and collective group of modules that define the remote procedure calls (RPCs) for Junos OS operational mode commands. You can download Juniper Networks YANG modules from the website, or you can generate the modules by using the `show system schema format yang module juniper-command` operational command on the local
device. The `juniper-command` module is bound to the namespace URI http://yang.juniper.net/yang/1.1/jrpc and uses the prefix `jrpc`. 

[See Understanding the Juniper Networks YANG Modules for Operational Commands.]

**Support for adding non-native YANG modules to the Junos OS schema (MX Series and T Series)**—Starting with Junos OS Release 16.1, you can load standard (IETF, OpenConfig) or custom YANG models on devices running Junos OS to add data models that are not natively supported by Junos OS but can be supported by translation. Doing this enables you to augment the configuration hierarchies with data models that are customized for your operations. The ability to add data models to a device is also beneficial when you want to create device- and vendor-agnostic configuration models that enable the same configuration to be used on different devices from one or more vendors. You can load YANG modules that add configuration hierarchies by using the `request system yang add` operational command. 

[See Understanding the Management of Non-Native YANG Modules on Devices Running Junos OS.]

**Juniper Extension Toolkit for Junos (JET for Junos) provides a modern programmatic interface for developers of third-party applications**—As of Junos OS Release 16.1, JET for Junos, an evolution of the Junos SDK, allows customers and partners to build and run applications either directly on Junos OS devices or off-box. These applications can interact with Junos OS native features. A framework is provided in the Python language for Python JET for Junos application developers. This framework allows your applications to run directly on Junos OS devices. JET for Junos is based on Apache Thrift; thus, it also supports multiple languages running off-box to interact with the same JET for Junos APIs. This gives developers true flexibility to adapt Junos OS devices to business processes.

Developers can view JET guides at Juniper Extension Toolkit, Release 1.0. For the JET Applications Guide, see Understanding JET Interaction with Junos OS.

**MPLS**

**Longest matching route for label mapping (MX Series)**—Starting with Junos OS Release 16.1, LDP uses the longest match to learn the routes aggregated or summarized across OSPF areas or IS-IS levels in the interdomain.

**Explicit notifications for pseudowire termination (MX Series)**—Starting with Junos OS Release 16.1R1, MX Series routers can provide notifications on the service node when the access pseudowire goes down, and provide efficient termination capabilities when Layer 2 and Layer 3 segments are interconnected. This feature also provides termination of pseudowire into virtual routing and forwarding (VRF) and virtual private LAN service (VPLS) routing instances without pseudowire redundancy, which includes:

- Termination of an access pseudowire into VRF.
- Termination of an access pseudowire into a VPLS instance.

[See Pseudowire Termination: Explicit Notifications for Pseudowire Down Status.]

**Support for NIST Deterministic Random Bit Generator (DRBG) recommendations (MX Series)**—Starting with Release 16.1, Junos OS supports NIST computer security
standards recommended in Recommendation for Random Number Generation Using Deterministic Random Bit Generators, NIST Special Publication 800-90A; Recommendation for the Entropy Sources Used for Random Bit Generation, NIST DRAFT Special Publication 800-90B; and Recommendation for Random Bit Generator (RBG) Constructions, DRAFT NIST Special Publication 800-90C.

NOTE: Junos OS supports Recommendation for the Entropy Sources Used for Random Bit Generation, NIST DRAFT Special Publication 800-90B and Recommendation for Random Bit Generator (RBG) Constructions, DRAFT NIST Special Publication 800-90C only when the system is operating in Junos-FIPS mode.

• BGP Prefix-Independent Convergence (PIC) Edge for RSVP (MX Series)—Starting with Junos OS Release 16.1, BGP PIC Edge for RSVP enables you to implement a solution where a protection path is calculated in advance to provide an alternative forwarding path in case of path failure.

With BGP PIC Edge in an MPLS VPN network, IGP failure triggers a repair of the failing entries and causes the Packet Forwarding Engine to use the pre-populated protection path until global convergence has re-resolved the VPN routes. This feature helps to reduce the convergence time taken to repair the remote provider edge (PE) link failure, when compared to the traditional approach of re-resolving each prefix. The convergence time is no longer dependent on the number of prefixes.

Earlier, this feature used LDP as the transport protocol, which is now extended to support BGP PIC Edge with RSVP as the transport protocol. When RSVP receives a tunnel down notification at the ingress PE router, it sends a notification to the Packet Forwarding Engine to start making use of the tunnel to the alternate egress PE router. The tunnel route to the alternate egress PE router is calculated and installed in advance.

[See show rsvp version.]

• Protection against incorrect label injection across ASBRs (MX Series)—Starting in Junos OS Release 16.1, you can use regular BGP export policies to control route advertisement to a VPN ASBR peer in a given routing instance. This is especially useful in the service provider context of Inter-AS VPN Option-B ASBRs because it prevents peer ASBRs in a neighboring AS from injecting a VPN label intended for a different peer-AS, or intra-AS PEs, into the common ASBR. The common ASBR only accepts MPLS packets from a peer ASBR that has explicitly advertised the label to the common ASBR.

To support this new functionality, the statement forwarding-context is introduced at the [edit protocols bgp group] hierarchy level, and the instance type mpls-forwarding is introduced at the [edit routing-instances] hierarchy level.

• Support for inet and inet6 families on pseudowire subscriber logical interface (MX Series)—Starting with Junos OS Release 16.1R1, inet and inet6 families are supported on the services side of an MPLS pseudowire subscriber as well as non-subscriber logical interfaces. You use family inet6 to assign an IPv6 address. You use family inet to assign an IPv4 address. A logical interface can be configured with both an IPv4 and IPv6 address.
Support for Inline IPFIX on pseudowire subscriber logical interface (MX Series)—Starting with Junos OS Release 16.1R1, Inline IPFIX is supported on the services side of an MPLS pseudowire subscriber logical interface. With Inline IPFIX you can configure active sampling to be performed on an inline data path without the need for a services Dense Port Concentrator (DPC). To enable this feature, define a sampling instance with specific properties. One Flexible PIC Concentrator (FPC) can support only one instance. For each instance, either services PIC-based sampling or inline sampling is supported per family. As a result, a particular instance can define PIC-based sampling for one family and inline sampling for a different family. Both IPv4 and IPv6 are supported for inline sampling.

RSVP scalability (MX Series and T Series)—Starting with Junos OS Release 16.1, RSVP Traffic Engineering (TE) protocol extensions for fast reroute (FRR) facility protection are introduced to allow greater scalability of LSPs and faster convergence times. RSVP-TE runs in enhanced FRR profile mode by default and includes FRR extensions as defined in RFC 2961. In mixed environments, where a subset of LSPs traverse nodes do not include this feature, RSVP-TE behavior is unchanged—backward compatibility is fundamentally supported in the design.

Enhancements to MPLS RSVP-TE LSP (MX Series and T Series)—The Junos OS implementation of MPLS RSVP-TE is scaled to enhance the usability, visibility, configuration, and troubleshooting of label-switched paths (LSPs) in Junos OS Release 16.1 and later releases. These enhancements make the RSVP-TE configuration easier at scale by:

- Ensuring that the LSP data-plane readiness during LSP resignaling (before traffic traverses the LSP) by using the RSVP-TE LSP self-ping mechanism.
- Removing the current hard limit of 64K LSPs on an ingress router, and thereby enabling scaling to be constrained only by the total number of LSPs RSVP-TE signaling can sustain.
- Preventing abrupt tearing down of LSPs by the ingress router because of delay in signaling the LSP at the transit routers.
- Enabling flexible view of LSP data-sets to facilitate LSP characteristic data visualization.

Leaking MPLS routes to nondefault routing instances (MX Series with MPC/MIC interfaces)—Starting in Junos OS Release 16.1, you can use the import-labeled-routes statement to specify one or more nondefault routing instances where you want MPLS pseudowire labeled routes to be leaked from the mpls.0 path routing table in the master routing instance. This capability prevents traffic loss in an L2VPN/VPLS configuration where the remote PE router is learned from the IGP in a nondefault routing instance. Because ingress-labeled routes are installed only in the master mpls.0 table by default, no route is found in the routing-instance-name.mpls.0 table when L2VPN/VPLS traffic is received on the core-facing interface, and that traffic is dropped.
• Support for Ethernet circuit cross-connect (CCC) encapsulation on pseudowire subscriber logical interface (MX Series)—Starting with Junos OS Release 15.1R3 and 16.1R1 and later releases, CCC encapsulation is supported on the transport side of an MPLS pseudowire subscriber logical interface. This feature helps in migrating or deploying seamless MPLS architectures in access networks. Customers deploying either business edge or broadband residential edge access networks use this feature to configure interfaces over the virtual Ethernet interface similar to what is already available on physical Ethernet interfaces.

You can define only one transport logical interface per pseudowire subscriber logical interface. Although the unit number can be any valid value, we recommend that unit 0 represent the transport logical interface. Two types of pseudowire signaling are allowed: Layer 2 circuit and Layer 2 VPN.

[See Pseudowire Subscriber Logical Interfaces Overview.]

• Support for DDoS on pseudowire subscriber logical interface (MX Series)—Starting with Junos OS Release 15.1R3 and 16.1R1 and later releases, distributed denial-of-service (DDoS) protection is supported on the services side of an MPLS pseudowire subscriber logical interface. DDoS protection identifies and suppresses malicious control packets while enabling legitimate control traffic to be processed. This protection enables the device to continue functioning, even when attacked from multiple sources. Junos OS DDoS protection provides a single point of protection management that enables network administrators to customize a profile appropriate for the control traffic on their networks.

• Support for Policer and Filter on pseudowire subscriber logical interface (MX Series)—Starting with Junos OS Release 15.1R3 and 16.1R1 and later releases, Policer and Filter are supported on the services side of an MPLS pseudowire subscriber logical interface. Policer defines a set of traffic rate limits and sets consequences for traffic that does not conform to the configured limits. Firewall filters restrict traffic destined for the Routing Engine based on its source, protocol, and application. Also, firewall filters limit the traffic rate of packets destined for the Routing Engine to protect against flood or denial-of-service (DoS) attacks.

• Support for accurate transmit logical interface statistics on pseudowire subscriber logical interface (MX Series)—Starting with Junos OS Release 15.1R3 and 16.1R1 and later releases, accurate transmit statistics on logical interface are supported on the services side of an MPLS pseudowire subscriber logical interface. These statistics report actual transmit statistics instead of the offered load statistics given by the router for the pseudowire subscriber service logical interfaces.

[See Pseudowire Subscriber Logical Interfaces Overview.]

• Egress peer engineering of service labels (BGP, MPLS) and egress peer protection for BGP-LU (MX Series)—Beginning with Junos OS Release 14.2R4, you can enable traffic engineering of service traffic, such as MPLS LSP traffic between autonomous systems (ASs), using BGP-labeled unicast for optimum utilization of the advertised egress routes. You can specify one or more backup devices for the primary egress AS boundary router. Junos OS installs the backup path in addition to the primary path in the MPLS forwarding table, which enables MPLS fast reroute (FRR) when the primary link fails.
• **MPLS Encapsulated Payload load-balancing (MX Series)**—Starting with Junos OS Release 16.1, configure `zero-control-word` option to indicate the start of Ethernet frame in an MPLS ether-pseudowire payload. On seeing this control word, four bytes having numerical value of all zeros, the hash generator assumes the start of the Ethernet frame and continues to parse the packet from here and generate hash. For DPC I-chip based cards, configure the `zero-control-word` option at the `[edit forwarding-options hash-key family mpls ether-pseudowire]` hierarchy level, and for MPC cards, configure `zero-control-word` option at the `[edit forwarding-options enhanced-hash-key family mpls ether-pseudowire]` hierarchy level.

• **LDP native IPv6 support (MX Series)**—Starting with Junos OS Release 16.1, LDP is supported in an IPv6 network only, and in an IPv6 or IPv4 dual-stack network. Configure the address family as `inet` for IPv4 or `inet6` for IPv6. By default, IPv6 is used as the TCP transport for an LDP session with its peers when both IPv4 and IPv6 are enabled. The `dual-transport` statement allows Junos OS LDP to establish the TCP connection over IPv4 with IPv4 neighbors, and over IPv6 with IPv6 neighbors as a single-stack LSR. The `inet-lsr-id` and `inet6-lsr-id` are the two LSR IDs that have to be configured to establish an LDP session over IPv4 and IPv6 TCP transport. These two IDs should be non-zero and must be configured with different values.

• **MPLS-TP enhancements for on-demand connectivity verification (MX Series)**—Starting with Junos OS Release 16.1, the transport profile (TP) of MPLS supports two additional channel types for the default LSPING channel type. These additional channel types provide on-demand connectivity verification (CV) with and without IP/UDP encapsulation.

With this feature, the following channel types are supported in the MPLS-TP mode:

• On-demand CV (0x0025)—This channel type is a new pseudowire channel type and is used for on-demand CV without IP/UDP encapsulation, where IP addressing is not available or non-IP encapsulation is preferred.

• IPv4 (0x0021)—This channel type uses the IP/UDP encapsulation and provides interoperability support with other vendor devices using IP addressing.

• LSPING (0x0008)—This is the default channel type for Junos OS, and the GACH-TLV is used along with this channel type.

As per RFC 7026, GACH-TLV is deprecated for 0x0021 and 0x0025 channel types.

To configure a channel type for MPLS-TP, include the `lsping-channel-type channel-type` statement at the `[edit protocols mpls label-switched-path lsp-name oam mpls-tp-mode]` and `[edit protocols mpls oam mpls-tp-mode]` hierarchy levels.
Multicast

- Improved multicast convergence and RPT-SPT support for BGP-MVPN (MX Series)—Starting with Junos OS Release 16.1, support for multicast forwarding-cache threshold is extended to rendezvous-point tree shortest-path tree (RPT-SPT) mode for BGP-MVPN. In addition, for both Rosen and next-generation MVPNs, PE routers across all sites should see the same set of multicast routes even if the configured forwarding-cache limit is exceeded.

To configure a specific threshold for MVPN RPT, set one or both of the mvpn-rpt-suppress and mvpn-rpt-reuse statements at the [edit routing-instances name routing-options multicast forwarding-cache] or [edit logical system name routing-instances name routing-options multicast forwarding-cache] hierarchy level.

In addition, the show multicast forwarding-cache statistics command provides information about both the general and RPT suppression states. Likewise, a list of suppressed customer-multicast states can be seen by running the show mvpn suppressed general| mvpn-rpt inet| inet6 instance name summary command.

- Improved scaling for multicast OIFs (MX Series)—Starting with Junos OS Release 16.1, for both Rosen and NGEN-MVPN, improvements have been made to increase the number of possible outgoing interfaces (OIFs) used in virtual routing and forwarding (VRF). Changes have also been made to improve the efficiency of PIM Join/Prune message processing and to support the increased scaling.

These changes are implemented by default and do not need to be explicitly enabled. The following operational commands support the increased scale:

  - show multicast next-hops terse
  - show multicast route oif-count
  - show multicast statistics interface
  - show pim join downstream-count

- Fast-failover according to flow rate (MX Series with MPCs)—Starting in Junos OS Release 16.1, for routers operating in Enhanced IP Network Services mode, you can configure a threshold that triggers fast failover in NG MVPNs with hot-root standby on the basis of aggregate flow rate. For example, fast failover (as defined in Draft Morin L3VPN Fast Failover 05) is triggered if the flow rate of monitored multicast traffic from the provider tunnel drops below the set threshold.

- SAFI 129 NLRI compliance with RFC 6514 (MX Series)—Starting in Junos OS Release 16.1, the Network Layer Reachability Information (NLRI) format used for BGP VPN multicast has changed. Now Junos OS uses Subsequent Address Family Identifier (SAFI) 129, as defined in RFC 6514, which is length, prefix. Previous releases of Junos OS use SAFI 128 (which is length, label, prefix).

- Latency fairness optimized multicast (MX Series)—Starting with Junos OS Release 16.1R1, you can reduce latency in the multicast packet delivery by optimizing multicast packets sent to the Packet Forwarding Engines. You can achieve this by enabling the ingress or local-latency-fairness option in the multicast-replication configuration statement at the [edit forwarding-options] hierarchy level. The multicast-replication
statement is supported only on platforms with the enhanced-ip mode enabled. This feature is not supported in VPLS networks and Layer 2 bridging.

Network Management and Monitoring

- **Support for RFC 4878 (MX Series and T Series)**—Starting with Release 16.1, Junos OS supports IETF standard RFC 4878, Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on Ethernet-Like Interfaces.

  To enable generation of SNMP traps, `dot3OamThresholdEvent` and `dot3OamNonThresholdEvent`, you must configure the new `dot3oam-events` statement at the `[edit snmp trap-groups <group-name> categories]` hierarchy level.

  **NOTE:**
  - Junos OS does not support the `dot3oamFramesLostDueToOam` object in the `dot3OamStatsEntry` table. In addition, Junos OS does not support the SNMP set operations for the OAM MIBs.
  - On an Aggregated Ethernet bundle if link fault management (LFM) is configured, you must do SNMP operations individually for each interface in the AE bundle because some OAM MIB tables are maintained only for member interfaces in the AE bundle.

- **SNMP support to monitor the total number of subscribers per PIC and per slot**—Starting in Junos OS Release 16.1R1, you can monitor the total number of subscribers per PIC and per slot. The MIB tables `jnxSubscriberPicCountTable` and `jnxSubscriberSlotCountTable` are added to the Juniper Networks enterprise-specific Subscriber MIB to support this feature. In releases earlier than Junos OS Release 16.1, you need to use the `show subscribers summary pic` and `show subscribers summary slot` operational commands, respectively, to display the total number of subscribers per PIC and per slot.

- **SNMP support for the timing feature on MPC5E and MPC6E**—Starting in Junos OS Release 16.1R1, SNMP supports the timing feature on MPC5E and MPC6E. Currently, SNMP support is limited to defect and event notifications through SNMP traps. The enterprise-specific MIB, Timing Feature Defect/Event Notification MIB, allows you to monitor the operation of PTP clocks within the network. The trap notifications are disabled by default. To enable trap notifications for timing events and defects, include the `timing-event` statement at the `[edit snmp trap-group trap-group object categories]` hierarchy level.

- **Support for Entity State MIBs (T Series)**—Starting with Junos OS Release 16.1, support for IETF standard RFC 4268, Entity State MIB, is extended to the T Series. Junos OS provides only read-only support to Entity State MIB.

- **IPv6 support for traceroute with AS number lookup (MX Series and T Series)**—Starting with Junos OS Release 16.1R1, IPv6 is supported for traceroute with the `as-number-lookup` option. Traceroute is an application used to display a list of routers between the device and a specified destination host. Traceroute also provides an option to look up the autonomous system (AS) number of each intermediate hop on the path from the host to the destination.
• Support for the interface-set SNMP index (MX Series)—Starting with Release 16.1, Junos OS supports the interface-set SNMP index that provides information about interface-set queue statistics. The following interface-set SNMP index MIBs are introduced in the Juniper Networks enterprise-specific Class-of-Service MIB:
  • jnxCosIfTable in jnxCos MIB
  • jnxCosIfsetQstatTable in jnxCos MIB

• SNMP support for fabric queue depth, WAN queue depth, and fabric counter (MX240, MX480, MX960, MX2010, and MX2020)—Starting with Release 16.1, Junos OS provides SNMP support for WAN queue depth, fabric queue depth, and fabric counter. The following SNMP MIB tables include the associated objects:
  • jnxCosQstatTable table
  • jnxCosIngressQstatTable table
  • jnxFabricMib table

In addition, this feature supports the following traps for the Packet Forwarding Engine resource monitoring MIBs:
  • jnxPfeMemoryTrapVars
  • jnxPfeMemoryNotifications

• New SNMP MIB object for RADIUS accounting subscribers (MX Series)—Starting with Release 16.1, Junos OS supports a new SNMP MIB object, jnxSubscriberAccountingTotalCount, in JUNIPER-SUBSCRIBER-MIB whose object identifier is {jnxSubscriberGeneral 7}. The jnxSubscriberAccountingTotalCount object provides information about the total number of subscribers that have RADIUS accounting enabled.

• Support for Agent Capabilities MIB (MX Series)—Starting with Release 16.1, Junos OS introduces the Agent Capabilities MIB, which provides information about the implementation characteristics of an Agent subsystem in a network management system. The MIB provides you details of the MIB objects and tables that are supported by an Agent, the conformance and variance information associated with the managed objects in the Agent, and the access level of each object. Currently, the Agent Capability MIB is applicable only for the MPLS and multicast MIBs.

• New indicators for the jnxLEDState MIB (MX5, MX10, MX40, MX80, MX104, and MX240 routers)—Starting with Release 16.1, Junos OS introduces the following six new indicators for the jnxLEDState MIB object in the jnxLEDEntry MIB table:
  • off—Offline, not running
  • blinkingGreen—Entering state of ok, good, normally working
  • blinkingYellow—Entering state of alarm, warning, marginally working
  • blinkingRed—Entering state of alert, failed, not working
• **blinkingBlue**—Entering state of ok, online as an active primary

• **blinkingAmber**—Entering state of offline, not running


### Operation Administration and Management

• **Configuration support for multiple up MEPs for interfaces belonging to a single VPLS service or a bridge domain (MX Series with MPC)**—Starting with Junos OS Release 16.1R1, you can configure multiple up maintenance association endpoints (MEP) for a single combination of maintenance association ID and maintenance domain ID for interfaces belonging to a particular VPLS service or a bridge domain.

To configure multiple up MEPS, specify `mep mep-id` statement at the `[edit protocols oam ethernet connectivity-fault-management maintenance-domain domain-name maintenance association ma-name]` hierarchy level, when the MEP direction is configured as direction up.

• **Ethernet loss measurement counter support for each class in a multiclass environment**—Junos OS supports Ethernet loss measurement (ETH-LM) for multiclass services. The ETH-LM feature is used by operators to collect frame loss counter values for ingress and egress service frames. Starting with Junos OS Release 16.1R1, the ETH-LM feature is extended to support the frame loss measurement counters for each class of packets in a multiclass environment. Counters for each class of packets are supported for point-to-point services only.

| NOTE: ETH-LM is currently supported for VPWS services only. |

ETH-LM maintains counters based on the forwarding class and loss priority of a packet. The loss priority determines the color of a packet—for example, green indicates low loss priority, yellow indicates medium-high for excess information rate (EIR). The color (green and yellow) counters are maintained for each class of packets. Based on the counters supported on an interface, you can configure accounting modes with color or without color for Ethernet loss measurement:
• Forwarding class-based accounting with color—In this mode, traffic is serviced based on packet loss priority and forwarding class. Two counters—green and yellow—are maintained for each forwarding class on each service interface. In this mode, an OAM (operation, accounting, and maintenance) packet collects counters based on the forwarding class.

To configure this mode of loss measurement accounting, use the enable-multiclass-loss-measurement statement at the [set protocols oam ethernet connectivity-fault-management performance-monitoring] hierarchy level for global configuration or at the [set protocols oam ethernet connectivity-fault-management performance-monitoring interface interface-name] hierarchy level for interface-level configuration.

• Forwarding class-based accounting without color—In this mode, traffic is serviced based on the forwarding class only. Only one counter is maintained for each forwarding class in each service interface.

To configure this mode of loss measurement accounting, use the enable-multiclass-loss-measurement and colorless-loss-measurement statements at the [set protocols oam ethernet connectivity-fault-management performance-monitoring] hierarchy level for global configuration or at the [set protocols oam ethernet connectivity-fault-management performance-monitoring interface interface-name] hierarchy level for interface-level configuration.

• Color-based accounting—In this mode, traffic is serviced based on the loss priority. Two counters—green and yellow—are maintained for each service interface. Color-based accounting is the default loss measurement mode and requires no configuration.

• Code point-based accounting (without color)—In this mode, traffic is serviced based on the 802.1p priority bits. One counter is maintained for each code point (priority bit) on each service interface. If there are user virtual LAN or 802.1p rewrite rules configured, loss measurement accounting is done before applying the rewrite rules.

To configure this mode, use the code-point-based-lm-accounting statement at the [set protocols oam ethernet connectivity-fault-management performance-monitoring] hierarchy level for global configuration or at the [set protocols oam ethernet connectivity-fault-management performance-monitoring interface interface-name] hierarchy level for interface-level configuration.

NOTE: Code point-based accounting mode does not work if virtual LAN pop or push is configured on the interface. If pop or push is configured, the 802.1p bits are removed from the data packets. Therefore in such cases, you can use forwarding class-based accounting if a one-to-one mapping exists between a forwarding class and the 802.1p bits value; else you can use the priority-based accounting mode.

• Priority-based accounting—In this mode, four counters are maintained for each forwarding class for each interface, with each counter corresponding to either green or yellow colors. To configure this mode, use the priority-based-lm-accounting statement at the [set protocols oam ethernet connectivity-fault-management performance-monitoring interface interface-name] hierarchy level for interface-level configuration.
**performance-monitoring** hierarchy level for global configuration or at the **[set protocols oam ethernet connectivity-fault-management performance-monitoring interface interface-name]** hierarchy level for interface-level configuration.

- **Support extended for IEEE 802.1ag Ethernet OAM (MX Series routers with MPC2E, MPC3E, MPC5E, and MPC6)**—Support for the IEEE 802.1ag standard for Operation, Administration, and Maintenance (OAM) is now available on MX Series routers with MPC2E, MPC3E, MPC5E, and MPC6. The IEEE 802.1ag specification provides for Ethernet connectivity fault management (CFM), which monitors Ethernet networks that might comprise one or more service instances for network-compromising connectivity faults.

- **Support for MEF-36-compliant performance monitoring (MX Series)**—Starting in Release 16.1R1, Junos OS supports performance monitoring that is compliant with Technical Specification MEF 36. You can enable MEF-36-compliant performance monitoring by configuring the `measurement-interval` statement at the **[edit protocols oam ethernet cfm performance-monitoring]** hierarchy level.

  **NOTE:** When MEF-36-compliant performance monitoring is enabled, an SNMP get next request for a variable might not fetch the current value unless an SNMP walk is performed before performing the get next request. This limitation applies only to the current statistics for delay measurement, loss measurement, and synthetic loss measurement.

When MEF-36-compliant performance monitoring is enabled:

- The output for the field **Current delay measurement statistics** might display a measurement interval of 0 (zero) and an incorrect timestamp until the first cycle time has expired.

- Supported data TLV size for performance monitoring protocol data units (PDUs) is 1386 bytes when MEF-36-compliant performance monitoring is enabled. The TLV size is 1400 bytes in legacy mode.

- The maximum configurable value for the lower threshold bin is 4,294,967,294.

- Frame loss ratio (FLR) is excluded in loss measurements during period of unavailability for synthetic loss measurement only. In case of loss measurement, FLR is included even during period of unavailability.

- During a period of loss of continuity (adjacency down), although SOAM PDUs are not sent, FLR and availability calculations are not stopped. These calculations are performed with the assumption of 100% loss.

- The number of SOAM PDUs that are sent during the first measurement interval might be less than expected. This is because of a delay in detecting the adjacency state at the performance monitoring session level.

- The number of SOAM PDUs transmitted during a measurement interval for a cycle time of 100 ms might not be accurate. For example, in a measurement interval of two minutes with a cycle time 100 ms, the SOAM PDUs transmitted might be in the range of 1198—2000.
Routing Policy and Firewall Filters

- **New load-balancing options using source or destination IP address only (MX Series)**—Starting in Junos OS Release 16.1, new load-balancing options based solely on the source or destination IP address are available. Using only source IP or destination IP as the basis for generating load-balancing hashes helps service providers to ensure that both incoming and outgoing traffic through provider edge (PE) routers is sent toward the content server that maintains subscriber state for a given subscriber. These options are intended for use in deep packet inspection (DPI) networks with per-subscriber awareness and in environments that employ transparent caching.

- **Policer overhead adjustment at the interface level (MX Series)**—Starting in Junos OS Release 16.1, policer-overhead adjustment for ingress and egress policers is defined on a per IFL/direction granularity in order to address MEF CE 2.0 requirements to the bandwidth profile. The **policer-overhead** adjustment is the range of -16 bytes to +16 bytes. It is applied for all the policers that take into account L1/L2 packet length that are exercised in the specified IFL/direction, including corresponding IFF feature policers, and is applied only to interface/filter-based policers.

  [See Configuring the Accounting of Policier Overhead in Interface Statistics.]

- **New packet-per-second (pps)-based policer for transit and control traffic (MX Series)**—Starting in Junos OS Release 16.1, a new pps-based policer is available at the [edit firewall policer policer-name] hierarchy level. This new policer is configured using the if-exceeding-pps configuration statement. Compared to bandwidth-based policers, the pps-based policer is more effective at combating low-and-slow types of DDoS attacks. The pps-based policer can be applied in the same manner and the same locations as bandwidth-based policers, but it cannot be used as a percentage-based policer.

- **New route-filter-list and source-address-filter-list configuration statements (MX Series)**—Starting in Junos OS Release 16.1, the new route-filter-list and source-address-filter-list statements provide an additional means of configuring route filters and source address filters. Now you can configure route-filter-list or source-address-filter-list at the [edit policy-options] hierarchy level for later use in a policy statement. The lists are used in the same contexts as the route-filter and source-address-filter statements. You can use the lists in multiple policy statements.

  [See Understanding Route Filter and Source Address Filter Lists for Use in Routing Policy Match Conditions.]

- **Priority for Route Prefixes in RPD Infrastructure (MX Series)**—Starting in Junos OS Release 16.1, you can specify a priority of high or low through the existing import policy in protocols. Through priority, you can control the order in which the routes get updated from LDP/OSPF to RPD, and RPD to kernel. In the event of a topology change, high priority prefixes are updated in the routing table first, followed by low priority prefixes. Routes that are not explicitly assigned a priority are treated as medium priority.

  [See Example: Configuring the Priority for Route Prefixes in the rpd Infrastructure.]

- **New multifield ingress queuing classifier filter (MX Series with MPCs)**—Starting in Junos OS Release 16.1, you can apply the ingress-queuing-filter filter-name statement at the [edit interfaces interface-name family family-name] hierarchy level for the following
protocol families: bridge, cc, inet, inet6, mpls, and vpls. The `ingress-queuing-filter` statement allows you to set the forwarding class and loss priority for a packet prior to ingress queue selection by applying a previously configured firewall filter. Multiple fields within the packet header can be matched based on the configured protocol family within the firewall filter.

- **Support for logical queue-depth in the PFE for IP options packets for a given protocol (MX Series)** — Starting with Junos OS Release 16.1R1, you can configure logical queue-depth in the PFE for IP options packets for a given protocol. The queue-depth indicates the number of IP options packets which can be enqueued in the PFE logical queue, beyond which it would start dropping the packets.

**Routing Protocols**

- **BGP flow specification for IPv6 (MX Series)** — Starting with Junos OS Release 16.1, this feature extends IPv6 support to the BGP flow specification and allows propagation of traffic flow specification rules for IPv6 and IPv6 VPN. The BGP flow specification automates coordination of traffic filtering rules in order to mitigate distributed denial-of-service attacks. In earlier Junos OS releases, flow-specific rules were propagated for IPv4 over BGP as network layer reachability information.

  To enable the BGP flow specification for IPv6, include the `flow` statement at the [edit routing-options] hierarchy level for global configuration or at the [edit routing-instances routing-instance-name routing-options] hierarchy level for instance-level configuration.

  [See `flow-ipv6`.]  

- **Support for PTP over Ethernet (MX Series)** — Starting in Junos OS Release 16.1R1, the Precision Time Protocol (PTP) is supported over IEEE 802.3 or Ethernet links on MX Series routers. This functionality is supported in compliance with the IEEE 1588-2008 specification.

  For the base station vendors that support only packet interfaces by using Ethernet encapsulation for PTP packets for time and phase synchronization, you can configure any node (an MX Series router) that is directly connected to the base station to use the Ethernet encapsulation method for PTP on a master port to support a packet-based timing capability.

  To configure Ethernet as the encapsulation type for transport of PTP packets on master or slave interfaces, use the `transport 802.3` statement at the [edit protocols ptp slave interface interface-name multicast-mode] or [edit protocols ptp master interface interface-name multicast-mode] hierarchy level.

- **Maximum period for autogeneration of keepalives by the kernel using precision timer feature (MX Series)** — Starting with Junos OS Release 16.1, precision timers in the kernel autogenerate keepalives on behalf of BGP after a switchover event from standby to master for a specified maximum period of time.

- **IS-IS Layer 2 mapping (MX Series and T Series)** — Beginning with Junos OS Release 16.1, you can enable Layer 2 mapping of next-hop addresses using the IS-IS LAN and point-to-point Hellos that supply all relevant Layer 2 and Layer 3 binding address information for address resolution. The device at the receiving end can extract the information and populate the ARP or Neighbor Discovery table even before the
installation of routes. Layer 2 mapping is a topology driven rather than traffic driven next-hop resolution that minimizes traffic loss while activating an Ethernet link.

[See Layer 2 Mapping for IS-IS.]

- IPv6 support for IS-IS BFD (MX Series and T Series)—Starting with Junos OS Release 16.1, you can configure IS-IS BFD sessions for IPv6. You can enable IS-IS BFD sessions by including the `bfd-liveness-detection` statement at the `[edit protocols isis interface interface-name family inet|inet6]` hierarchy level. Currently, IS-IS BFD configuration is available at the `[edit protocols isis interface interface-name]` hierarchy level. At present, BFD configuration is supported at both of these hierarchy levels.

[See bfd-liveness-detection.]

- IS-IS FRR route convergence (MX Series)—Starting with Junos OS Release 16.1R1, IS-IS fast reroute (FRR) route convergence enables you to restore sub-second service. Sub-second service restoration is a key requirement for service providers on MPLS and native IP-based networks.

There are many ways to achieve fast reroute with suboptimal next hop to reach a destination, such as loop-free alternate (LFA) and remote loop-free alternate (RLFA). In these cases, IGP downloads the primary and backup next hops beforehand in the forwarding information base (FIB). The Packet Forwarding Engine does a local repair when the primary next hop loses its reachability to a given destination. Because the Packet Forwarding Engine already has an alternative path to reach its destination, sub-second restoration is possible. If the destination is reachable through equal-cost multipath (ECMP), only the primary path is downloaded to the FIB. When the bandwidth of the ECMP links is lower than the required bandwidth for a destination, fast convergence is not possible.

The best ECMP links are grouped as a unilist of primary next hops to reach the destination. Suboptimal ECMP links are grouped as a unilist of backup next hops to reach the destination. If the bandwidth of the primary next hops falls below the desired bandwidth, the Packet Forwarding Engine does a local repair and traffic switch to back up the unilist next hops.

[See IS-IS Fast Reroute Route Convergence Overview.]

- Advertising IPv4 routes over BGP IPv6 sessions (MX Series and T Series)—Beginning with Junos OS Release 16.1, you can configure BGP to advertise IPv4 unicast reachability with IPv4 next hop over an IPv6 BGP session. In earlier Junos OS releases, BGP could advertise only inet6 unicast, inet6 multicast, and inet6 labeled unicast address families over BGP IPv6 sessions. This feature allows BGP to exchange all the BGP address families over an IPv6 BGP session.

[See Advertising IPv4 Routes over IPv6 Overview.]

- BGP route prefix prioritization (MX Series and T Series)—Starting in Junos OS Release 16.1, you can prioritize BGP route updates using output queues. The output queues are serviced using a token mechanism that allows you to assign routes to queues using policies. There is an expedited queue and 16 numbered queues that range in priority from lowest priority (1) to highest priority (16). The lowest priority queue (1) is designated as the default queue. Routes that are not explicitly assigned to a queue by automatic protocol determination or by user policy are placed in this queue.
• **ISIS Purge Originator Identification TLV (MX Series)**—Beginning with Junos OS Release 15.1F4, Junos OS supports RFC 6232, *Purge Originator Identification TLV for IS-IS*, which defines a type, length, and value (TLV) for identifying the origin of a purge initiated by the IS-IS protocol. You can configure this feature to add this TLV to a purge along with the system ID of the Intermediate System (IS) that has initiated this purge. This makes it easier to locate the origin of the purge and its cause. A new show command `show isis purge log` is introduced to view the purge history and to identify the purge originator. [See IS-IS Purge Originator Identification Overview.]

• **Weighted ECMP support for one-hop IS-IS neighbors (MX Series)**—Beginning with Junos OS Release 15.1F4, you can configure the IS-IS protocol to get the logical interface bandwidth information associated with the gateways of equal-cost multipath (ECMP) next hop. During per-packet load balancing, traffic distribution is based on the available bandwidth to facilitate optimal bandwidth usage for incoming traffic on an ECMP path of one hop distance. The Packet Forwarding Engine does not distribute the traffic equally, but considers the balance values and distributes the traffic according to the bandwidth availability. However, this feature is not available for ECMP paths that are more than one hop away. [See Weighted ECMP Traffic Distribution on One Hop IS-IS Neighbors Overview.]

• **Statements introduced to delay the DHCP-OFFER and DHCP-ADVERTISE for DHCPv4 and DHCPv6 server bindings**—Starting in Junos OS 16.1R1, you can delay the DHCP-OFFER/DHCP-ADVERTISE sent to the subscribers. This feature is applicable only for DHCPv4 and DHCPv6 server bindings. You can configure the OFFER/ADVERTISE delay per ACI/ARI. You can configure the delay time between 1 and 30 seconds. If you don’t configure any delay time, then the default value of 3 seconds will be used.

To configure the DHCP-OFFER delay for DHCPv4 server bindings, use the `delay-offer delay-time <time in seconds>` statement at the [edit system services dhcp-local-server overrides] hierarchy level. The delay will take effect only if at least one of the options (option-60/option-70/option-82) are configured. To configure options, go to the [edit system services dhcp-local-server overrides based-on] hierarchy level.

To configure the DHCP-ADVERTISE delay for DHCPv6 server bindings, use `delay advertise delay-time <time in seconds>` at the [edit system services dhcp-local-server dhcpv6 overrides] hierarchy level. The delay will take effect only if at least one of the options (option-15/option-16/option-17/option-37) are configured. To configure options, go to the [edit system services dhcp-local-server dhcpv6 overrides based-on] hierarchy level.

• **Support for BGP Optimal Route Reflection (BGP-ORR) (MX Series)**—Starting with Junos OS Release 16.1R1, you can configure BGP-ORR with IS-IS as the interior gateway protocol (IGP) on a route reflector to advertise the best path to the BGP-ORR client groups by using the shortest IGP metric from a client’s perspective, instead of the route reflector’s view.

To enable BGP-ORR, include the `optimal-route-reflection` statement at the [edit protocols bgp group group-name] hierarchy level.

Client groups sharing the same or similar IGP topology can be grouped as one BGP peer group. You can configure `optimal-route-reflection` to enable BGP-ORR in that BGP
peer group. You can also configure one of the client nodes as the primary node (igp-primary) in a BGP peer group so that the IGP metric from that primary node is used to select the best path and advertise it to the clients in the same BGP peer group. Optionally, you can also select another client node as the backup node (igp-backup), which is used when the primary node (igp-primary) goes down or is unreachable.

- **Flow-aware transport pseudowire for BGP L2VPN and BGP VPLS (MX Series)—** Starting with Junos OS Release 16.1, the flow-aware transport (FAT) label that is supported for BGP-signaled pseudowires such as L2VPN and VPLS is configured only on the label edge routers (LERs). This causes the transit routers or label-switching routers (LSRs) to perform load balancing of MPLS packets across equal-cost multipath (ECMP) paths or link aggregation groups (LAGs) without the need for deep packet inspection of the payload. The FAT flow label can be used for LDP-signaled forwarding equivalence class (FEC128 and FEC129) pseudowires for VPWS and VPLS pseudowires.

- **Control word feature for LDP VPLS and FEC129 VPLS (MX Series)—** Starting with Junos OS Release 16.1, the control word feature is supported for LDP VPLS and FEC129 VPLS.

- **Flow-aware transport pseudowire for BGP L2VPN and BGP VPLS (MX Series)—** Starting with Junos OS Release 16.1R1, the flow-aware transport (FAT) label is supported for BGP-signaled pseudowires such as L2VPN and VPLS. Configuring flow-label-receive and flow-label-transmit on the label edge routers (LERs) enables the transit routers or label-switching routers (LSRs) to perform load balancing of MPLS packets across equal-cost multipath (ECMP) paths or link aggregation groups (LAGs) without the need for deep packet inspection of the payload.

**Security**

- **Support for IPv6 NDP DoS issue (MX Series)—** Starting with Junos OS Release 16.1R1, you can address the IPv6 Neighbor Discovery Protocol (NDP) denial-of-service (DoS) issue at the Routing Engine.

  Unlike IPv4 subnets, IPv6 subnets have large address spaces in which a majority of them remain unassigned. When a network scan tool or an attacker initiates traffic to nonexistent hosts through a router on a subnet that is directly connected to the router, the router attempts to perform address resolution on a large number of destinations. This condition can cause the inability to resolve new neighbors, unreachability to the existing neighbors, and can also result in a DoS attack.

  NDP inspection or protection addresses the NDP DoS issue by implementing the prioritization of NDP activities on the Routing Engine. At the ingress router, neighbor discovery (ND) packets are classified and handled according to a predefined priority with multiple ingress queues. On the egress path, neighbor solicitations (NS) sent for previously not seen hosts are handled with a lower priority by deferring the process of next-hop creation and sending out the packet.

  [See Supported IPv6 Standards.]

- **Support for mitigating potential DDoS issues with IPv6 NDP and resolve traffic (MX Series)—** Starting with Junos OS Release 16.1R1, you can resolve potential distributed denial-of-service (DDoS) issues with the IPv6 Neighbor Discovery Protocol (NDP) and traffic.
The fundamental challenge of IPv6 NDP DDoS is the large address space of IPv6 that allows attackers to trigger a huge number of resolves that exhaust the router resources. The resolution mechanism and DDoS NDP policer help mitigate the problem to some extent.

The functionality primarily extends the flow-detection CLI and optimizes the hostbound classification (HBC) filter to make packet-type searching faster. It also extends the NDP DDoS protocol group to classify the NDP types. Full Ethernet or IPv6 fields support is added by allowing destination addresses.

[See Understanding Distributed Denial-of-Service Protection with IPv6 Neighbor Discovery Protocol.]

**Services Applications**

- **Data plane inline support for 6rd and 6to4 tunnels connecting IPv6 clients to IPv4 networks (MX Series with MPC5E and MPC6E)—Starting with Release 16.1R1, Junos OS supports inline 6rd and 6to4 on MPC5E and MPC6E line cards. In releases earlier than Junos OS Release 16.1R1, inline 6rd and 6to4 was supported on MPC3E line cards only.**

- **Support for inline MPLS Junos Traffic Vision with IPFIX and v9 (MX Series)—Starting in Junos OS Release 15.1F2 and 16.1R1, support of the MX Series routers for the inline Junos Traffic Vision feature is extended to the MPLS family (MPLS and MPLS-IPv4 templates) consisting of the IP Flow Information Export (IPFIX) protocol and flow monitoring version 9 (v9). In previous releases, the inline Junos Traffic Vision feature is supported only for IPv4, IPv6, and VPLS families. In this release, Inline Junos Traffic Vision feature is extended to MPC5E and MPC6E for the VPLS address family.**

- **Support for inline video monitoring on MPC5 and MPC6 (MX Series routers)—Starting in Junos OS Release 16.1, support for video monitoring using media delivery indexing (MDI) criteria is expanded to include the MPC5 and MPC6.**

[See Inline Video Monitoring Overview.]

- **Support for RFC 2544-based benchmarking tests (MX Series)—Junos OS Release 16.1 extends support for the reflector function and the corresponding RFC 2544-based benchmarking tests on MX Series routers with MPC1 (MX-MPC1-3D), MPC2 (MX-MPC2-3D), and the 16-port 10-Gigabit Ethernet MPC (MPC-3D-16XGE-SFP). The RFC 2544 tests are performed to measure and demonstrate the service-level agreement (SLA) parameters before activation of the service. The tests measure throughput, latency, frame loss rate, and back-to-back frames. RFC 2544-based benchmarking tests on MX Series routers support the following reflection functions:**

  - Ethernet pseudowire reflection (ingress and egress direction) (ELINE service—supported for family ccc)
  - Layer 2 reflection (egress direction) (ELAN service—supported for family bridge, vpls)
  - Layer 3 IPv4 reflection (limited support)
To run the benchmarking tests on the MX Series routers, you must configure reflection (Layer 2 or pseudowire) on the supported MPC. To configure the reflector function on the MPC, use the `chassis fpc fpc-slot-no slamon-services rfc2544` statement at the [edit] hierarchy level.

- **Support for RPM probes with IPv6 sources and destinations (MX Series routers with MPCs)**—Starting in Junos OS Release 16.1, the RPM client router (the router or switch that originates the RPM probes) can send probe packets to the RPM probe server (the device that receives the RPM probes) that contains an IPv6 address. To specify the destination IPv6 address used for the probes, include the `target (url ipv6-url | address ipv6-address)` statement at the [edit services rpm probe owner test test-name] hierarchy level. You can also define the RPM client or the source that sends RPM probes to contain an IPv6 address. To specify the IPv6 protocol-related settings and the source IPv6 address of the client from which the RPM probes are sent, include the `inet6-options source-address ipv6-address` statement at the [edit services rpm probe owner test test-name] hierarchy level.

- **Provide egress VLAN ID and flow direction information in sampling records (MX Series)**—Starting in Junos OS Release 16.1R1, Junos OS can include flow direction and egress VLAN ID information in the output records when you perform inline sampling on IPv4 or IPv6 traffic by using the IPFIX or version 9 templates. You can optionally include VLAN IDs in both the ingress and egress directions in the flow key.

  [See Configuring Flow Aggregation to Use Version 9 Flow Templates and Configuring Flow Aggregation to Use IPFIX Flow Templates.]

- **Support for inline MPLS Junos Traffic Vision with IPFIX and v9 (MX Series)**—Starting in Junos OS Release 16.1, support for the inline Junos Traffic Vision feature on MX Series routers is extended to the MPLS family (MPLS and MPLS-IPv4 templates), consisting of the IP Flow Information Export (IPFIX) protocol and flow monitoring version 9 (v9). In previous releases, the inline Junos Traffic Vision feature is supported only for IPv4, IPv6, and VPLS families.

  The inline Junos Traffic Vision feature is extended to the MPC5E and MPC6E for VPLS address family. Also, Inline Junos Traffic Vision support using version 9 templates is extended to the VPLS family.

  **NOTE:** This feature is documented but not supported in Junos OS Release 16.1R1.

- **IPsec multipath forwarding with UDP encapsulation (MX Series routers with MS-MPCs and MS-MICs)**—Starting in Junos OS Release 16.1, you can enable the UDP encapsulation of the IPsec encapsulated packets between peers, which appends a UDP header after the ESP header. Doing this provides Layer 3 and 4 information to the intermediate routers, and the IPsec packets are forwarded over multiple paths, which increases the throughput.

  [See IPsec Multipath Forwarding With UDP Encapsulation.]
**Subscriber-aware and application-aware traffic treatment (MX Series with MS-MPC)**—Although present in the code, the subscriber-aware and application-aware traffic treatment features are not supported in Junos OS Release 16.1R1. Subscriber-aware and application-aware traffic treatment identifies the mobile or fixed-line subscriber and enforces traffic treatment based on policies assigned to the subscriber. A subscriber policy can be based on Layer 7 application information for the IP flow (for example, YouTube) or can be based on Layer 3/Layer 4 information for the IP flow (for example, the source and destination IP address). Subscriber policy actions can include:

- Redirecting HTTP traffic to another URL or IP address
- Forwarding packets to a routing instance so that packets are directed to external service chains (predefined sequence of services)
- Setting the forwarding class
- Setting the maximum bit rate
- Performing HTTP header enrichment
- Setting the gating status to blocked or allowed

**Service redundancy daemon support for redundancy across multiple gateways (MX Series with MPC)**—Although present in the code, the service redundancy daemon support for redundancy across multiple service gateways is not supported in Junos OS Release 16.1R1. The redundancy actions are based on the results of monitoring system events.

**Traffic load balancer (MX Series with MS-MPC or MPC)**—Although present in the code, the traffic load balancer (TLB) features are not supported in Junos OS Release 16.1R1. TLB runs on MX Series routers with Multiservices Modular Port Concentrator (MS-MPC) services PICs and Modular Port Concentrator (MPC) line cards. TLB enables you to distribute traffic among multiple next-hop servers. TLB employs an MS-MPC-based control plane and a data plane using the MX Series router forwarding engine.
NOTE: This feature is documented but not supported in Junos OS Release 16.1R1.

Enhancements to stateful synchronization (MS-MIC, MS-MPC)—Although present in the code, enhancements to stateful synchronization for long-running flows is not supported in Junos OS Release 16.1R1. These enhancements include:

- Automatic replication of NAT flows for all service sets: NAT44 flows are automatically synchronized for all eligible service sets. You can selectively disable replication for individual service sets by including the `disposable-replication-capability` statement at the `[edit services service-set service-set-name replicate-services]` hierarchy level.

- Checkpointing of IPv4 and IPv6 stateful firewall flows and NAPT-44 with address pooling paired (APP): To manage the frequency of checkpointing, include the `replication-threshold seconds` statement at the `[edit interfaces interface-name redundancy-options]` hierarchy level.

- Exclude interfaces support in flowspec (rpd-infra) (MX Series)—Starting in Release 15.1, Junos OS excludes applying the `flowspec` filter to traffic received on specific interfaces. A new term is added at the beginning of the `flowspec` filter that accepts any packet received on these specific interfaces. The new term is a variable that creates an exclusion list of terms attached to the forwarding table filter as a part of the flow specification filter.

To exclude the `flowspec` filter from being applied to traffic received on specific interfaces, you must first configure a `group-id` on such interfaces by including the family `inet` filter group `group-id` statement at the `[edit interfaces]` hierarchy level and then attach the `flowspec` filter with the interface group by including the `flow interface-group group-id exclude` statement at the `[edit routing-options]` hierarchy level. You can configure only one `group-id` per routing instance with the `set routing-options flow interface-group group-id` statement.

[See Understanding BGP Flow Routes for Traffic Filtering.]

Software Installation and Upgrade

- Validate system software against running configuration on remote host—Beginning with Junos OS Release 16.1R1, you can use the `on (host host <username username> | routing-engine routing-engine)` option with the `request system software validate package-name` command to verify candidate system software against the running configuration on the specified remote host or Routing Engine.

- Validate system software add against running configuration on remote host or routing engine—Beginning with Junos OS Release 16.1R1, you can use the `validate-on-host hostname` and `validate-on-routing-engine routing-engine` options with the `request system software add package-name` command to verify a candidate software bundle against the running configuration on the specified remote host or Routing Engine.

[See request system software add.]
• ISSU support for upgrading from FreeBSD 6.1-based Junos OS to FreeBSD 10.x-based Junos OS (MX Series)—Starting with Junos OS Release 16.1R1, you can upgrade from a FreeBSD 6.1-based Junos OS MX Series router to a FreeBSD 10.x-based Junos OS MX Series router by performing an upgrade Junos OS with upgraded FreeBSD in-service software upgrade (ISSU). A unified (ISSU) enables you to upgrade between two different Junos OS releases with minimal disruption on the control plane and with minimal disruption of traffic.

Before performing a unified ISSU from a FreeBSD 6.1-based Junos OS to an upgraded FreeBSD 10.x-based Junos OS, the configuration must be validated on a remote host or on a routing engine. The remote host or the routing engine must be running a Junos OS with an upgraded FreeBSD.

[See Example: Performing a Unified ISSU.]

[See Upgrading Junos OS with Upgraded FreeBSD.]

• New way to provision new routers automatically (MX Series)—As of Junos OS Release 16.1, zero touch provisioning (ZTP) allows you to provision new routers in your network automatically either by executing a script file or by loading a configuration file. In either case, the information is detected in a file on the Dynamic Host Control Protocol (DHCP) server. In releases earlier than Junos OS Release 16.1, automatically provisioning a new device was available only for switches.

[See Configuring Zero Touch Provisioning.]

• Limited encryption Junos image (“Junos Limited”) created for customers in Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia (MX80, MX104, MX240, MX480, MX960, MX2010, MX2020)—Starting in Junos OS Release 16.1R1, customers in the Eurasian Customs Union (currently comprised of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) should use the “Junos Limited” image for MX240, MX480, MX960, MX2010, and MX2020 routers instead of the “Junos Worldwide” image. The “Junos Limited” image does not have data-plane encryption and is intended only for countries in the Eurasian Customs Union because these countries have import restrictions on software containing data plane encryption. Unlike the “Junos Worldwide” image, the “Junos Limited” image supports control plane encryption through Secure Shell (SSH) and Secure Sockets Layer (SSL), thus allowing secure management of the system.

NOTE: The limited encryption Junos image (“Junos Limited”) is to be used by customers in Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia. Customers in all other countries should use “Junos” image which was introduced in 15.1R1 to replace “Junos Domestic” image.

• Limited encryption Junos image (“Junos Limited”) created for customers in Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia (MX80 and MX104)—Starting in Junos OS Release 16.1R1, customers in the Eurasian Customs Union (currently comprised of Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia) should use the “Junos Limited” image for MX80 and MX104 routers instead of the “Junos Worldwide” image. The “Junos Limited” image does not have data-plane encryption and is intended only for countries in the Eurasian Customs Union because these countries have import restrictions on software containing data plane encryption.
restrictions on software containing data plane encryption. Unlike the "Junos Worldwide" image, the "Junos Limited" image supports control plane encryption through Secure Shell (SSH) and Secure Sockets Layer (SSL), thus allowing secure management of the system.

NOTE: The limited encryption Junos image ("Junos Limited") is to be used by customers in Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Russia.

Software Defined Networking

- **Support of Internet draft draft-ietf-pce-stateful-pce-07 for the stateful PCC implementation (MX Series and T Series)**—The partial client-side implementation of the stateful Path Computation Element (PCE) architecture is currently based on version 2 of Internet draft draft-ietf-pce-stateful-pce. Starting with Junos OS Release 16.1, this implementation is upgraded to support version 7, as defined in Internet draft draft-ietf-pce-stateful-pce-07.

  Releases prior to 16.1 support the older version of the PCE draft, causing interoperability issues between a Path Computation Client (PCC) running a previous release and a stateful PCE server that adheres to Internet draft draft-ietf-pce-stateful-pce-07.

  [See Example: Configuring Path Computation Element Protocol for MPLS RSVP-TE.]

- **Support for PCEP-based reporting of point-to-multipoint LSPs (MX Series and T Series)**—A stateful Path Computation Element (PCE) provides external path computation of traffic engineered (TE) label-switched paths (LSPs) for a Path Computation Client (PCC) in an MPLS network. After a PCEP session is established between a PCE and a PCC, the PCC reports all the LSPs in the system to the PCE for LSP state synchronization. Currently, this includes PCC-controlled, PCE-delegated, and PCE-initiated point-to-point RSVP-TE LSPs. Starting with Junos OS Release 15.1F6 and 16.1R1, this capability of a PCC is extended to report point-to-multipoint RSVP-TE LSPs as well.

  By default, a PCC does not support reporting of point-to-multipoint LSPs to a PCE. To add this capability, include the p2mp-lsp-report-capability statement at the [edit protocols pcep pce pce-name] or [edit protocols pcep pce-group group-id] hierarchy levels.

  A PCC configured with the capability of reporting point-to-multipoint LSPs to a PCE enables the PCE to have greater visibility of individual per-LSP, per-device bandwidth demands in the MPLS network.

  [See Support of Path Computation Element Protocol for RSVP-TE Overview and Example: Configuring Path Computation Element Protocol with Support for PCE Controlled Point-to-Multipoint RSVP-TE LSPs.]

- **Support for securing PCEP sessions using MD5 authentication (MX Series and T Series)**—Starting with Junos OS Release 16.1, you can secure a Path Computation Element Protocol (PCEP) session using TCP-MD5 authentication as per RFC 5440. To enable the MD5 security mechanism for a PCEP session, it is recommended that you define and bind the MD5 authentication key at the [edit protocols pcep pce pce-id]
hierarchy level for a PCEP session. You can, however, also use a predefined keychain from the [edit security authentication-key-chains key-chain] hierarchy level to secure a PCEP session. In this case, you should bind the predefined keychain into the PCEP session at the [edit protocols pcep pce pce-id] hierarchy level.

The following configuration is executed on the Path Computation Client (PCC) to establish a secure PCEP session with a Path Computation Element (PCE):

- Using MD5 authentication key:
  [edit protocols pcep pce pce-id]
  user@PCC# set authentication-key key

- Using predefined authentication keychain:
  [edit protocols pcep pce pce-id]
  user@PCC# set authentication-key-chain key-chain
  user@PCC# set authentication-algorithm md5

For secure PCEP sessions to be established successfully, the MD5 authentication should be configured with the pre-shared authentication key on both the PCE and the PCC. The PCE and PCC use the same key to verify the authenticity of each segment sent on the TCP connection of the PCEP session.

This feature protects the communication between a PCE and PCC over a PCEP session, which might be subject to an attack, and can disrupt network services.

You can view the authentication keychain used by a PCEP session by executing the show path-computation-client status and show protocols pcep commands.

[See Support of Path Computation Element Protocol for RSVP-TE Overview.]

**Subscriber Management and Services**

**NOTE:** Although present in the code, the subscriber management features are not supported in Junos OS Release 16.1R1. Documentation for subscriber management features is included in the Junos OS Release 16.1 documentation set.
• **Wildcard domain map (MX Series)**—Starting in Junos OS Release 16.1R1, you can configure a wildcard domain map that is used by subscribers when there is no exact match to the subscriber’s domain name, but there is a partial match. For example, if you create a wildcard domain map with the name `xyz*.com`, subscribers with the domain names `xyz-eastern.com` and `xyz-northern.com` are both mapped to that wildcard domain when there was no exact match for the subscriber’s domain name.

To configure a wildcard domain map, you include the asterisk wildcard character in the `map domain-map-name` statement at the `[edit access domain]` hierarchy level.

Wildcard domain mapping is also useful to provide a partial match when subscriber management derives subscriber usernames from the DHCPv4 Agent Remote ID (option 82 suboption 2) or the DHCPv6 Remote-ID (option 37). For example, a username might be `EricSmith#premiumTier1#314159265#0000` (where the `#` character is the delimiter). For domain mapping for this subscriber, you might create the wildcard domain map, `domain map premiumTier1*`. [See Configuring a Wildcard Domain Map.]

• **DHCP-initiated service change based on client Remote ID (MX Series)**—Starting in Junos OS Release 16.1R1, DHCP local server enables you to update a client’s current service based on the client’s remote ID. DHCP-initiated service updates are particularly useful in dual-stack environments and other networks that do not include RADIUS support.

When a DHCP client is initially established, DHCP preserves the client’s incoming remote ID in the DHCP client database. You can configure DHCP local server to compare the client’s initial remote ID to the remote ID that the server subsequently receives in DHCP Renew or Rebind messages. If DHCP local server detects a mismatch between the two remote IDs, the server tears down the existing binding, which initiates a client reconnect sequence. The service change is encoded within the new remote ID string, and is activated when the client reconnects.

DHCP local server receives the remote ID in option 82, suboption 2 for DHCPv4 clients, and in DHCPv6 option 37 for DHCPv6 clients.

To configure DHCP local server to support the remote ID service change feature, use the `remote-id-mismatch disconnect` statement at the `[edit system services dhcp-local-server]` hierarchy level. You can configure support globally or for a specific group. [See DHCP-Initiated Service Change Based on Remote ID.]

• **New support for Framed-IP-Netmask for access-internal routes (MX Series)**—Starting in Junos OS Release 16.1, the mask value returned by RADIUS in the Framed-IP-Netmask attribute during PPP negotiation is considered for application to the access-internal route for the subscriber session. In earlier releases, the attribute mask is ignored and a /32 netmask is always applied, with the consequence that the address is set to the value of the Framed-IP-Address attribute returned by RADIUS.

Now, when the SDB_FRAMED_PROTOCOL attribute is equal to AUTHD_FRAMED_PROTOCOL_PPP, the value of SDB_USER_IP_MASK is set to 255.255.255.255 by default. This value is overridden by the Framed-IP-Netmask value, if present.
When the SDB_FRAMED_PROTOCOL attribute is equal to AUTHD_FRAMED_PROTOCOL_PPP, the `show subscribers` command now displays the actual value of Framed-IP-Netmask in the IP Netmask field. Otherwise, the field displays the default value of 255.255.255.255.

- **Disabling DHCP snooping filters for DHCP traffic that can be directly forwarded (MX Series)**—Starting in Junos OS Release 16.1, you can disable DHCP snooping filters for an address family in the routing context in which snooping is configured.

  When you first enable DHCP snooping, all DHCP traffic is snooped by default and only DHCP packets associated with subscribers (or their creation) will be handled; all other DHCP packets will be discarded. You can optionally modify this dropping behavior based on the type of interface: configured interfaces, non-configured interfaces, or all interfaces. All snooped DHCP traffic is still forwarded to the routing plane in the routing instance, and in some cases, this results in excessive DHCP traffic being sent to the routing plane for snooping. The `no-snoop` statement disables snooping filters for DHCP traffic that can be forwarded directly from the hardware control plane, such as Layer 3 unicast traffic with a valid route, preventing that DHCP traffic from being forwarded to the slower routing plane of the routing instance.

  [See DHCP Snooping Support.]

- **Changes to AAA accounting statistics counters (MX Series)**—Starting in Junos OS Release 16.1, 17 new statistics counters have been added to the output of the `show network-access aaa statistics accounting detail` command to report accounting information that is backed up when RADIUS accounting servers are unreachable and RADIUS backup accounting options are configured.

  In earlier releases, the general statistics counters display aggregate values for original accounting events plus backup events. Now the Accounting response success, Accounting retransmissions, and Requests received counters no longer include requests that are sent to the backup accounting mechanism.

  Two non-backup statistics counters have also been added, Accounting request failures and Accounting request success.

  The Timed out requests counter has been renamed to Accounting request timeouts.

  [See show network-access aaa statistics.]

- **New option for service type added to test aaa commands (MX Series)**—Starting in Junos OS Release 16.1, you can include the service-type option with the `test aaa ppp user` and `test aaa dhcp user` commands to test the AAA configuration of a subscriber.

  You can use this option to distinguish a test session from an actual subscriber session. The option specifies a value for the Service-Type RADIUS attribute [6] in the test Access-Request message; when you do not include this option, the test uses a service type of Framed. You can specify a number in the range 1 through 255, or you can specify a string that corresponds to an RFC-defined service type. When the Service-Type RADIUS attribute [6] is received in an Access-Accept message, it overrides the value inserted in the Access-Request message by this command.

  [See test aaa dhcp user and test aaa ppp user.]
• **New predefined variable for dynamic underlying interfaces (MX Series)**—Starting in Junos OS Release 16.1, you can use the Juniper Networks predefined variable, $junos-underlying-ifd-name, to reference the underlying physical interface when you configure CoS properties for an underlying logical interface in a dynamic profile. The new variable is useful when the $junos-interface-ifd-name variable already references a different physical interface, such as in configurations with stacked logical interfaces. For example, in a PPPoE session where the PPP logical interface is stacked over a demux VLAN logical interface, $junos-interface-ifd-name is set to the pp0 physical interface. In this case you can specify the $junos-underlying-ifd-name predefined variable with the interfaces statement at the [edit dynamic-profiles profile-name class-of-service] hierarchy level to reference the underlying physical interface.

• **Support for service session termination causes (MX Series)**—Starting in Junos OS Release 16.1, new internal identifiers are available that identify the reasons that authd initiates termination of individual service sessions. In earlier releases, the termination cause for a service session is the same as that for the parent subscriber session.

The service termination causes map to default code values that are reported in the RADIUS Acct-Terminate-Cause attribute (49) in Acct-Stop messages for the service. You can use the new service-shutdown option with the terminate-code aaa statement at the [edit access] hierarchy level to remap any of the new termination causes to any number in the range 1 through 4,294,967,295:

- **network-logoff**—Termination was initiated by deactivation of one family for a dual-stack subscriber, typically triggered by termination of the corresponding Layer 3 access protocol. Default code value is 6.
- **remote-reset**—Termination was initiated by an external authority, such as a RADIUS CoA service-deactivation. Default code value is 10.
- **subscriber-logoff**—Overrides the default inheritance of the subscriber session value with a different value when you map it to a different value. Default code value is 1, meaning that it inherits the terminate cause from the parent subscriber session.
- **time-limit**—Service time limit was reached. Default code value is 5.
- **volume-limit**—Service traffic volume limit was reached. Default code value is 10.

The show network-access aaa terminate-code aaa detail command displays the new termination causes and their current code values.

[See Understanding Session Termination Causes and RADIUS Termination Cause Codes.]

• **Support for a static unnumbered interface with $junos-routing-instance (MX Series)**—Starting in Junos OS Release 16.1, you can configure a static logical interface as the unnumbered interface in a dynamic profile that includes dynamic routing instance assignment by means of the $junos-routing-instance predefined variable.

NOTE: This configuration fails commit if you also configure a preferred source address, either statically with the preferred-source-address statement or dynamically with the $junos-preferred-source-address predefined variable for IPv4 (family inet) addresses or the $junos-preferred-source-ipv6-address predefined variable for IPv6 (family inet6) addresses.
NOTE: The static interface must belong to the routing instance; otherwise the profile instantiation fails.

In earlier releases, when the dynamic profile includes the $junos-routing-instance predefined variable, you must do both of the following, else the commit fails:

- Use the $junos-loopback-interface-address predefined variable to dynamically assign an address to the unnumbered interface. You cannot configure a static interface address.

- Use the $junos-preferred-source-address or $junos-preferred-source-ipv6-address predefined variable to dynamically assign a secondary IP address to the unnumbered interface. You cannot configure a static preferred source address.

[See Configuring an Unnumbered Interface.]

- Logical interface option for show ptp port command (MX Series)—Starting in Junos OS Release 16.1, you can display PTP port information for a specific logical interface by using the ifl logical-interface-name option with the show ptp port command:

```
user@host> show ptp port ifl ge-1/0/5.0
PTP port-data:
Local Interface   : ge-1/0/5.0
Local Address     : 2001:db8:00:05:85:73:b0:aa
Remote Address    : 2001:db8:01:80:c2:00:00:0e
Clock Stream      : 0              Clock Identity    :
2001:db8:85:ff:fe:73:b7:d0
Port State        : Master         Delay Req Interval: -4
Announce Interval : 1              Announce Timeout  : 3
Sync Interval     : -6             Delay Mechanism   : End-to-end
Port Number       : 1              Operating Mode    : Master only
```

- Enhancements to test aaa statements for VLAN-OOB subscribers (MX Series)—Starting in Junos OS Release 16.1, you can use the no-address-request option with the test aaa dhcp user and test aaa ppp user statements for testing subscribers in a Layer 2 scenario where no address allocation request is required.

The output of these two statements now displays two additional user attributes. **Dynamic Profile** is the name of the profile received in the Client-Profile-Name VSA (26-174). **Routing Instance** is the name of the routing instance conveyed by the Virtual-Router VSA (26-1). The existing **Virtual Router Name** attribute is the locally configured name of the logical system.

[See Testing a Subscriber AAA Configuration.]

- New predefined variables and Juniper Networks VSAs for family any interface filters (MX Series)—Starting in Junos OS Release 16.1, you can use the $junos-input-interface-filter and $junos-output-interface-filter predefined variables to attach a filter to a dynamic interface created for family any. The filter names are derived from the Juniper Networks VSAs, Input-Interface-Filter (26-191), and Output-Interface-filter (26-192). These VSAs are conveyed in the following RADIUS messages: Access-Request, Acct-Start, Acct-Stop, and Acct-Interim-Interval. You can specify the variables as the filter names with input and output statements at the [edit
dynamic-profiles profile-name interfaces interface-name unit logical-interface-number filter] hierarchy level.

[See Juniper Networks VSAs Supported by the AAA Service Framework.]

- New predefined variable to group subscribers on a physical interface (MX Series)—Starting in Junos OS Release 16.1, you can specify the new Juniper Networks predefined variable, $junos-phy-ifd-interface-set-name, with the interface-set statement at the [edit dynamic-profiles profile-name interfaces] hierarchy level to configure an interface set associated with the underlying physical interface in a dynamic profile. This predefined variable enables you to group all the subscribers on a specific physical interface so that you can apply services to the entire group of subscribers.

  Another use case is optimizing CoS level 2 node resources by grouping residential subscribers into an interface set associated with the physical interface in a topology where residential and business subscribers share the interface, enabling the use of CoS level 2 nodes for the interface set rather than for each residential interface.

  [See CoS for Interface Sets of Subscribers Overview.]

- Configuring default values for routing instances (MX Series)—Starting in Junos OS Release 16.1, you can define a default value for the Juniper Networks predefined variable, $junos-routing-instance. This value is used in the event RADIUS does not supply a value for $junos-routing-instance. To configure a default value, use the predefined-variable-defaults statement at the [edit dynamic-profiles] hierarchy level. For example, to set the default value to RI-default:

  [edit dynamic-profiles profile-name]
  user@host# set predefined-variable-defaults routing-instance RI-default

- Address-assignment pool hold-down (MX Series)—Starting in Junos OS Release 16.1, you can place an active address-assignment pool in a hold-down state. When a pool is in the hold-down state, no additional addresses are allocated from that pool. However, the hold-down state does not affect any existing subscribers that are using addresses previously assigned from the pool.

  As the existing subscribers disconnect, their IP addresses are marked as free in the pool, but the addresses are not reallocated because of the pool’s hold-down state. Eventually, when all subscribers have disconnected and their addresses are returned to the pool, the pool becomes inactive. When the pool is in the inactive state, you can safely perform maintenance on the pool (such as adding, changing, or deleting addresses) without affecting any active subscribers.

  [See Configuring Address-Assignment Pool Hold Down.]

- Support for subscriber management and services feature parity (MX104)—Starting in Release 16.1, the MX104 supports all subscriber management and services features that are supported on the MX240, MX480, and MX960 routers as of Junos OS Release 14.1R1. Previously, the MX104 matched feature support with the MX80 as of Junos OS Release 13.3R1.

- PPPoE-over-ATM support and other enhancements to PPPoE subscriber session lockout (MX Series)—Starting in Junos OS Release 16.1, PPPoE subscriber session lockout supports PPPoE-over-ATM subscriber interfaces and also adds the following enhancements:
Persistence of the lockout condition after automatic removal of dynamic VLAN or VLAN demultiplexing (demux) subscriber interfaces.

Termination of the lockout condition after administratively clearing the lockout or resetting the interface module.

Ability to clear the lockout condition or display information about the lockout status by specifying encapsulation type identifier characteristics when no underlying interface exists for the subscriber session:

- VLAN identifiers (device name, S-VLAN ID, and VLAN ID) in the `clear pppoe lockout vlan-identifier` and `show pppoe lockout vlan-identifier` commands
- ATM identifiers (device name, VPI, and VCI) in the `clear pppoe lockout atm-identifier` and `show pppoe lockout atm-identifier` commands

[See PPPoE Subscriber Session Lockout Overview.]

New reject action for a LAC receiving change requests from the LNS (MX Series)—Starting in Junos OS Release 16.1, you can configure the LAC to reject change requests received in SCCRP messages from the LNS. During tunnel establishment, the LNS might include a request for the LAC to change the destination IP address, UDP port, or both, that it uses to communicate with the LNS. When a LAC that is configured to reject these requests receives one, it sends a StopCCN message to the original address or port and then terminates the connection to that LNS. This reject option is in addition to the previously available accept and ignore options.

[See Configuring How the LAC Responds to Address and Port Changes Requested by the LNS.]

Enhanced subscriber management support for Ethernet OAM on S-VLANs with associated C-VLANs and subscriber interfaces (MX Series routers with MPCs/MICs)—This feature is supported in Junos OS Release 16.1 with no changes from the original 13.2R1 implementation. As such, when Ethernet IEEE 802.1ag Operation, Administration, and Maintenance (OAM) connectivity fault management (CFM) is configured on a static single-tagged service VLAN (S-VLAN) logical interface on a Gigabit Ethernet, 10-Gigabit Ethernet, or Aggregated Ethernet physical interface, you can configure the router to propagate the OAM state of the S-VLAN to the associated dynamic or static double-tagged customer VLAN (C-VLAN) logical interfaces. If the CFM continuity check protocol detects that the OAM state of the S-VLAN is down, you can configure the underlying physical interface to bring down all associated C-VLANs on the interface with the same S-VLAN (outer) tag as the S-VLAN interface. In addition, the router brings down all DHCP, IP demultiplexing (IP demux), and PPPoE logical subscriber interfaces configured on top of the C-VLAN. Propagation of the S-VLAN OAM state to associated C-VLANs ensures that when the OAM state of the S-VLAN link is down, the associated C-VLANs and all subscriber interfaces on top of the C-VLANs go down as well.

To enable propagation of the S-VLAN OAM state to associated C-VLAN logical interfaces, use the `oam-on-svlan` option when you configure a Gigabit Ethernet (ge), 10-Gigabit Ethernet (xe), or Aggregated Ethernet (ae) interface.

Ethernet OAM support for S-VLANs and associated C-VLANs is not currently supported for use with dynamic profiles, S-VLAN trunk interfaces, or C-VLAN trunk interfaces.
• **Support for manual targeting**—Starting in Junos OS Release 16.1R1, service providers can configure manual targeting—assigning specific member links as primary and backup links per subscriber so that all traffic goes through those links. Manual targeting enhances the distribution of targeted VLANs or subscribers across member links of an aggregated Ethernet bundle by making it bandwidth-aware.

You configure the targeting options by including the `targeted-options` statement at the `[edit interfaces ae aggregated-ether-options]` hierarchy level.

You can select the targeting type for an aggregated Ethernet bundle as **manual** or **auto** at the `[edit interfaces ae aggregated-ether-options targeted-options]` hierarchy level.

When you configure manual targeting, you must always configure a primary link. Configuring a backup link is optional. You specify the primary and backup links for a subscriber in the individual interface configuration.

If the aggregated Ethernet bundle is configured for manual targeting, then all the subscribers in that bundle can be optionally configured for manual targeting, but none of them can be configured for autotargeting (targeted distribution). That is, you cannot have a configuration that contains a mix of manual targeting and autotargeting among subscribers. If the aggregated Ethernet bundle is not configured for manual targeting, then you can optionally configure autotargeting for all the subscribers, but you cannot configure manual targeting for any of them. Manual targeting and autotargeting are supported only on static interfaces.

• **Grouping of subscribers with similar bandwidth usage**—Junos OS Release 16.1R1 supports grouping of subscribers with similar bandwidth usage and ensures even distribution of subscribers in each group across the member links of an aggregated Ethernet bundle. Service providers can group together subscribers with similar bandwidth usage and optionally assign a group name. Subscribers that are configured for targeted distribution without a group name are added to the `default` group and distributed evenly across member links. Grouping of subscribers is supported only for static subscribers.

You can specify the group name by including the `group` statement at the `[edit interfaces interface-name unit logical-unit-number targeted-options]` hierarchy level.

• **Configurable session limits for L2TP (MX Series)**—Starting in Junos OS Release 16.1, you can configure a limit on the maximum number of L2TP sessions allowed for the chassis, for all tunnels, for a tunnel-group, for a client group, and for a client. When the session limit is reached, no new sessions can be established until the number of current sessions drops below the configured limit. One use of this feature is to control the number of sessions from an enterprise customer that is connected over LACs in multiple locations. These configured session limits have no effect on the maximum supported chassis limits that are imposed through the Juniper Networks license.

  [See Limiting the Number of L2TP Sessions Allowed by the LAC or LNS.]

• **Ensuring IPCP negotiation for IPv4 DNS addresses (MX Series)**—Starting in Junos OS Release 16.1, the router can prompt customer premises equipment (CPE) to negotiate both primary and secondary IPv4 DNS addresses during IPCP negotiation. This feature is useful when the CPE fails to send DNS address options in the IPCP configure request message, or when the options are sent but rejected. In earlier releases,
either situation results in no DNS address negotiation even though IPv4 DNS addresses are available on the router. This DNS option enables the router to control IPv4 DNS address provisioning for dynamic and static, terminated PPPoE and LNS subscribers.

[See Ensuring IPCP Negotiation for Primary and Secondary DNS Addresses.]

- **Filters for duplicate RADIUS accounting interim reports (MX Series)**—Starting in Junos OS Release 16.1, you can specify which accounting servers receive the RADIUS accounting interim reports when RADIUS accounting duplicate reporting is active.

Subscriber management supports the following filtering for RADIUS accounting duplicate reporting:

  - Duplicated accounting interim messages—The accounting messages are sent only to RADIUS accounting servers in the subscriber’s access profile.
  
  - Original accounting interim messages—The accounting messages are sent only to servers in a duplication access profile other than the subscriber’s access profile.
  
  - Excluded RADIUS attributes—RADIUS attributes in accounting messages are filtered based on the `exclude` statement configuration.

  The `exclude` statement supports new attributes.

  [See Understanding RADIUS Accounting Duplicate Reporting.]

- **Multiple DHCPv6 IA_NA and IA_PD requests (MX Series)**—Starting in Junos OS Release 16.1, DHCPv6 relay agent supports multiple DHCPv6 IA_NA or IA_PD requests within the same Solicit message, up to a maximum of eight requests. This support enables each negotiated lease to have its own lease expiration time and also allows one lease to expire without tearing down any other active leases. The multiple IA address support also enables customers to delegate multiple address blocks to a CPE router, which simplifies flow classification and service monetization.

  In Junos OS releases before Release 16.1, the router supports one IA_NA request or one IA_PD request, or a combination of one of each type of request.

  [See Multiple DHCPv6 IA_NA and IA_PD Requests Per Client Interface.]

- **New VSAs for IPv4 and IPv6 link addresses of first DHCP relay into RADIUS Auth and Accounting Messages (MX Series)**—Starting in Junos OS Release 16.1, two new VSAs, `DHCP-First-Relay-IPv4-Address` and `DHCP-First-Relay-IPv6-Address`, are available for configuration of a RADIUS server. The values of these new VSAs are the link address of the first relay of a DHCPv4 or DHCPv6 client/server binding. These new VSAs are sent to RADIUS as part of Access-Request, Accounting-Start, Accounting-Interim, and Accounting-Stop Messages. These VSAs enable RADIUS to identify clients uniquely for your business purposes, such as keeping track of your billing clients.

  [See Juniper Networks VSAs Supported by the AAA Service Framework.]
Five-Level Hierarchical CoS (MX240, MX480, MX960, and MX2020 Series)—Starting in Junos OS Release 16.1, the Broadband Network Gateway (BNG) supports 5-level hierarchical CoS (HCoS) in dynamic configurations. It allows you to differentiate and shape traffic at the following levels:

- Level 1—Physical interface (port level)
- Level 2—Interface set, for example, S-VLAN (access node)
- Level 3—Customer VLAN (C-VLAN)
- Level 4—Session logical interface (ppp or dhcp)
- Level 5—Service queues (up to 8)

The use cases that five-level HCoS supports include:

- Residential and business traffic on the same access node (if business interfaces are dynamic).
- Multiple retail ISPs on the same access node.
- Multiple subscriber sessions for a household on the same C-VLAN.

This feature is not supported on agent circuit identifier (ACI) sets or aggregated Ethernet (AE) interfaces.

[See Understanding Hierarchical CoS for Subscriber Interfaces.]

Support for IP reassembly on an L2TP connection (MX Series routers with MPC5E)—Starting in Junos OS Release 16.1, you can configure the service interfaces on MX Series routers with MPC5E to support IP packet reassembly on a Layer 2 Tunneling Protocol (L2TP) connection. The IP packet is fragmented over an L2TP connection when the packet size exceeds the maximum transmission unit (MTU) defined for the connection. Depending on the direction of the traffic flow, the fragmentation can occur either at the L2TP access concentrator (LAC) or at the L2TP network server (LNS), and reassembly occurs at the peer interface. (In an L2TP connection, a LAC is a peer interface for the LNS and vice versa.)

You can configure the service interfaces on the LAC or on the LNS to reassemble the fragmented packets before they can be further processed on the network. On a router running Junos OS, a service set is used to define the reassembly rules on the service interface. The service set is then assigned to the L2TP service at the [edit services l2tp] hierarchy level to configure IP reassembly for L2TP fragments.

[See IP Packet Fragment Reassembly for L2TP Overview.]

Diameter Network Access Server Requirements (NASREQ) authentication and authorization (MX Series)—Starting in Junos OS Release 16.1, Junos OS supports the Diameter-based Network Access Server Requirements (NASREQ) protocol for authentication and authorization at login. NASREQ is described in RFC 7155. Junos OS supports the following NASREQ protocol exchanges:

- AA-Request/Answer—The authentication/authorization request at login.
- Session-Termination-Request/Answer—Notification that the subscriber’s session has been terminated.
• Abort-Session-Request/Answer—Request to terminate the subscriber’s session from a NASREQ server.

[See Diameter Network Access Server Requirements (NASREQ).]

• Communicating with RADIUS servers over IPv6 (MX Series)—Starting in Junos OS Release 16.1, subscriber management supports RADIUS connectivity over IPv6, in addition to IPv4 connectivity. This support enables you to specify the IPv6 addresses of your targeted RADIUS servers, and also enables you to specify IPv6 addresses for the source address configuration of your RADIUS servers.

Also in Release 16.1, the AAA process now supports the NAS-IPv6-Address RADIUS attribute (attribute 95), which identifies the IPv6 address of the NAS that requests subscriber authentication.

[See Configuring Router or Switch Interaction with RADIUS Servers.]

• Limiting the subscriber sessions per aggregated Ethernet or Packet Forwarding Engine bundle (MX Series)—Starting in Junos OS Release 16.1, you can restrict the number of Point-to-Point Protocol over Ethernet (PPPoE) subscriber sessions per aggregated Ethernet or Packet Forwarding Engine bundle by using the existing PPPoE Service-Name table. You can modify the existing PPPoE Service-Name table by changing its default configuration to eliminate the default empty Service-Name entry in the Service-Name table.

In earlier releases, each PPPoE service name table in the service (PPPoE) configuration statement included one empty service entry by default.

• Support for unlocking destinations during LAC tunnel selection (MX Series)—Starting in Junos OS Release 16.1, the tunnel selection process for a subscriber login enables the LAC to cycle through the tunnel preference levels until it establishes a session to a destination or has attempted to contact every valid destination but failed.

In earlier releases, if the LAC reaches the lowest level and all valid destinations at that level are locked, it selects the destination with the shortest remaining lockout time, removes the lockout, and attempts to connect to that destination. If it fails, it does not cycle back through the preference levels.

You can use the new clear services l2tp destination lockout command to manually clear all locked destinations or only locked destinations that match the specified local or remote gateway address.

[See LAC Tunnel Selection Overview.]

• Support for DHCPv6 duplicate client DUIDs (MX Series)—Starting in Junos OS Release 16.1, you can configure DHCPv6 relay agent and DHCPv6 local server to support DHCP clients that have the same DHCP unique identifier (DUID) when the DHCPv6 requests are received on different underlying interfaces.

Typically, the router treats a request from a duplicate client as a renegotiation, and replaces the existing client entry with a new entry. However, in some cases, the duplicate request is from a different client, and replacement is not desired. When you enable duplicate client support, the router uses the underlying interfaces to differentiate between two clients with the same DUID, enabling both clients to be granted leases.
The router retains the existing client entry, and creates a new entry for the duplicate client.

[See DHCPv6 Duplicate Client DUIDs.]

- Improved multicast convergence and RPT-SPT support for BGP-MVPN (MX Series)—Starting with Junos OS Release 16.1, support for multicast forwarding-cache threshold is extended to rendezvous-point tree shortest-path tree (RPT-SPT) mode for BGP-MVPN. In addition, for both Rosen and next-generation MVPNs, PE routers across all sites should see the same set of multicast routes even if the configured forwarding-cache limit is exceeded.

To configure a specific threshold for MVPN RPT, set one or both of the `mvpn-rpt-suppress` and `mvpn-rpt-reuse` statements at the `[edit routing-instances name routing-options multicast forwarding-cache]` or `[edit logical system name routing-instances name routing-options multicast forwarding-cache]` hierarchy level.

In addition, the `show multicast forwarding-cache statistics` command provides information about both the general and RPT-suppression states. Likewise, a list of suppressed customer-multicast states can be seen by running the `show mvpn suppressed general|mvpn-rpt inet|inet6 instance name summary` command.

- Targeted distribution for VLAN demux logical interface sets over aggregated Ethernet (MX Series)—Starting in Junos OS Release 16.1R1, you can enable targeted distribution to guarantee that subscribers, who are members of the same interface set of VLAN demux logical interfaces over an aggregated Ethernet bundle, each receive the same link selection. By collectively configuring link selection for an entire interface set of subscribers, you can effectively eliminate possible human errors by having to configure link selection on a per-subscriber basis.

**System Logging**

- System log messages to indicate checksum errors on the DDR3 interface—Starting in Junos OS Release 13.3 R9, two new system log messages, `XMCHIP_CMERROR_DDRIF_INT_REG_CHKSUM_ERR_MINOR` and `XMCHIP_CMERROR_DDRIF_INT_REG_CHKSUM_ERR_MAJOR`, are added to indicate memory-related problems on the interfaces to the double data rate type 3 (DDR3) memory. These error messages indicate that an FPC has detected a checksum error, which is causing packet drops.

  The following error threshold values classify the error as a major error or a minor error:

  - Minor error—6-254 errors per second
  - Major error—255 and more errors per second

- New configuration statement for filtering text substring in system log messages (MX Series and T Series)—Starting with Junos OS Release 16.1, a new configuration statement, `match-string <string-name>`, helps you display specified text substrings in the system log messages when using the `show system syslog` statement. The `match-string <string-name>` configuration statement can be configured at the following hierarchy levels:

  - `edit system syslog file <file-name>`
• edit system syslog host <host-name>

• edit system syslog user <user-name>

This statement can be configured along with the match <string-name> configuration statement. In addition, it reduces the CPU usage while filtering the text substring in the system log messages.

[See match-string.]

System Management

• Statement introduced to deny hidden commands—Starting in Release 16.1, Junos OS allows users to deny hidden commands to all users except root. To deny hidden commands to all users except root, use the set system no-hidden-commands statement at the [edit] hierarchy level.

Timing and Synchronization

• Support for PTP over IPv6/UDP encapsulation (MX240, MX480, and MX960)—Starting with Junos OS Release 16.1, Precision Time Protocol (PTP) is supported over IPv6/UDP encapsulation on MX240, MX480, and MX960 routers. This functionality is supported in compliance with PTP over IPv6/UDP encapsulation defined in Annex E of 1588 standard.

NOTE: In earlier Junos releases, PTP is supported over IPv4/UDP encapsulation.

User Interface and Configuration

• Support for JSON format for configuration data (MX Series and T Series)—Starting with Junos OS Release 16.1, you can configure devices running Junos OS using configuration data in JavaScript Object Notation (JSON) format in addition to the existing text, Junos XML, and Junos OS set command formats. You can load configuration data in JSON format in the Junos OS CLI by using the load (merge | override | update) json command or from within a NETCONF or Junos XML protocol session by using the <load-configuration format="json"> operation. You can load JSON configuration data either from an existing file or as a data stream. Configuration data that is provided as a data stream must be enclosed in a <configuration-json> element.

[See load, Defining the Format of Configuration Data to Upload in a Junos XML Protocol Session, and Mapping Junos OS Configuration Statements to JSON.]

• Extend the Junos CLI command set with custom scripts (MX Series)—Starting with Junos OS Release 16.1, you can configure devices running Junos OS to allow your custom scripts to be invoked in the Junos OS CLI or from within a NETCONF or Junos XML protocol session. The custom script can be written in either SLAX or Python. Configure
your custom script to act as a native command using Yang's RPC keyword extension. Its location in the command schema is specified in a Yang module.

[See Junos Automation Scripting Overview, Using Juniper Networks YANG Modules.]

Virtual Chassis

- **MX Series Virtual Chassis support for L2TP LNS (MX Series)—**Starting in Junos OS Release 16.1, MX Series Virtual Chassis configurations support L2TP LNS functionality.

[See L2TP for Subscriber Access Overview.]

- **MX Series Virtual Chassis commit time improvements (MX Series with MPCs/MiCs)—**Starting in Junos OS Release 16.1, the commit process for MX Series Virtual Chassis is optimized to provide faster commit times. No additional configured is required to take advantage of the improved commit times. You can use the 
  commit | display detail 
  command to monitor the steps of the new commit process.

- **MX Series Virtual Chassis support for MX240 and MX480 member routers in a VC containing MX2010 or MX2020 member routers (MX Series with MPCs/MiCs)—**Starting in Junos OS Release 16.1, you can configure a MX240 router or MX480 router as a member router in an MX Series Virtual Chassis that contains a MX2010 or MX2020 member router. In earlier releases, MX2010 routers and MX2020 routers could only interoperate with MX960 routers.

The following member router combinations are introduced in Junos OS Release 15.2 for a two-member Virtual Chassis configuration:

- MX240 router and MX2010 router
- MX240 router and MX2020 router
- MX480 router and MX2010 router
- MX480 router and MX2020 router

VPNs

- **Redundant virtual tunnels on MPCs (MX Series)—**In multicast Layer 3 VPNs, virtual tunnel (VT) interfaces are needed to facilitate virtual routing and forwarding (VRF) table lookup based on MPLS labels. Beginning with Junos OS Release 16.1, support for redundant VTs at the Packet Forwarding Engine level is provided to improve resiliency in delivering multicast traffic.

[See Redundant Virtual Tunnels Providing Resiliency in Delivering Multicast Traffic Overview.]

- **MVPN source-active upstream multicast hop selection and redundant source improvements (MX Series)—**Starting in Junos OS Release 16.1, you can use new configuration statements available at the [edit protocols mvpn] hierarchy level to influence the source-active upstream multicast hop selection process. You can use the 
  umh-selection-additional-input 
  statement to influence the upstream multicast hop selection by making the MVPN consider a combination of route preference and RSVP tunnel status. You can use the 
  source-redundancy 
  statement so that the MVPN acts on all redundant sources sending to a specific group address as the same source.
NOTE: This feature is documented but not supported in Junos OS Release 16.1R1.

Support for common Public Key Infrastructure (PKI) functionality (MX Series)—Starting in Junos OS Release 16.1R1, MX Series devices support the following common PKI functionalities:

- **Certificate chaining**—Certificate-based authentication is an authentication method supported on MX Series devices during IKE negotiation. In large networks, multiple certificate authorities (CAs) can issue end entity (EE) certificates to their respective end devices. It is common to have separate CAs for individual locations, departments, and organizations. With a single-level hierarchy for certificate-based authentication, all EE certificates in the network must be signed by the same CA. All firewall devices must have the same CA certificate enrolled for peer certificate validation. The certificate payload sent during IKE negotiation only contains EE certificates.

  In Junos OS Release 16.1R1, the certificate payload sent during IKE negotiation can contain a chain of EE and CA certificates. A certificate chain is the list of certificates required to certify the subject in the EE certificate. The certificate chain includes the EE certificate, intermediate CA certificates, and the root CA certificate. CA certificates can be enrolled using the Simple Certificate Enrollment Process (SCEP) or loaded manually. There is no new CLI configuration statement or command for certificate chains; however, every end device must be configured with a CA profile for each CA in the certificate chain.

  The network administrator needs to ensure that all peers participating in IKE negotiation have at least one common trusted CA in their respective certificate chains. The common trusted CA does not have to be the root CA. The number of certificates in the chain, including certificates for EEs and the topmost CA in the chain, cannot exceed 10.

- **Online Certificate Status Protocol (OCSP)**—OCSP checks the revocation status of X509 certificates. Requests are sent to the OCSP server(s) configured in a CA profile with the `ocsp url` statement at the `[edit security pki ca-profile profile-name revocation-check]` hierarchy level. The `use-ocsp` option must also be configured. If there is no response from the OCSP server, the request is then sent to the location specified in the certificate’s AuthorityInfoAccess extension.

- **Digital certificate validation**—The PKI daemon on MX Series devices performs X509 certificate policy, path, key usage, and distinguished name validation, as specified in RFC 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*.

- **New configuration statement to manage VCCV BFD session state (MX Series)**—Starting with Junos OS Release 16.1, the `ping-multiplier` statement is introduced to delay the virtual circuit connectivity verification (VCCV) Bidirectional Forwarding Detection (BFD) session from going down by the specified number of LSP ping packets. The VCCV BFD session is signaled down only after the specified number of LSP ping packets are lost. This feature is supported for Layer 2 Circuit, Layer 2 VPN, and VPLS technologies.
To configure the LSP ping multiplier feature, include the `ping-multiplier` `number-of-packets` statement at the `[edit protocols l2circuit neighbor neighbor-address interface interface-name oam]`, `[edit routing-instances routing-instances-name protocols l2vpn oam]`, and `[edit routing-instances routing-instances-name protocols vpls oam]` hierarchy levels for Layer 2 circuit, Layer 2 VPN, and VPLS, respectively.

### Related Documentation
- Changes in Behavior and Syntax on page 107
- Known Behavior on page 121
- Known Issues on page 124
- Resolved Issues on page 129
- Documentation Updates on page 132
- Migration, Upgrade, and Downgrade Instructions on page 134
- Product Compatibility on page 142

### 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 16.1R1 for MX Series and T Series.

- General Routing on page 107
- Interfaces and Chassis on page 108
- Junos FIPS on page 108
- Junos OS XML API and Scripting on page 109
- Layer 2 Features on page 109
- MPLS on page 110
- Network Management and Monitoring on page 110
- Routing Policy and Firewall Filters on page 111
- Routing Protocols on page 111
- Security on page 112
- Services Applications on page 114
- Software Installation and Upgrade on page 115
- Subscriber Management and Services (MX Series) on page 115
- System Logging on page 120
- System Management on page 120
- User Interface and Configuration on page 120

### General Routing

- **New option introduced** under `show` | `display xml` | `display`—Starting in Junos OS 16.1R1, you can use the `show` | `display xml` | `display` | `mark-changed` statement to view the "mark-changed" status of the nodes. This is useful for debugging purpose.
Enhancement to request support information command—Starting in Junos OS Release 16.1R1, the request support information command is enhanced to capture the following additional details:

- file list detail /var/rundb/—Displays the size of configuration databases.
- show system configuration database usage—Displays the actual usage of configuration database.

**NOTE:** This information will be displayed only if the show system configuration database usage command is supported in the release.

- file list detail /config/—Contains the db_ext file and shows the size of it to indicate whether extend_size is enabled or disabled.

Modified output of the clear services sessions | display xml command (MX Series)—In Junos OS Release 16.1, the output of the clear services sessions | display xml command is modified to include the `<sess-marked-for-deletion>` tag instead of the `<sess-removed>` tag. In releases before Junos OS Release 14.1X55-D30, the output of this command includes the `<sess-removed>` tag. The replacement of the `<sess-removed>` tag with the `<sess-marked-for-deletion>` tag aims at establishing consistency with the output of the clear services sessions command that includes the field Sessions marked for deletion.

Interfaces and Chassis

- Change in enforcement of vtmapping restriction for Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP (H)—Starting with Junos OS Release 16.1, a commit error occurs when you include the `vtmapping` statement under the `[edit interfaces interface-name sonet-options]` hierarchy for cau4 interfaces on the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP (H). Prior to Junos OS Release 16.1R1, a commit error was not displayed when this restriction was violated.

- Starting in Junos OS Release 16.1, the show pfe statistics traffic command now displays the following fabric statistics:
  - Fabric Input packets—Number and rate of incoming fabric packets
  - Fabric Output packets—Number and rate of outgoing fabric packets

See show pfe statistics traffic.

Junos FIPS

- Change in range of client alive messages for SSH—Starting with Junos OS Release 16.1R1, you can configure 0 through 255 as the range for configuring the number of client alive messages that can be sent without sshd receiving any messages back from the client. In releases before Junos OS Release 16.1R1, the range for configuring client alive messages is 1 through 255.

[See client-alive-count-max.]
Change in default configuration for root login through SSH—Starting with Junos OS Release 16.1R1, deny-password is the default option at the [edit system services ssh root-login] hierarchy level. That is, by default, users are allowed to log in to the router or switch as root through SSH when the authentication method does not require a password. In releases before Junos OS Release 16.1R1, the allow is the default option at the [edit system services ssh root-login] hierarchy level.

[See root-login and Configuring SSH Service for Remote Access to the Router or Switch.]

Junos OS XML API and Scripting

Support for a configuration revision identifier to enable NMS determine synchronization status of devices (MX Series and T Series)—Starting in Junos OS Release 16.1, a configuration revision identifier string, the <commit-revision-information> tag, is supported within the <commit-results> tag. The configuration revision identifier is used to determine whether the configuration settings on devices being managed by a network management server (NMS) application is in synchronization (sync) with the CLI of devices running Junos OS. In a real-world network deployment, out-of-band configuration commits might occur on a device, such as during a maintenance window for support operations. In such cases, the NMS application queries Junos OS to retrieve the latest revision number and compares it against the revision number stored locally to validate whether it is out-of-sync or in-sync with the device to detect the out-of-band commits.

Layer 2 Features

Discrepancy in the reported BUM traffic—There is a discrepancy in the amount of BUM traffic reported on the aggregated Ethernet (AE) link between a designated forwarder (DF) and non-DF router. In an active-active configuration, the interface on the router in a DF role reports receiving twice as many packets as was sent from the interface of the router in a non-DF role.

Option to display the age of a single MAC entry—Beginning with Junos OS Release 16.1, a new option age is added to the command show vpls mac table to display the age of a single MAC address for a given VPLS instance. For GE interfaces, age displays the MAC address aging time for a given VPLS instance. For AE interfaces, the age is reported for a given VPLS instance, separately for all the line cards.

[See show vpls mac-table.]

Option to display the age of a single MAC entry—Beginning with Junos OS Release 16.1, a new option age is added to the command show bridge mac table to display the age of a single MAC address for a given bridge. For GE interfaces, age displays the MAC address aging time for a given bridge instance. For AE interfaces, the age is reported for a given bridge instance, separately for all the line cards.

[See show bridge mac-table.]

Option to display the age of a single MAC entry—Beginning with Junos OS Release 16.1, a new option age is added to the command show evpn mac table to display the age of a single MAC address for a given evpn instance.
[See show evpn mac-table.]

- **Support for configuring MAC move parameters globally (MX Series)**—Starting in Junos OS Release 16.1, you can configure parameters for media access control (MAC) address move reporting by including the `global-mac-move` statement and its substatements at the `[edit protocols l2-learning]` hierarchy level. When a MAC address appears on a different physical interface or within a different unit of the same physical interface and this behavior occurs frequently, it is considered a MAC move. You can configure the router to report a MAC address move based on the following parameters: the number of times a MAC address move occurs, a specified period of time over which the MAC address move occurs, and the specified number of times a MAC address move occurs in one second.

**MPLS**

- **LSPs displayed in lexicographic order (MX Series)**—Starting with Junos OS Release 16.1, the LSPs are displayed in lexicographic order in the output of the `show mpls lsp` command. In earlier releases, this command displayed the LSPs in the order in which they were configured.

- **Inline BFD support on IRB interfaces (MX Series routers with MPCs or MICs)**—Starting with Junos OS Release 16.1, the inline BFD sessions transmitted or received from FPC hardware are supported on integrated routing and bridging (IRB) interfaces. This enhancement is available only on MX Series routers with MPCs/MICs that have configured the `enhanced-ip` option.

- **Point-to-multipoint LSP ping echo reply ignored on Juniper side in Cisco-Juniper interoperability (MX Series and T Series)**—Currently, in a Juniper-Cisco interoperation network scenario, a point-to-multipoint LSP ping echo reply message from a Cisco device in a different IGP area is dropped on the Juniper device when the source address of the reply message is an interface address other than the loopback address or router ID.

Starting with Junos OS Release 14.2R6, 15.1R4, 16.1, and later releases, such point-to-multipoint LSP ping echo reply messages are accepted by the Juniper device and the messages get logged as uncorrelated responses.

**Network Management and Monitoring**

- **Updated unified container set in enterprise-specific Chassis MIB (MX Series)**—Starting with Junos OS Release 16.1, the Juniper Networks enterprise-specific Chassis MIB (`jnxBoxAnatomy`) provides a unified container set that represents all supported MX Series chassis types when MX Series Virtual Chassis mode is active.

- **New lease query and bulk lease query definitions for the DHCP MIB (MX Series)**—Starting in Junos OS Release 16.1R1, the DHCP mib, `jnx-jdhcp.mib`, now includes the following definitions to collect statistics for DHCP lease query and bulk lease query messages for DHCP local server and DHCP relay:

<table>
<thead>
<tr>
<th>In <code>jnx-jdhcpLocalServerStatistics</code></th>
<th>In <code>jnx-jdhcpRelayStatistics</code></th>
</tr>
</thead>
<tbody>
<tr>
<td><code>jnxJdhcpLocalServerLeaseQueryReceived</code></td>
<td><code>jnxJdhcpRelayLeaseQuerySent</code></td>
</tr>
</tbody>
</table>
In jnxDhcpLocalServerStatistics

| jnxDhcpLocalServerBulkLeaseQueryReceived | jnxDhcpLocalServerBulkLeaseQuerySent |
| jnxDhcpLocalServerLeaseActiveSent        | jnxDhcpLocalServerLeaseActiveReceived |
| jnxDhcpLocalServerLeaseUnknownSent       | jnxDhcpLocalServerLeaseUnknownReceived |
| jnxDhcpLocalServerLeaseUnAssignedSent    | jnxDhcpLocalServerLeaseUnAssignedReceived |
| jnxDhcpLocalServerLeaseQueryDoneSent     | jnxDhcpLocalServerLeaseQueryDoneReceived |

- **SNMP proxy feature (MX Series)**—Starting with Junos OS Release 16.1, you must configure `interface <interface-name>` statement at the [edit snmp] hierarchy level for the proxy SNMP agent. Earlier, configuring interface for the proxy SNMP agent was not mandatory.

- **Change in the output of snmp mib walk of the jnxVpnIfStatus MIB object (MX Series)**—Starting with Junos OS Release 16.1R1, the `show snmp mib walk jnxVpnIfStatus` command provides information for all interfaces, except the Juniper Networks specific dynamic interfaces.

Routing Policy and Firewall Filters

- **New policy actions to set and modify AIGP attribute (MX Series and T Series)**—Beginning with Junos OS 16.1, a new policy action `metric-aigp` is added to configure the accumulated interior gateway protocol (AIGP) metric value as the IGP metric and `aigp-adjust` is introduced to modify this configured accumulated interior gateway protocol (AIGP) attribute at the [edit policy-options policy-statement policy-name term term-name then] hierarchy levels. You can make minor adjustments on the AIGP from another AS or for scaling from one IGP domain to another.

  [See `aigp-adjust`.

Routing Protocols

- **New option to configure the bandwidth-based metric (MX Series)**—Beginning with Junos OS Release 16.1, you can configure the delay time that the IS-IS takes before replacing the metric with a new metric value when the bundle changes from a worse metric to a better metric. The new configuration option `interface-group-holddown-delay` is available at the [edit protocols isis interface interface-name] hierarchy level.

A new show command `show isis interface-group` displays the status information for the specified interface group.

  [See `show isis interface-group`.

- **New option to configure IPv6 router advertisement preference (MX Series)**—Beginning with Junos OS Release 16.1, you can configure preference for routers, which is communicated to IPv6 hosts through router advertisements. A new configuration
statement preference is introduced at the [edit protocols router-advertisement interface interface-name] hierarchy level.

[See preference.]

• Change in command output for system statistics for IP and IP6—Beginning with Junos OS Release 16.1, the output of show system statistics ip and show system statistics ip6 operations commands is modified. The output now displays the field fragment sessions dropped (queue overflow) for IP instead of fragments dropped (queue overflow), and fragment sessions dropped (queue overflow) for IP6, instead of fragments that exceeded limit.

• Support of sham-links on default instances—Starting with Junos OS Release 16.1, OSPF sham-links are supported on default instances. The cost of the sham-link is dynamically set to the aigp-metric of the BGP route if no metric is configured on the sham-link by the user.

• New option to delay BGP route advertisements (MX Series)—Beginning with Junos OS Release 15.1f6, you can delay BGP route updates to its peers until the forwarding table is synchronized. This is to avoid premature route advertisements that might result in traffic loss. A new configuration statement delay-route-advertisements is available at the [edit routing-instances routing-instance-name protocols bgp group group-name family inet unicast] hierarchy level. You can configure both minimum and maximum delay periods to suit your network requirements.

[See delay-route-advertisements.]

• Contradictory configuration options not allowed—Beginning with Junos OS Release 15.1R4, you cannot configure both resolve and retain options for a statically configured route at the [edit routing-options] hierarchy level because they behave contradictorily. Resolved next hops cannot be retained, therefore you can configure only one of these options at a time.

Security

• Changes to DDoS protection protocol group and packet type support (MX Series)—Starting in Junos OS Release 16.1, the following changes have been made to the protocols statement at the [edit system ddos-protection] hierarchy level and to the output of the show ddos-protection protocols command:
  • Removed the firewall-host protocol group.
  • Removed the unclassified packet type from the mcast-snoop protocol group.
  • Added the unclassified packet type to the tcp-flags protocol group.

• Changes to distributed denial of service (DDoS) protection protocol groups and packet types (MX Series, T4000 with FPC5)—Starting in Junos OS Release 16.1, the following syntax changes have been made:
  • The mlp protocol group has been modified as follows to provide DDoS protection with full control of the bandwidth:
    • The aging-exc, packets, and vxlan packet types have been removed from the mlp protocol group.
• The \textit{add, delete, and lookup} packet types have been added to the \textit{mlp} protocol group. These packets correspond to the MAC learning command codes.

• The \textit{keepalive} protocol group has been renamed to \textit{tunnel-ka}.

• The \textit{firewall-host} protocol group and the \textit{mcast-copy} packet type in the \textit{unclassified} protocol groups have been removed from the CLI. They are now classified by the internal host-bound classification engine on the line card.

• \textbf{Changes to distributed denial of service (DDoS) protection default values for MLP packets (MX Series, T4000 with FPC5)}—Starting in Junos OS Release 16.1, the following default bandwidth (pps) and burst (packets) values apply for MLP packets by line card:

<table>
<thead>
<tr>
<th>Policier</th>
<th>MPC1, MPC2, MPC5, and MPC6</th>
<th>MPC3, MPC4, and FPC5</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Bandwidth</td>
<td>Burst</td>
</tr>
<tr>
<td>aggregate</td>
<td>10,000</td>
<td>20,000</td>
</tr>
<tr>
<td>add</td>
<td>4096</td>
<td>8192</td>
</tr>
<tr>
<td>delete</td>
<td>4096</td>
<td>8192</td>
</tr>
<tr>
<td>lookup</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td>unclassified</td>
<td>1024</td>
<td>1024</td>
</tr>
</tbody>
</table>

• \textbf{Changes to distributed denial of service (DDoS) protection flow detection defaults (MX Series, T4000 with FPC5)}—Starting in Junos OS Release 16.1, flow detection defaults to \textit{disabled} for the following protocol groups and packet type, because they do not have typical Ethernet, IP, or IPv6 headers. Global flow detection does not enable flow detection for these groups and the packet type.

  • Protocol groups: \textit{fab-probe, frame-relay, inline-ka, isis, jfm, mlp, pfe-alive, pos, services}.

  • Packet type: \textit{unclassified} in the \textit{ip-opt} protocol group.

• \textbf{Changes to show ddos-protection protocols command output (MX Series, T4000 with FPC5)}—Starting in Junos OS Release 16.1, when you disable DDoS protection policers on the Routing Engine or on an FPC for a specific packet type, an asterisk is displayed next to that field in the CLI output. For example, if you issue the following statements:

  \begin{verbatim}
  user@host# set system ddos-protection protocols mlp lookup disable-routing-engine
  user@host# set system ddos-protection protocols mlp lookup fpc 1 disable-fpc
  \end{verbatim}

the fields are marked as in the following sample output:

\begin{verbatim}
user@host> show ddos-protection protocols mlp lookup
Currently tracked flows: 0, Total detected flows: 0
* = User configured value
Protocol Group: MLP
\end{verbatim}
Packet type: lookup (MLP lookup request)

Individual policer configuration:
  Bandwidth: 1024 pps

Routing Engine information:
  Bandwidth: 1024 pps, Burst: 2048 packets, disabled*
  Policer is never violated
  Received: 0  Arrival rate: 0 pps
  Dropped: 0  Max arrival rate: 0 pps
  Dropped by aggregate policer: 0

FPC slot 1 information:
  Bandwidth: 100% (1024 pps), Burst: 100% (2048 packets), disabled*
  Policer is never violated
  Received: 0  Arrival rate: 0 pps
  Dropped: 0  Max arrival rate: 0 pps
  Dropped by aggregate policer: 0
  Dropped by flow suppression: 0

Services Applications

- **Class** `pcp-logs` and `alg-logs` are not configured for ms-interface (MX Series)—Starting with Junos OS Release 16.1R1, for multiservices (ms-) interfaces, you cannot configure system logging for PCP and ALGs by including the `pcp-logs` and `alg-logs` statements at the `[edit services service-set service-set-name syslog host hostname class]` hierarchy level. An error message is displayed if you attempt to commit a configuration that contains the `pcp-logs` and `alg-logs` options to define system logging for PCP and ALGs for ms- interfaces.

- **Support for configuring maximum number of measured video flows**—Starting in Junos OS Release 16.1, you can configure the maximum number of video flows that can be measured at a time. To configure the maximum number of flows measured, include the `flow-table-size max-flows` statement at the `[edit chassis fpc slot inline-video-monitoring]` hierarchy level.

  [See Configuring Inline Video Monitoring.]

- **Anycast address 0/0 must not be accepted in the from-clause of Detnat rule (MX Series)**—Starting with Junos OS Release 16.1R1, for multiservices (ms-) interfaces, anycast configuration is not allowed as the source-address when translation type is deterministic NAT.

- **Disabling NAT-traversal for IPsec-protected packets (MX Series)**—Starting in Junos OS release 16.1R1, you can include the `disable-natt` statement at the `[edit services ipsec-vpn]` hierarchy level to disable NAT-traversal (NAT-T) on MX Series routers. When you disable NAT-T, the NAT-T functionality is globally switched off. Also, even when a NAT device is present between the two IPsec gateways, only Encapsulating Security Payload (ESP) is used when you disable NAT-T. When NAT-T is configured, IPsec traffic is encapsulated using the UDP header, and port information is provided for the NAT devices. By default, Junos OS detects whether either one of the IPsec tunnels is behind a NAT device and automatically switches to using NAT-T for the protected traffic. However, in certain cases, NAT-T support on MX Series routers might not work as desired. Also, you might require NAT-traversal to be disabled if you are aware that the network uses IPsec-aware NAT. In such cases, you can disable NAT-T.
• **Exclude interfaces support in flowspec (rpdp-infra) (MX Series)**—Starting release 16.1, Junos OS excludes applying the flowspec filter to traffic received on specific interfaces. A new term is added at the beginning of the flowspec filter that accepts any packet received on these specific interfaces. The new term is a variable that creates an exclusion list of terms attached to the forwarding table filter as a part of the flow specification filter.

To exclude the flowspec filter from being applied to traffic received on specific interfaces, you must first configure a group-id on such interfaces by including the family inet filter group group-id statement at the [edit interfaces] hierarchy level, and then attach the flowspec filter with the interface group by including the flow interface-group group-id exclude statement at the [edit routing-options] hierarchy level. You can configure only one group-id per routing instance with the set routing-options flow interface-group group-id statement.

• **Support for deterministic NAPT (MX Series)**—You can configure deterministic port block allocation for Network Address Port Translation (NAPT) on MX Series routers with MS-MPCs or MS-MICs. By configuring deterministic NAPT, you ensure that translation of internal host IP (private IP to public IP and vice versa) is deterministic thus eliminating the need for address translation logging for each connection. To use deterministic port block allocation, you must specify deterministic-napt44 as the translation type in your NAT rule.

### Software Installation and Upgrade

• **Asia/Kolkata option replaces Asia/Calcutta option in time-zone statement**—Beginning with Junos OS Release 16.1, the time-zone statement has replaced the Asia/Calcutta option with Asia/Kolkata.

• **request system software add command options updated (MX Series and T Series)**—As of Junos OS Release 16.1, the upgrade-with-config-format option in the request system software add command is removed. The upgrade-with-config option applies to the file indicated. Specify .text or .xml. The upgrade-with-config option does not accept files with the extension .txt.

### Subscriber Management and Services (MX Series)

**NOTE:** Although present in the code, the subscriber management features are not supported in Junos OS Release 16.1R1. Documentation for subscriber management features is included in the Junos OS Release 16.1 documentation set.

• **Including termination reason for user logout events (MX Series)**—Starting in Junos OS Release 16.1, when the you enable the user-access flag at the [edit system processes general-authentication-service traceoptions] hierarchy level, the system log messages generated for authd include a termination reason for user logout events. In earlier releases, the log does not report any termination reasons.

Sample output before the behavior change:
g-e-1/0.100:100-1

Sample output after the behavior change:

Aug  6 21:15:55.106031 UserAccess:zf@example.com session-id:3 state:log-out
g-e-1/2/0.1:1 reason: ppp lcp-peer-terminate-term-req
Aug  6 21:16:42.654181 UserAccess:user234@example.com session-id:4 state:log-out
g-e-1/2/0.1:1 reason: ppp lower-interface-down
Aug  6 21:17:43.991585 UserAccess:duser9five@example.com session-id:5
state:log-out ge-1/2/0.1:1 reason: aaa shutdown-session-timeout

• Change in support for L2TP statistics-related commands (MX Series)—Starting in
  Junos OS Release 16.1, statistics-related show services l2tp commands cannot be
  issued in parallel with clear services l2tp commands from separate terminals. In earlier
  releases, you can issue these show and clear commands in parallel. Now, when any of
  these clear commands is running, you must press Ctrl+c to make the clear command
  run in the background before issuing any of these show commands.

  NOTE: You cannot run multiple clear services l2tp commands from separate
  terminals. This behavior is unchanged.

  [See clear services l2tp destination, clear services l2tp session, and clear services l2tp
tunnel.]

• Support for longer CHAP challenge local names (MX Series)—Starting in Junos OS
  Release 16.1, the supported length of the CHAP local name is increased to 32 characters.
  In earlier releases, only 8 characters are supported even though the CLI allows you to
  enter a longer name. You can configure the name with the local-name statement at the
  [edit dynamic-profiles profile-name interfaces pp0 unit "$junos-interface-unit"
  ppp-options] or [edit dynamic-profiles profile-name interfaces
  "$junos-interface-ifd-name" unit "$junos-interface-unit" ppp-options] hierarchy level.
  The maximum length of the local name for PAP authentication remains unchanged
  at 8 characters.

  [See Configuring the PPP Challenge Handshake Authentication Protocol.]

• Local DNS configurations available when authentication order is set to none (MX
  Series)—Starting in Junos OS Release 16.1, subscribers get the DNS server addresses
  when both of the following are true:

  • The authentication order is set to none at the [edit access profile profile-name
    authentication-order] hierarchy level.

  • A DNS server address is configured locally in the access profile with the
    domain-name-server, domain-name-server-inet, or domain-name-server-inet6
    statement at the [edit access profile profile-name] hierarchy level.

In earlier releases, subscribers get an IP address in this situation, but not the DNS server
addresses.

• Increased maximum limits for accounting and authentication retries and timeouts
  (MX Series)—Starting in Junos OS Release 16.1, you can configure a maximum of 100
  retry attempts for RADIUS accounting (accounting-retry statement) or authentication
(retry statement). In earlier releases, the maximum value is 30 retries. You can also configure a maximum timeout of 1000 seconds for RADIUS accounting (accounting-timeout statement) or authentication (timeout statement). In earlier releases the maximum timeout is 90 seconds.

NOTE: The maximum retry duration (the number of retries times the length of the timeout) cannot exceed 2700 seconds. An error message is displayed if you configure a longer duration.

[See Configuring Router or Switch Interaction with RADIUS Servers.]

- **Change in Routing Engine-based CPCD (MX Series)**—Starting in Junos OS Release 16.1, you must specify a URL with the `redirect` statement. You must also specify `destination-address address` with the `rewrite` statement. In earlier releases, you can successfully commit the configuration without these options.

- **Change in displayed value of LCP State field for tunneled subscriber sessions (MX Series)**—Starting in Junos OS Release 16.1, when a subscriber session has been tunneled from the LAC to the LNS, the LCP State field displayed by the `show interfaces ppp0 .unit` command has a value of Stopped, which correctly reflects the actual state of the LCP negotiation (because at this stage LCP is terminated at the LNS).

  In earlier releases, this field incorrectly shows a value of Opened, reflecting the state of LCP negotiation before tunneling started. In earlier releases, you must issue the `show ppp interface .unit` command to display the correct LCP state.

- **Improved result code reporting in stopCCN and CDN messages (MX Series)**—Starting in Junos OS Release 16.1, the LAC provides more accurate result codes and always includes error messages in the Result-Error Code AVP (1) included in the stopCCN and CDN messages that it sends to the LNS. Packet captures display the relevant information in the Result code, Error code, and Error Message fields of the AVP.

  In earlier releases, the result code is does not provide sufficient information about the cause of the event, and the error message is omitted for some result codes.

- **Syntax change for the show ancp neighbor command (MX Series)**—Starting in Junos OS 16.1, to specify a neighbor for display, the `show ancp neighbor` command allows you to enter either an IP address or a MAC address for the neighbor:

```
show ancp neighbor <brief | detail> <ip-address | system-name mac-address>
```

  In earlier releases, the CLI permitted you to use enter both an IP address and a MAC address to specify a neighbor.

- **Changes to show ancp subscriber and clear ancp subscriber commands (MX Series)**—Starting in Junos OS Release 16.1, multiple simultaneous filtering options are no longer allowed for the `show ancp neighbor`, `show ancp subscriber`, and `clear ancp subscriber` commands. In earlier releases, you can issue commands with both the `identifier` and `neighbor` options or both the `ip-address` and `system-name` options on the same line. Now you can enter only one of these options at a time.

  To improve consistency, the `neighbor` option has been replaced with `ip-address` for the `show ancp subscriber` command, to match the `show ancp neighbor`, `clear ancp neighbor`,
and clear ancp subscriber commands. For example, to display information about
subscribers connected to a specific access node identified by its address, use the show
ancp subscriber ip-address ip-address command; in earlier releases you use the show
ancp subscriber neighbor ip-address command.

The system-name mac-address option is now available for the show ancp subscriber
and clear ancp subscriber commands.

• Enhancements to test aaa statements for VLAN-OOB subscribers (MX
Series)—Starting in Junos OS Release 16.1, you can use the no-address-request
option with the test aaa dhcp user and test aaa ppp user statements for testing subscribers in
a Layer 2 scenario where no address allocation request is required.

The output of these two statements now displays two additional user attributes.
Dynamic Profile is the name of the profile received in the Client-Profile-Name VSA
(26-174). Routing Instance is the name of the routing instance conveyed by the
Virtual-Router VSA (26-1). The existing Virtual Router Name attribute is the locally
configured name of the logical system.

[See Testing a Subscriber AAA Configuration.]

• Subscriber secure policies and service change of authorization requests (MX
Series)—Starting in Junos OS Release 16.1, a subscriber secure policy cannot be
instantiated by a CoA that includes any other subscriber service activation or
deactivation. Use a separate CoA to apply a subscriber secure policy.

• Change to the show network-access aaa commands (MX Series)—Starting in Junos
OS Release 16.1, the outputs from the show network-access aaa statistics authentication
detail command and the show network-access aaa radius-servers detail command
have changed as follows:
  • The Accounting request timeouts field displayed by the show network-access aaa
    statistics authentication detail command has been renamed to Timed out requests.
  • The Round Trip Time field of the show network-access aaa radius-servers detail
    command has been renamed to Last Round Trip Time.

• Change to using the UID as part of a variable expression (MX Series)—Starting in
Junos OS Release 16.1, you cannot use the UID (the unique identifier of variables defined
in dynamic profiles) as part of a variable expression, because the hierarchy of evaluation
is as follows:
  • The user variable expressions are first evaluated for the UIDs to be resolved.
  • If the expression contains UIDs, it might result in unpredictable results.

Using a variable expression with a UID now results in a commit check failure.

• Subscriber management support for rpd in 64-bit mode (MX Series)—Starting in
Junos OS Release 16.1, subscriber management is now supported when the routing
protocol daemon (rpd) is running in 64-bit mode. In earlier releases, subscriber
management support required rpd to run in 32-bit mode.

• Extended range for RADIUS request rate (MX Series)—Starting in Junos OS Release
16.1, the range for the request-rate statement at the [edit access radius-options]
hierarchy level has been extended to 100 through 4000 requests per second. In earlier
releases, the range is 500 through 4000 requests per second. The default value is unchanged at 500 requests per second.

- **L2TP statistics now included in the output of the show system subscriber-management statistics command**—Starting in Junos OS Release 16.1, a new option displays the L2TP plugin statistics in the output of the `show system subscriber-management statistics` command.

The possible completions for the `show system subscriber-management statistics` command are:

- `<[Enter]>` executes this command
- `all`—Displays all statistics
- `dhcp`—Displays the DHCP statistics
- `dvlan`—Displays the DVLAN statistics
- `l2tp`—Displays the L2TP statistics
- `ppp`—Displays the PPP statistics
- `pppoe`—Displays the PPPoE statistics
- `/`—Pipes through a command

- **Error messages generated for L2TP access concentrator (LAC) logins can be prevented from appearing in the syslogs**—Starting with Junos OS Release 16.1, setting the syslogs log level to WARNING or higher prevents error messages generated for Layer 2 Tunneling Protocol (L2TP) subscribers from appearing in the syslogs. The syslogs are L2TP packet statistics counters (Rx/Tx) that are displayed every minute. If no packets are received or L2TP is not configured, these messages do not appear in the syslogs.

  In earlier releases, the severity of the log level was ERROR, which now has changed to NOTICE. The error messages are filtered out if the log level is set to WARNING or higher (ERROR, CRITICAL, ALERT, or EMERGENCY). Setting the log level to NOTICE or lower (INFORMATIONAL or DEBUG) allows the error messages to appear in the syslogs.

- **VLAN demux interfaces over pseudowire interfaces (MX Series)**—Starting in Junos OS Release 16.1, VLAN demux interfaces are supported over pseudowire subscriber logical interfaces.

- **Extended range for RADIUS request rate (MX Series)**—Starting in Junos OS Release 16.1, the range for the `request-rate` statement at the `edit access radius-options` hierarchy level has been extended to 100 through 4000 requests per second. In earlier releases, the range is 500 through 4000 requests per second. The default value is unchanged at 500 requests per second.

- **Automatic limit set for transmit window size (MX Series)**—Starting in Junos OS Release 16.1R2, when the LAC receives a receive window size of more than 128 in the Start-Control-Connection-Reply (SCCRP) message, it sets the transmit window size to 128 and logs an Error level syslog message.

  In earlier releases, the LAC accepts any value sent in the Receive Window Size attribute-value pair (AVP 10) from an L2TP peer. Some implementations send a receive
window size as large as 65530. Accepting such a large value causes issues in the L2TP congestion/flow control and slow start. The router may run out of buffers because it can support only up to a maximum of 60,000 tunnels.

System Logging

- **Support for system log message: UI_SKIP_SYNC_OTHER_RE (MX Series)**—Starting with Junos OS Release 16.1R1, configuration synchronization with a remote Routing Engine is skipped when the configuration is already in sync with another Routing Engine with database revision.

  **NOTE:** This system log message is generated when the graceful Routing Engine switchover feature is enabled.

  This system log message reports an event, not an error, and has notice as Severity and LOG_AUTH as Facility.

  [See Understanding Graceful Routing Engine Switchover in the Junos OS.]

System Management

- **Change to process health monitor process (MX Series)**—Starting in Junos OS Release 15.1R2, the process health monitor process (pmond) is enabled by default on the Routing Engines of MX Series routers, even if no service interfaces are configured. To disable the pmond process, include the **disable** statement at the [edit system processes process-monitor] hierarchy level.

  [See process-monitor.]

- **New option to suppress ARP response from kernel to non-subscribers**—Beginning with Junos OS Release 13.3R9, you can suppress the ARP response from the kernel when there is an ARP request for a loopback interface from non-subscribers. To drop ARP requests from non-subscribers, include the **non-subscriber-no-response** statement at the [edit system arp] hierarchy level.

  [See non-subscriber-no-response.]

User Interface and Configuration

- **New default implementation for serialization for JSON configuration data (MX Series and T Series)**—Starting with Junos OS Release 16.1, the default implementation for serialization for configuration data emitted in JavaScript Object Notation (JSON) has changed. The new default is as defined in Internet drafts draft-ietf-netmod-yang-json-09, *JSON Encoding of Data Modeled with YANG*, and draft-ietf-netmod-yang-metadata-06, *Defining and Using Metadata with YANG*.

  [See Mapping Junos OS Configuration Statements to JSON.]

- **output-file-name option for show system schema command is deprecated (MX Series and T Series)**—Starting with Junos OS Release 16.1, the **output-file-name** option for the **show system schema** operational command is deprecated. To direct the output to
a file, use the `output-directory` option and specify the directory. By default, the filename for the output file uses the module name as the filename base and the format as the filename extension. If you also include the `module-name` option in the command, the specified module name is used for both the name of the generated module and for the filename base for the output file.

[See show system schema.]}

**Related Documentation**

- New and Changed Features on page 53
- Known Behavior on page 121
- Known Issues on page 124
- Resolved Issues on page 129
- Documentation Updates on page 132
- Migration, Upgrade, and Downgrade Instructions on page 134
- Product Compatibility on page 142

**Known Behavior**

This section contains the known behavior, system maximums, and limitations in hardware and software in Junos OS Release 16.1R1 for 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.

- Bridging and Learning on page 121
- General Routing on page 121
- MPLS on page 122
- Routing Protocols on page 122
- Software Installation and Upgrade on page 122
- Subscriber Management and Services on page 122
- System Logging on page 123
- VPNs on page 123

**Bridging and Learning**

- **Clearing bridge statistics in PBB-EVPN**—Junos OS does not support clearing of bridge statistics for provider backbone bridging EVPN (PBB-EVPN).

**General Routing**

- The date and time zones are synchronized from the admin guest Junos OS to host OS on the MX240, MX480, MX960, MX2010, and MX2020 routers and use same time zones. Therefore, there is no difference in the timestamp in system log files of Junos OS and the host OS.
The temperature conditions of the Routing Engine FRU for RE-MX-X8 are now displayed correctly. The show chassis zones command now displays the accurate temperature conditions.

**MPLS**

- **Removal of SRLG details from the SRLG table only on the next reoptimization of the LSP**—If an SRLG is associated with a link used by an ingress LSP in the router, then on deleting the SRLG configuration from that router, the SRLG gets removed from the SRLG table only on the next reoptimization of the LSP. Until then, the output displays Unknown-XXX instead of the SRLG name and a nonzero srlg-cost of that SRLG for the run show mpls srlg command.

- The configuration flow-label-transmit and flow-label-receive statements are not supported in OAM CFM session over L2Circuit.

**Routing Protocols**

- **BGP advertises inactive routes when advertise-inactive statement is not configured**—When BGP advertises a network layer reachability information (NLRI) with a label, and the advertised route resides in xxx.xxx.3 routing table such as inet.3, Junos OS automatically advertises such inactive routes even if you have not configured the advertise-inactive statement.

**Software Installation and Upgrade**

- **Option upgrade-with-config Accepts Only Configuration Files with Extension .text or .xml (MX Series and T Series)**—In the request system software add command, the upgrade-with-config option does not apply the configuration if the configuration file has the extension .txt. This option accepts only files with the extension .text or .xml.

**Subscriber Management and Services**

- On MX Series routers, when you configure the subscriber-awareness statement on a service set by committing the set services service-set service-set-name service-set-options subscriber-awareness statement, the service sessions fail to create. To avoid this issue, on MX Series routers that support the Service Control Gateway solution, ensure that the Junos OS Mobility package software is installed on the router.

  The Service Control Gateway solution is supported only in 14.1X55 releases. For Junos OS Releases 14.2, 15.1, and 16.1, ensure that the subscriber-awareness statement is not set.

- **Enhanced subscriber management performance and scale (MX Series)**—Starting in Junos OS Release 16.1, subscriber management supports a denser subscriber scale per platform, per line card, and per port. It also provides improved performance of call setup rates. These enhancements are available through a software upgrade, which retains feature parity with existing broadband edge implementations, except as noted for “enhanced subscriber management” in these release notes. New hardware is not required.
The increased scale and faster setup rates apply to PPP client scaling, PPP LAC sessions, LAC and termination and aggregation (PTA) combinations, and PPP client scaling over LNS on the PPP interface for IPv4, IPv6, and concurrent sessions. It also applies to DHCP client scaling stateless address autoconfiguration (SLAAC), IPv6 over Ethernet, and DHCPv4 clients.

- **Dynamic provisioning in Layer 2 wholesaling (MX Series)**—Starting with Release 15.1R3, Junos OS does not support dynamic VLAN mapping into VPLS instances. (You can still configure static VLAN interface mapping to VPLS instances.) By extension, dynamic provisioning for Layer 2 wholesaling is also not supported in this release.

  The following example shows the statements that are not currently available
  (encapsulation vlan-vpls and family vpls at the [edit dynamic interfaces] hierarchy level):

  ```
  interfaces {
    "$junos-interface-ifd-name" {
      unit "$junos-interface-unit" {
        encapsulation vlan-vpls
        vlan-id "$junos-vlan-id";
        family vpls;
      }
    }
  }
  ```

**System Logging**

- On MX Series routers, when you configure a rate limit for system log messages by setting the **message-rate-limit** statement for a multiservices interface, ensure that the **syslog host** option for that interface is configured. This configuration ensures that the system log statistics reflect the rate limit set for the interface.

**VPNs**

- **Traffic stops flowing when different VLAN IDs are configured**
  (PBB-EVPN)—PBB-EVPN does not support different VLAN IDs under I-Component BDs that are extended into different PEs. Packets will not forward properly unless all of the PE VLAN IDs in the extended I-Component have the same value.

**Related Documentation**

- New and Changed Features on page 53
- Changes in Behavior and Syntax on page 107
- Known Issues on page 124
- Resolved Issues on page 129
- Documentation Updates on page 132
- Migration, Upgrade, and Downgrade Instructions on page 134
- Product Compatibility on page 142
Known Issues

This section lists the known issues in hardware and software in Junos OS Release 16.1R1 for 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 on page 125
- General Routing on page 125
- Interfaces and Chassis on page 126
- Layer 2 Features on page 127
- MPLS on page 127
- Platform and Infrastructure on page 127
- Provider Edge Satellite Software on page 128
- Routing Protocols on page 128
- Services Applications on page 128
- Software Installation and Upgrade on page 129
- VPNs on page 129
Forwarding and Sampling

- It is known that policing filter application to the LSP is catastrophic. Any active LSP carrying traffic when applied a policing filter will tear down and resignal and drop traffic for ~2 seconds. In 16.1R1 it would take up to 30 seconds for the LSP to come up if 1. Creation of the policing filter and application of the same to the LSP via config in the same commit sequence 2. Load override of a config file that has policing filter and policing filter application to the LSP followed by commit. The plan is to rectify this behavior in 16.2. PR1160669

General Routing

- EVPN uses several different subtypes of routes within the EVPN address family which are advertised through the control plane between PEs using BGP. Multihoming PEs use Ethernet segment (ES) routes to advertise the fact that the PEs are connected to a given multihomed segment. All other multihoming PEs attached to the same multihomed segment import those ES routes, and combined with their own local state, elect a single designated forwarder (DF) for each EVPN instance that is part of the multihomed segment. When a new PE is added to an existing EVPN, the new PE needs to download the full set of EVPN routes advertised by the other existing PEs. In cases of high MAC scaling, it is possible that remote PEs will generate and send BGP updates for MAC routes (or other EVPN route types) before generating and sending the ES routes. If the time taken by the original multihoming PE(s) to send the ES routes is longer than the DF election hold timer on the new PE, the new PE and an existing multihoming PE may both consider themselves to be the DF for the same EVPN ES simultaneously. In this situation, broadcast traffic could be flooded by both PEs. Additionally, in the case of single-active multihoming, transient/spurious MAC moves could happen between the two PEs both considering themselves to be the DF, causing unnecessary BGP update churn and slowing convergence. PR968428

- The L2ald may crash after interface flap. PR1015297

- On XL-based cards such as MPC5/MPC6, PPE thread timeout errors (resulting in PPE trap files) can be triggered when the FPC allocates illegal memory space for the forwarding state of router operations. In certain cases, this can result in packet loss, depending on how many packets use this forwarding state. PR1100357

- In case of IPsec if the member interface say mams-x/y/z is part of ams bundle in one-to-one mode. The same numbered ms-x/y/z interface should not be used for IPsec or any other services. PR1134645

- When successive back-to-back commits are performed on a scaled configuration, there could be a timeout or a delay in completing the commit check operation. PR1139206

- The ICMP time exceeded error packet is not generated on an IPsec router on the decap side. The problem is fixed for MS-MPC/MIC and works fine if the session is there. There is no other way to return the time exceeded message over a tunnel. There is no plan to fix this for MS-DPC. PR1163472
• Despite MX240/MX480/MX960 being configured with the network analytics feature, the analytics daemon might not run. As a result, the network analytics feature might be unable to collect traffic and queue statistics and generate reports. PR1165768

• A micro BFD session sourced from an interface’s L3 address works even when the interface is not assigned the related UBFD address. PR1180109

• Chef for Junos OS supports additional resources to enable easier configuration of networking devices. These are available in the form of netdev-resources. The netdev-resource developed for interface configuration has a limitation to configure XE interface. Netdev-interface resource assumes that 'speed' is a configurable parameter which is supported on a GE interface but not on an XE interface. Hence netdev-interface resource cannot be used to configure an XE interface due to this limitation. This limitation is applicable to packages chef-11.10.4.1.1.*.tgz chef-11.10.4.2.0_*.tgz in all platforms {i386/x86-32/powerpc}. PR1181475

• Syslog error "rt_nh_topo_handler: Rcvd NH delete before RT delete" might be seen for some IPv6 configurations which can be ignored. This does not cause any traffic loss or other undesirable behaviors. PR1184561

• During the unified ISSU from 15.1 (or previous release) to 16.1R1 on TX platform, Packet Forwarding Engines will get rebooted. This might cause traffic loss during unified ISSU. PR1194032

• Line card is crashed while doing internal testing. Line card is busy looping/not yielding to other threads so chassisD sent an NMI and crashed the line card. This is observed only once and unable to reproduce. PR1194692

• PTP support MPC2E-NG and MPC3E-NG is not working in 16.1R1 release. Issue came because incorrect branch sync removing support checks for these MPCs. There is no workaround for this. PR1194734

• When ldp is deactivated, there may still be route entries left in the ldp shadow routing table. RPD will core due to stranded route entries in the ldp routing table. PR1196405

• In a L3VPN setup, telnet to CE via ae intf may cause "ls -ltr /etc" to be stuck. PR1198825

• On executing "show task replication" command, IS-IS could be shown as "Complete" if IS-IS is not configured on the device. If IS-IS is configured, the replication will be shown correctly (NotStarted/InProgress/Complete). No other functionality impacted. PR1199596

**Interfaces and Chassis**

• In a VPLS scenario the flood NH for the default mesh group might not be programmed properly. A complete black-holing for the VPLS instance would be seen as a consequence. PR1166960

• CFM enhanced-iterator functionality will be affected with scale if "deactivate protocol oam" is done with working configurations. The workaround is to do the following steps in the given order 1. "deactivate protocols oam ethernet connectivity-fault-management performance-monitoring enhanced-sla-iterator" 2. "deactivate protocol oam" On following the above order of commit the problem will not be seen. PR1185842
• During configuration changes and reuse of Virtual IP on an interface as a interface address; It is required to delete the configuration do a commit and then add the interface address configuration in the following commit. PR1191371

Layer 2 Features

• When a CFM down-mep is configured on a STP-blocked interface which is housed on a DPCE card, flooding of traffic in the local L2 broadcast network might happen, leading to side-effects such as flapping of OSPF sessions, BFD sessions, or similar. PR1174175

MPLS

• User is allowed to configure both "load-balance-label-capability" and "no-load-balance-label-capability" together. This is incorrect and confusing. PR1126439

• When configuring CCC remote-interface switch or LSP-switch, self-ping should be disabled on the LSPs, referred-to in the CCC configuration, by configuring the following: [edit protocols mpls label-switched-path lsp1] + no-self-ping; Not doing the above, would cause the LSPs to not complete MBB (make before break). PR1181407

• When RSVP LSPs are signaled with loose hops in their explicit path (or no explicit path at all), then the new default RSVP refresh interval of 20 minutes may sometimes interfere with reacting to route changes in the network. A Junos OS LSP ingress router will signal loose hops when configured with an explicit path that contains loose hops and when also configured with the "no-cspf" option for the LSP. PR1186210

• With ldp egress protection in stub-alias mode, traffic loss occurs when the interface between the protector egress node and the primary egress node goes down. PR1190983

Platform and Infrastructure

• On T Series platform, when reloading the chassis which has SONET Clock Generators (SCGs) equipped, due to the timing issue (the issue may not be consistently observed), "No CG online" RED alarm might be displayed on the LCD panel and not cleared while in fact the SCGs are coming up later and this alarm should be cleared. PR991533

• In configurations with IRB interfaces, during times of interface deletion, such as an FPC reboot, the Packet Forwarding Engine may log errors stating "nh_uCAST_change:291Referenced I2ifl not found". This condition should be transient, with the system re-converging on the expected state. PR1054798

• In software versions which contain PR 1136360's code changes on MX-VC systems, when JFLOW is not configured and equal-cost multipath (ECMP) load-balanced routes occur, the linecards may stop forwarding packets after logging any of the below errors prior to possible linecard restart or offline: - PPE Thread Timeout Traps - PPE Sync XTXN Err Trap - Uninitialized EDMEM Read Error - LUCHIP FATAL ERROR - pio_read_u64() failed (A possible workaround is to configure JFLOW and restart all linecards.) In software versions which do not contain PR 1136360 solution, on MX Series Virtual Chassis (MX-VC) with "virtual-chassis locality-bias" configured, when equal-cost multipath (ECMP) load-balancing is occurring in the VC system, multicast streams and flooded Layer 2 streams may be duplicated or lost. Disabling "virtual-chassis locality-bias" from the configuration will eliminate the problem. PR1104096
Provider Edge Satellite Software

- When Multicast traffic is forwarding in the satellite local-replication mode (configured with the "forwarding-options satellite local-replication" configuration), the following commands, configuration changes, and hardware events may result in Multicast traffic being dropped for some receivers connected to satellite devices: 1. Restarting the Satellite Platform Management Daemon (SPMD), or Satellite Discovery Provisioning Daemon (SDPD) by issuing the following commands: "restart satellite-platform-management-process", "restart satellite-platform-management-process gracefully", "restart satellite-discovery-provisioning-process", or "restart satellite-discovery-provisioning-process gracefully". 2. Unprovisioning then reprovisioning selected satellite devices by deleting or deactivating, then re-adding or reactivating the following configuration: "chassissatellite-managementfpc<slotid>", while Multicast traffic is forwarding to these satellite devices. 3. A hardware failure that results in specific satellite devices that are forwarding Multicast traffic to be brought down, then up. PR1139592

Routing Protocols

- Symptoms: With NSR enabled, rpdmay core on standby Routing Engine when operations like RD modify or RD delete/RD operations are done. (Not always observed). Impact: There is no impact on traffic or other functionality. The core occurs only once on the standby Routing Engine. Standby Routing Engine recovers completely, with all replication done fully post core. PR1162665

- A route which has an IPv6 next hop which is resolved recursively over other routes may fail to resolve successfully. This problem could happen because the route resolver may incorrectly use the IPv4 family resolution tree to resolve the nexthop rather than the correct IPv6 resolution tree. As a result no route covering the IPv6 nexthop address can be located so the route with the IPv6 nexthop remains unresolved and unusable. PR1192591

Services Applications

- When polling to jnxNatSrcNumPortInuse via SNMP MIB get, it might not be displayed correctly. PR1100696

- In Junos OS Release 13.3 and later, when configuring a /31 subnet address under a NAT pool, the adaptive services daemon (SPD) will continuously crash. PR1103237
Software Installation and Upgrade

- Due to increasing in software requirement and hardware limitation of older hardware; USB installation image may not work correctly in platforms with RE-A-2000, RE-S-2000, or their variants. The result of using USB install image with these routing engine is for the routing engine to be in a boot loop. PR1196232

VPNs

- In the l2circuit environment, when l2ckt configuration has backup-neighbor, the flow-label operation is blocked at the configuration level. PR1056777

Related Documentation

- New and Changed Features on page 53
- Changes in Behavior and Syntax on page 107
- Known Behavior on page 121
- Resolved Issues on page 129
- Documentation Updates on page 132
- Migration, Upgrade, and Downgrade Instructions on page 134
- Product Compatibility on page 142

Resolved Issues

This section lists the issues fixed in the Junos OS main release and the maintenance releases 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.

- Resolved Issues: 16.1R1 on page 129

Resolved Issues: 16.1R1

- Forwarding and Sampling on page 129
- General Routing on page 130
- Interfaces and Chassis on page 131
- MPLS on page 131
- Platform and Infrastructure on page 131
- Routing Protocols on page 131

Forwarding and Sampling

- If bandwidth-percent based policer is applied on aggregated Ethernet (AE) bundle without the "shared-bandwidth-policer" configuration statement, traffic will hit policer even if the traffic is not exceeding the configured bandwidth. As a workaround, configure the "shared-bandwidth-policer" configuration statement under the policer. PR1125071
- SRRD daemon does not delete routes when the DELETE is received from RPD in few configuration cases. This results in build-up of memory in SRRD daemon and once SRRD reaches the limit, it crashes and restarts itself. This happens only when none of the SRRD clients (FPCs in Inline JFlow case and PICs in PIC based sampling) are interested in one or more families. Say, only IPv4 family is configured in all the clients and, IPv6 and MPLS families are not configured for sampling in any of the clients. PR1180158

**General Routing**

- On MX Series routers with MPC3E, MPC4E, MPC5E, MPC6E, Junos OS does not support short (sub-second) interface hold-time down configuration. A hidden configuration statement is introduced to ignore DFE tuning state during hold-down timer period. This configuration statement allows sub-second hold-down timer on MPC3E, MPC4E, MPC5E, MPC6E. Set interfaces <int name> hold-time up <U ms> down <D ms> alternative. The configuration statement does not work/support 'MPC5E 3D Q 2CGE+4XGE' and 'MIC6 2X100GE CFP2 OTN', and we recommend configuring hold-time down to be more than 3 seconds for these two cards. PR1012365

- During initial ramp-up of a IPsec session, a race condition could crash mspmand in rare circumstances. PR1116487

- On MX Series routers containing multiple Packet Forwarding Engines such as MX240/MX480/MX960/MX2010/MX2020, with MPC3E/MPC4E/MPC5E/MPC6E cards, if the routers have GRE decap, then certain packet sizes coming via these line cards, at very high rate can cause these line cards to exhibit a lockup, and one or more of their Packet Forwarding Engines corrupt traffic toward the router fabric. PR1117665

- On dual Routing Engine MX Series platforms, the "xe" interfaces of any of the line cards below may flap during in-service software upgrade (ISSU) due to missing support. The flapping may not happen every time and the probability of occurrence would increase if more number of SFP+ (e.g., SFP+-10G-SR) are connected on the FPC. The affected line cards are: * MIC3-3D-10XGE-SFP * MPC4E-3D-32XGE-SFP * MPC4E-3D-2CGE-8XGE * MPC5E-40G10G, MPC5EQ-40G10G * MX2K-MIC6-24XE, MX2K-MIC6-24XE-OTN. PR1118379

- On MX Series platforms, the MS-MPC crash might occur. The exact trigger of the issue is unknown; normally, this issue might happen over long hours (e.g., within a week) of traffic run (e.g., running HTTP/HTTPS/DNS/RTSP/TPF/FTP traffic profile). PR1124466

- In a IGMP oversubscriber environment with the configuration statement "remove-when-no-subscribers" configured, after performing graceful Routing Engine switchover, subscribers with multicast joins cannot re-login when the subscriber logs out before it sends an IGMP leave in the new master. PR1136646

- With Junos OS Release 15.1 and later, on MS-MPC or MS-PIC, OSPF adjacency may fail to establish when there is no static route pointing to service PIC. PR1164517

- When upgrading Junos software on REI, if at the time, REI is the "master RE", both Routing Engines will be in "backup" state. Resulting in losing remote connectivity, and all interfaces. Only "console" access will be available at this time. PR1172729
• ICMP pings destined to VRRP VIP address beyond 166 bytes are dropped as "my-mac check failed" on MPC7E/8E/9E. PR1186537

• On MX Series router, while using routing-instance for EVPN, and traceoptions is configured under global "protocols evpn", configuration of "vtep-source-interface" under global "switch-options" would be rejected. PR1189235

**Interfaces and Chassis**

• Chap Local-name defaults to 8 characters. Should be 32. PR996760

**MPLS**

• When OSPF LFA is enabled and there is an available backup path, after clearing the LDP session to the primary path or backup path, in a very rare condition, the LDP session on this router might flap multiple times. PR1119700

**Platform and Infrastructure**

• When a common scheduler is shared by multiple scheduler maps which applies to different VLANs of an aggregated Ethernet (AE) interface, if the configuration statement "member-link-scheduler" is configured at "scale", for some VLANs, the scheduler parameters are wrongly scaled among AE member links. As a workaround, we should explicitly configure different schedulers under the scheduler maps. PR11107013

• We have observed that on 32 bit images with scaled configuration, route-table memory is used more leading to veto logic. It is suggested to use 64 bit images for scaled configurations. PR1179029

**Routing Protocols**

• On the RSVP LSP scenario with IS-IS configured, memory leak might happen in rpd and Packet Forwarding Engine after the LSP re-optimization, and this might cause FPC crash. PR1187395

• During the testing of 16.1B1, a customer found rpd coring during BGP flow routes updates. This PR has now been fixed in the June 15th build of 16.1, and also in 16.1R1. PR1188502

• During 16.1B1 testing a customer has reported that while receiving certain combinations of BGP flow routes that they experience an rpd core. This issue is fixed in 16.1R1. PR1192875

**Related Documentation**

- New and Changed Features on page 53
- Changes in Behavior and Syntax on page 107
- Known Behavior on page 121
- Known Issues on page 124
- Documentation Updates on page 132
- Migration, Upgrade, and Downgrade Instructions on page 134
- Product Compatibility on page 142
Documentation Updates

This section lists the errata and changes in Junos OS Release 16.1R1 documentation for MX Series and T Series.

- **NETCONF XML Management Protocol Developer Guide on page 132**
- **Security Services Administration Guide on page 132**
- **SNMP MIBS and traps reference on page 133**
- **Syslog Reference Guide on page 133**
- **Standards Reference on page 133**
- **Subscriber Management Provisioning Guide on page 133**

**NETCONF XML Management Protocol Developer Guide**

- The **NETCONF XML Management Protocol Developer Guide** incorrectly states that you can load custom YANG modules and action scripts on devices running Junos OS to augment the operational command hierarchy with non-native YANG RPCs. Junos OS does not support loading custom RPCs on devices running Junos OS.

**Security Services Administration Guide**

- The “Distributed Denial-of-Service (DDoS) Protection Overview” topic has been updated to describe the built-in login overload protection mechanism that is available on MX Series routers.

  The login overload protection mechanism (also called a load-throttling mechanism) monitors the incoming subscriber login packets and admits only what the system is capable of handling in accordance with the prevailing load on the system. Packets in excess of what the system can handle are discarded. By shedding this excess load, the system is able to maintain optimal performance and prevent any degradation of login-completion rate under overload conditions. This mechanism uses minimal resources and is enabled by default; no user configuration is required.

  The protection provided by this mechanism is secondary to what distributed denial-of-service (DDoS) protection provides as a first level of defense against high rates of incoming packets. DDoS protection operates on the Packet Forwarding Engine and protects against all packet types of all protocols. In contrast, the login overload protection mechanism is located on the Routing Engine and specifically operates only on incoming connection-initiation packets such as DHCPv4 DHCPDISCOVER, DHCPv6 SOLICIT, and PPPoE PADI packets.

- The “protocols (DDoS)” and “show ddom-protection protocols” topics have been updated to report changes in syntax for the MLP protocol group. The `aging-exc`, `packets`, and `vxlans` packet types have been removed from the MLP protocol group. The `add`, `delete`, and `lookup` packet types have been added to the MLP protocol group. The `keapalve` protocol group has been renamed to `tunnel-ka`. The `firewall-host` protocol group and the `mcast-copy` packet type in the `unclassified` protocol groups have been removed from the CLI. Additionally, in the “show ddom-protection protocols” topic, the description for the global, Routing Engine, and FPC policer states have been expanded and clarified.
The “DDoS Protection Flow Detection Overview” and “Enabling Flow Detection for All Protocol Groups and Packet Types” topics now include a note about protocol groups and a packet type for which you cannot globally enable flow detection.

### SNMP MIBS and traps reference

- **SNMP MIBs and Traps Reference deprecation**—Starting in Junos OS Release 16.1, the SNMP MIBs and Traps Reference has been deprecated. To access information about SNMP MIB objects, tables, and notifications, use the SNMP MIB Explorer. For an overview of the MIBS supported on Junos OS, see the [Network Management Administration Guide](#).

### Syslog Reference Guide

- **System Log Messages Reference deprecation**—Starting in Junos OS Release 16.1, the System Log Messages Reference has been deprecated. To access information about system log messages, use the System Log Explorer or continue to use the CLI by executing the `help syslog <tag>` command, where the `tag` is the unique identifier of the error message. For an overview of system log messages, see [System Log Messages Configuration Guide](#).

### Standards Reference

- The [Supported Network Management Standards](#) topic incorrectly states that Junos OS supports mplsL3vpnIfConfTable as part of compliance with RFC 4382, *MPLS/BGP Layer 3 Virtual Private Network (VPN) MIB*. Junos OS does not support this table.

### Subscriber Management Provisioning Guide

The following topics indicate that you can configure an MX Series router to maintain a DHCP subscriber in the event the subscriber interface is deleted:

- “Subscriber Binding Retention During Interface Delete Events”
- “Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events”
- “Verifying and Managing the DHCP Maintain Subscribers Feature”
- “interface-delete (Subscriber Management or DHCP Client Management)”
- “maintain-subscriber”
- “subscriber-management (Subscriber Management)”

This feature is not supported on MX Series routers running Junos OS Release 15.1R4 or later with enhanced subscriber management enabled.

### Related Documentation

- New and Changed Features on page 53
- Changes in Behavior and Syntax on page 107
- Known Behavior on page 121
- Known Issues on page 124
- Resolved Issues on page 129
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 MX Series and T Series. Upgrading or downgrading Junos OS can take several minutes, depending on the size and configuration of the network.

Starting with Junos OS Release 15.1, in some of the devices, FreeBSD 10.x is the underlying OS for Junos OS instead of FreeBSD 6.1. This feature includes a simplified package naming system that drops the domestic and world-wide naming convention. However, in some of the routers, FreeBSD 6.1 remains the underlying OS for Junos OS. For more details about FreeBSD 10.x, see Understanding Junos OS with Upgraded FreeBSD.

NOTE: In Junos OS Release 15.1, Junos OS (FreeBSD 10.x) is not available to customers in Belarus, Kazakhstan, and Russia. Customers in these countries need to use the existing Junos OS (FreeBSD 6.1).

The following table shows detailed information about which Junos OS can be used on which products:

<table>
<thead>
<tr>
<th>Platform</th>
<th>FreeBSD 6.1-based Junos OS</th>
<th>FreeBSD 10.x-based Junos OS</th>
</tr>
</thead>
<tbody>
<tr>
<td>MX80, MX104</td>
<td>YES</td>
<td>NO</td>
</tr>
<tr>
<td>MX240, MX480, MX960, MX2010, MX2020</td>
<td>NO</td>
<td>YES</td>
</tr>
</tbody>
</table>

- Basic Procedure for Upgrading to Release 16.1 on page 134
- Upgrading from Junos OS (FreeBSD 6.1) to Junos OS (FreeBSD 10.x) on page 136
- Upgrading from Junos OS (FreeBSD 6.1) to Junos OS (FreeBSD 6.1) on page 137
- Upgrade and Downgrade Support Policy for Junos OS Releases on page 139
- Upgrading a Router with Redundant Routing Engines on page 139
- Upgrading Juniper Network Routers Running Draft-Rosen Multicast VPN to Junos OS Release 10.1 on page 140
- Downgrading from Release 16.1 on page 141

Basic Procedure for Upgrading to Release 16.1

When upgrading or downgrading Junos OS, always use the jinstall package. Use other packages (such as the jbundle package) only when so instructed by a Juniper Networks support representative. For information about the contents of the jinstall package and details of the installation process, see the Installation and Upgrade Guide and Upgrading Junos OS with Upgraded FreeBSD.
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 reinstall
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.
Upgrading from Junos OS (FreeBSD 6.1) to Junos OS (FreeBSD 10.x)


NOTE: This section does not apply to customers in Belarus, Kazakhstan, and Russia. Customers in these countries need to refer to the next section.

To download and install from Junos OS (FreeBSD 6.1) to Junos OS (FreeBSD 10.x):

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 a Juniper Networks representative.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

10. Install the new jinstall package on the routing platform.

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

- For 32-bit Routing Engine version:

  `user@host> request system software add no-validate reboot source/junos-install-mx-x86-32-16.1R1.9-signed.tgz`

- For 64-bit Routing Engine version:

  `user@host> request system software add no-validate reboot source/junos-install-mx-x86-64-16.1R1.9-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)

Do not use the validate option while upgrading from Junos OS (FreeBSD 6.1) to Junos OS (FreeBSD 10.x). This is because programs in the junos-upgrade-x package are built based on FreeBSD 10.x, and Junos OS (FreeBSD 6.1) would not be able to run these programs. You must run the no-validate option. The no-validate statement disables the validation procedure and allows you to use an import policy instead.

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

Rebooting occurs only if the upgrade is successful.

NOTE: You need to install the Junos OS software package and host software package on the routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. For upgrading the host OS on these routers with VM Host support use the junos-vmhost-install-x.tgz image and specify the name of the regular package in the request vmhost software add command. For more information see VM Host Installation topic in the Installation and Upgrade Guide.

NOTE: After you install a Junos OS Release 16.1 jinstall package, you cannot issue the request system software rollback command to return to the previously installed Junos OS (FreeBSD 6.1) software. Instead, you must issue the request system software add no-validate command and specify the jinstall package that corresponds to the previously installed software.

NOTE: A few of the existing request system commands are not supported on routers with the RE-MX-X6 and RE-MX-X8 Routing Engines. See the VM Host Software Administrative Commands in the Installation and Upgrade Guide.

Upgrading from Junos OS (FreeBSD 6.1) to Junos OS (FreeBSD 6.1)

Products impacted: All T Series routers, MX80, and MX104.

NOTE: Customers in Belarus, Kazakhstan, and Russia must use the following procedure for all MX Series routers running Junos OS Release 16.1

To download and install from Junos OS (FreeBSD 6.1) to Junos OS (FreeBSD 6.1):
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 a Juniper Networks representative.

7. Review and accept the End User License Agreement.

8. Download the software to a local host.

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

10. Install the new jinstall package on the routing platform.

   ![NOTE](https://via.placeholder.com/150)

   **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-16.1R1.9-domestic-signed.tgz
     ```

   - All other customers, use the following command:
     
     ```
     user@host> request system software add validate reboot source/jinstall-16.1R1.9-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.

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

Rebooting occurs only if the upgrade is successful.

**NOTE:** After you install a Junos OS Release 16.1 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 11.4, 12.3, and 13.3 are EEOL releases. You can upgrade from Junos OS Release 11.4 to Release 12.3 or even from Junos OS Release 11.4 to Release 13.3. 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 12.1 (a non-EEOL release) to Junos OS Release 13.3 or directly downgrade from Junos OS Release 13.3 to Junos OS Release 12.1.

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](http://www.juniper.net/support/eol/junos.html).

---

**Upgrading a Router with Redundant Routing Engines**

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

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

2. Install the new Junos OS release on the backup Routing Engine while keeping the currently running software version on the master Routing Engine.
3. After making sure that the new software version is running correctly on the backup Routing Engine, switch over to the backup Routing Engine to activate the new software.

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

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

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 address 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.

Downgrading from Release 16.1

To downgrade from Release 16.1 to another supported release, follow the procedure for upgrading, but replace the 16.1 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.

Related Documentation

• New and Changed Features on page 53
• Changes in Behavior and Syntax on page 107
• Known Behavior on page 121
• Known Issues on page 124
• Resolved Issues on page 129
• Documentation Updates on page 132
• Product Compatibility on page 142
Product Compatibility

- Hardware Compatibility on page 142

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 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/

Hardware Compatibility Tool

For a hardware compatibility matrix for optical interfaces and transceivers supported across all platforms, see the Hardware Compatibility tool.

Related Documentation

- New and Changed Features on page 53
- Changes in Behavior and Syntax on page 107
- Known Behavior on page 121
- Known Issues on page 124
- Resolved Issues on page 129
- Documentation Updates on page 132
- Migration, Upgrade, and Downgrade Instructions on page 134
Junos OS Release Notes for PTX Series Packet Transport Routers

These release notes accompany Junos OS Release 16.1R1 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 on page 143
- Changes in Behavior and Syntax on page 151
- Known Behavior on page 154
- Known Issues on page 155
- Documentation Updates on page 156
- Resolved Issues on page 157
- Migration, Upgrade, and Downgrade Instructions on page 157
- Product Compatibility on page 161

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 16.1R1 for the PTX Series.

- Hardware on page 143
- Class of Service (CoS) on page 145
- Forwarding and Sampling on page 145
- General Routing on page 145
- Junos OS XML API and Scripting on page 146
- Management on page 146
- MPLS on page 146
- Network Management and Monitoring on page 149
- Routing Protocols on page 150
- User Interface and Configuration on page 151
- VPNs on page 151

Hardware

- **New Routing Engine RE-PTX-X8-64G (PTX5000)**—Starting in Junos OS Release 16.1, the Routing Engine RE-PTX-X8-64G is supported on PTX5000 routers. This Routing Engine has an increased computing capability and scalability to support the rapid rise in the data plane capacity. The Routing Engine is based on a modular virtualized architecture and leverages the hardware-assisted virtualization capabilities.
The Routing Engine has a 64-bit CPU and supports a 64-bit kernel and 64-bit applications. With its multicore capabilities, the Routing Engine supports symmetric multiprocessing in the Junos OS kernel and hosted applications.

**NOTE:** The Routing Engine RE-PTX-X8-64G is supported only on the new Control Board CB2-PTX.

- **New Control Board support (PTX5000)**—Starting with Release 16.1, Junos OS supports the Routing Engine RE-PTX-X8-64G with an enhanced Control Board (CB) on PTX5000 routers. The CB supports chassis management and 16 additional 10-Gigabit Ethernet ports with small form-factor pluggable plus (SFP+) transceivers on the front panel of the router to support multichassis applications.

  The enhanced CB consists of the following components:
  - Ethernet switch used for intermodule communication
  - PCI Express bus to connect to the Routing Engine
  - PCI Express switch to connect to the SIBs
  - Switch Processor Mezzanine Board (SPMB)

- **High capacity single-phase AC PDU (PTX5000)**—In Junos OS Release 16.1, a single-phase AC power distribution unit (PDU)—PDU2-PTX-AC-SP—is introduced to provide power to the PTX5000 chassis. The PDU provides a single-phase AC input connection from the customer's AC source, an I/O interface to the power supply modules (PSMs), and a DC power connection to the system midplane. The PDU is powered by either eight 30-A or eight 20-A single-phase sources. Each of the eight PSMs connected to the AC PDU receives single-phase input.
Class of Service (CoS)

- **Support for shaping of the traffic exiting a physical interface (PTX Series)**—Beginning with Junos OS Release 16.1R1, you can shape the output traffic of an FPC1 or FPC2 physical interface on a PTX Series packet transport router so that the interface transmits less traffic than it is physically capable of carrying. Shaping on a PTX Series packet transport has a minimum rate of 1 Gbps and an incremental granularity of 0.1 percent of the physical interface speed after that (for example, 10 Mbps increments on a 10 Gbps interface). You can shape the output traffic of a physical interface by including the `shaping-rate` statement at the [edit class-of-service interfaces interface-name] or [edit class-of-service traffic-control-profiles profile-name] hierarchy level and applying the traffic control profile to an interface.

  [See shaping-rate (Applying to an Interface).]

Forwarding and Sampling

- **Support for Bidirectional Forwarding Detection (BFD)**—Starting in Junos OS Release 16.1R2, support is extended for Bidirectional Forwarding Detection (BFD). The BFD protocol uses control packets and shorter detection time limits to rapidly detect failures in a network. Hello packets are sent at a specified, regular interval by routing devices. A neighbor failure is detected when a routing device stops receiving a reply after a specified interval.

  On a PTX1000 router, you can configure BFD for static routes and for the BGP, IS-IS, OSPF, PIM, and RIP protocols.

General Routing

- **Support for virtualization on RE-PTX-X8-64G (PTX5000)**—Starting with Junos OS Release 15.1F3 the Routing Engine RE-PTX-X8-64G for PTX5000 supports virtualization.

  Virtualization enables the router to support multiple instances of Junos OS and other operating systems on the same Routing Engine. However, for Junos OS Release 15.1F3, one instance of Junos OS, which runs as a guest operating system, is launched by default. The user needs to log in to this instance for operations and management. For information see, `RE-MX-X6, RE-MX-X8, and RE-PTX-X8 with VM Host Support`.

  With virtualization of the Routing Engine, Junos OS supports new `request` and `show` commands associated with host and hypervisor processes. The commands are related to:

  - Reboot, halt, and power management for the host
  - Software upgrade for the host
• Disk snapshot for the host

Junos OS XML API and Scripting

• Support for Python language for commit, event, op, and SNMP scripts (PTX Series)—Starting in Junos OS Release 16.1, you can author commit, event, op, and SNMP scripts in Python on devices that include the Python extensions package in the software image. Creating automation scripts in Python enables you to take advantage of Python features and libraries, as well as leverage Junos PyEZ APIs supported in Junos PyEZ Release 1.3.1 and earlier releases, to perform operational and configuration tasks on devices running Junos OS. To enable execution of Python automation scripts, which the root user must own, configure the language python statement at the [edit system scripts] hierarchy level, and configure the filename for the Python script under the hierarchy level appropriate to that script type. Supported Python versions include Python 2.7.x.

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

Management

• YANG module that defines CLI formatting for RPC output (PTX Series)—Starting with Junos OS Release 16.1, Juniper Networks provides the junos-extension-odl YANG module. The module contains definitions for Junos OS Output Definition Language (ODL) statements, which determine the CLI formatting for RPC output when you execute the operational command corresponding to that RPC in the CLI or when you request the RPC output in text format. You can use statements in the junos-extension-odl module in custom RPCs to convert the XML output into a more logical and human-readable representation of the data. The junos-extension-odl module is bound to the namespace URI http://yang.juniper.net/yang/1.1/jodl and uses the prefix junos-odl.

[See Understanding Junos OS YANG Extensions for Formatting RPC Output.]

• YANG module that defines Junos OS operational commands (PTX Series)—Starting with Junos OS Release 16.1, Juniper Networks provides the juniper-command YANG module, which represents the operational command hierarchy and collective group of modules that define the remote procedure calls (RPCs) for Junos OS operational mode commands. You can download Juniper Networks YANG modules from the website, or you can generate the modules by using the show system schema format yang module juniper-command operational command on the local device. The juniper-command module is bound to the namespace URI http://yang.juniper.net/yang/1.1/jrpc and uses the prefix jrpc.

[See Understanding the Juniper Networks YANG Modules for Operational Commands.]

MPLS

• Explicit notifications for pseudowire termination (PTX Series routers)—Starting in Junos OS Release 15.2, this feature enables you to provide notifications on the service node when the access pseudowire goes down and provide efficient termination capabilities, when Layer 2 and Layer 3 segments are interconnected. This also provides
termination of pseudowire into VRF and VPLS routing instance without pseudowire redundancy, which includes:

- Termination of access pseudowire into virtual routing and forwarding (VRF)
- Termination of access pseudowire into virtual private LAN service (VPLS) instance

- **Packet Forwarding Engine fast reroute for P2MP link-protection (PTX Series)**—Starting with Junos OS Release 16.1, fast reroute (FRR) is enabled within the PFE on detection of link failure of the primary path of a point-to-multipoint (P2MP) sub-LSP, thereby reducing traffic loss. This support is provided for FPC1 and FPC2 of PTX Series routers.

- **RSVP scalability (PTX Series)**—Starting with Junos OS Release 16.1, RSVP traffic engineering (TE) protocol extensions for fast reroute (FRR) facility protection are introduced to allow greater scalability of LSPs and faster convergence times. RSVP-TE runs in **enhanced FRR profile** mode by default and includes FRR extensions as defined in RFC 2961. In mixed environments, where a subset of LSPs traverse nodes that do not include this feature, RSVP-TE behavior is unchanged—backward compatibility is fundamentally supported in the design.

- **Fast branch updates to existing point-to-multipoint LSPs (PTX Series with first generation and second generation FPCs)**—Beginning with Junos OS Release 16.1, fast branch updates, also known as fast make-before-break (FMBB), is supported by default on PTX Series routers. This feature allows changes to existing point-to-multipoint LSPs by performing incremental additions to the existing binary replication tree. Because the original binary tree is intact, no traffic loss is expected over the existing branches.

- **For point-to-multipoint LSPs, protect the Packet Forwarding Engine (PFE) from bandwidth saturation (PTX Series with first generation and second generation FPCs)**—When a PFE does not need to replicate traffic, the PFE’s bandwidth is less likely to become saturated. When you include the `no-mcast-replication` statement at the `[edit chassis fpc slot-number pic slot-number port port-number]` hierarchy level, the PFE is forced to be a leaf node in the multicast binary tree. Leaf nodes, unlike branch nodes, do not replicate traffic in the process of forwarding traffic. Because leaf nodes have no children, they do not need to replicate traffic, and therefore they are less likely to become saturated with traffic.

- **Support for MPLS Transport Profile (PTX Series with first generation and second generation FPCs)**—The MPLS Transport Profile (MPLS-TP) introduces new capabilities for Operations, Administration, and Management (OAM) when MPLS is used for transport services and transport network operations. This includes a generic mechanism to send OAM messages. This mechanism contains two main components:
  - **Generic Alert Label (GAL)**—A special label that enables an exception mechanism that informs the egress label-switching router (LSR) that a packet it receives on an LSP belongs to an associated control channel or the control plane.
  - **Generic Associated Control Channel Header (G-Ach)**—A special header field that identifies the type of payload contained in the MPLS label-switched paths (LSPs). G-Ach has the same format as a pseudowire associated control channel header.
For more information about MPLS-TP, see RFC 5654, *Requirements of an MPLS Transport Profile*. For more information about GAL and G-Ach, see RFC 5586, *MPLS Generic Associated Channel*.

The following capabilities are supported in the Junos OS implementation of MPLS-TP:

- MPLS-TP OAM can send and receive packets with GAL and G-Ach, without IP encapsulation.
- Two unidirectional RSVP LSPs between a pair of routers can be associated with each other to create an associated bidirectional LSP for binding a path for the GAL and G-Ach OAM messages. The associated bidirectional LSP model is only supported for associating the primary paths. A single Bidirectional Forwarding Detection (BFD) session is established for the associated bidirectional LSP.

The current Junos OS implementation of MPLS-TP does not support:

- P2MP RSVP LSPs and BGP LSPs
- Loss Measurement (LM) and Delay Measurement (DM)

[See *Configuring the MPLS Transport Profile for OAM*.]

**MPLS-TP enhancements for on-demand connectivity verification (PTX Series with FPC1 and FPC2 interfaces)**—Starting with Junos OS Release 16.1, the transport profile (TP) of MPLS supports two additional channel types for the default LSPING channel type. These additional channel types provide on-demand connectivity verification (CV) with and without IP/UDP encapsulation.

With this feature, the following channel types are supported in the MPLS-TP mode:

- On-demand CV (0x0025)—This channel type is a new pseudowire channel type and is used for on-demand CV without IP/UDP encapsulation, where IP addressing is not available or non-IP encapsulation is preferred.
- IPv4 (0x0021)—This channel type uses the IP/UDP encapsulation and provides interoperability support with other vendor devices using IP addressing.
- LSPING (0x0008)—This is the default channel type for Junos OS, and the GACH-TLV is used along with this channel type.

As per RFC 7026, GACH-TLV is deprecated for 0x0021 and 0x0025 channel types.

To configure a channel type for MPLS-TP, include the `lsping-channel-type channel-type` statement at the `[edit protocols mpls label-switched-path lsp-name oam mpls-tp-mode]` and `[edit protocols mpls oam mpls-tp-mode]` hierarchy levels.
Network Management and Monitoring

- **Support for RFC 4878 (PTX Series)**—Starting with Release 16.1, Junos OS supports IETF standard RFC 4878, *Definitions and Managed Objects for Operations, Administration, and Maintenance (OAM) Functions on Ethernet–Like Interfaces.*

  To enable generation of SNMP traps, `dot3OamThresholdEvent` and `dot3OamNonThresholdEvent`, you must configure the new `dot3oam-events` statement at the `[edit snmp trap-groups <group-name> categories]` hierarchy level.

  **NOTE:**
  - Junos OS does not support the `dot3oamFramesLostDueToOam` object in the `dot3OamStatsEntry` table. In addition, Junos OS does not support the SNMP set operations for the OAM MIBs.
  - On an aggregated Ethernet bundle, if link fault management (LFM) is configured, you must do SNMP operations individually for each interface in the AE bundle because most of the OAM MIB tables are maintained only for member interfaces in the AE bundle.

- **Support for Entity State MIBs (PTX Series)**—Starting with Junos OS Release 16.1, support for IETF standard RFC 4268, *Entity State MIB*, is extended to the PTX Series. Junos OS provides only read-only support to Entity State MIBs.


- **SNMP MIB support for Ethernet OAM (PTX3000 and PTX5000)**—SNMP MIB support is enabled for Ethernet OAM on PTX3000 and PTX5000 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.

- **New indicators for the jnxLEDState MIB (PTX 3000)**—Starting with Release 16.1, Junos OS introduces the following six new indicators for the `jnxLEDState` MIB object in the `jnxLEDEntry` MIB table:
  - `off`—Offline, not running
  - `blinkingGreen`—Entering state of ok, good, normally working
  - `blinkingYellow`—Entering state of alarm, warning, marginally working
  - `blinkingRed`—Entering state of alert, failed, not working
  - `blinkingBlue`—Entering state of ok, online as an active primary
  - `blinkingAmber`—Entering state of offline, not running

- **Support for Agent Capabilities MIB (PTX Series)**—Starting with Release 16.1, Junos OS introduces the Agent Capabilities MIB, which provides information about the implementation characteristics of an Agent subsystem in a network management
system. The MIB provides you details of the MIB objects and tables that are supported by an Agent, the conformance and variance information associated with the managed objects in the Agent, and the access level of each object. Currently, the Agent Capability MIB is applicable only for the MPLS and multicast MIBs.

**Routing Protocols**

- **IS-IS purge originator identification TLV (PTX Series)**—Beginning with Release 15.1F4, Junos OS supports RFC 6232, *Purge Originator Identification TLV for IS-IS*, which defines a type, length, and value (TLV) for identifying the origin of a purge initiated by the IS-IS protocol. You can configure this feature to add this TLV to a purge, along with the system ID of the Intermediate System (IS) that has initiated this purge. This makes it easier to locate the origin of the purge and its cause.
  
  [See IS-IS Purge Originator Identification Overview.]

- **LDP native IPv6 support (PTX Series)**—Starting with Junos OS Release 16.1, LDP is supported in an IPv6 network only, and in an IPv6 or IPv4 dual-stack network. Configure the address family as `inet` for IPv4 or `inet6` for IPv6. By default, IPv6 is used as the TCP transport for an LDP session with its peers when both IPv4 and IPv6 are enabled. The `dual-transport` statement allows Junos OS LDP to establish the TCP connection over IPv4 with IPv4 neighbors, and over IPv6 with IPv6 neighbors as a single-stack LSR. The `inet-lsr-id` and `inet6-lsr-id` are the two LSR IDs that have to be configured to establish an LDP session over IPv4 and IPv6 TCP transport. These two IDs should be non-zero and must be configured with different values.

- **Weighted ECMP support for one-hop IS-IS neighbors (PTX Series)**—Beginning with Junos OS Release 15.1F4, you can configure the IS-IS protocol to get the logical interface bandwidth information associated with the gateways of equal-cost multipath (ECMP) next hop. During per-packet load balancing, traffic distribution is based on the available bandwidth to facilitate optimal bandwidth usage for incoming traffic on an ECMP path of one hop distance. The Packet Forwarding Engine does not distribute the traffic equally, but considers the balance values and distributes the traffic according to the bandwidth availability. However, this feature is not available for ECMP paths that are more than one hop away.

  [See Weighted ECMP Traffic Distribution on One Hop IS-IS Neighbors Overview.]
User Interface and Configuration

- **Support for JSON format for configuration data (PTX Series)**—Starting with Junos OS Release 16.1, you can configure devices running Junos OS using configuration data in JavaScript Object Notation (JSON) format in addition to the existing text, Junos XML, and Junos OS set command formats. You can load configuration data in JSON format in the Junos OS CLI by using the `load (merge | override | update) json` command or from within a NETCONF or Junos XML protocol session by using the `<load-configuration format="json">` operation. You can load JSON configuration data either from an existing file or as a data stream. Configuration data that is provided as a data stream must be enclosed in a `<configuration-json>` element.

[See load, Defining the Format of Configuration Data to Upload in a Junos XML Protocol Session, and Mapping Junos OS Configuration Statements to JSON.]

VPNs

- **New configuration statement to manage VCCV BFD session state (PTX Series)**—Starting with Junos OS Release 16.1, the `ping-multiplier` statement is introduced to delay the virtual circuit connectivity verification (VCCV) Bidirectional Forwarding Detection (BFD) session from going down by the specified number of LSP ping packets. The VCCV BFD session is signaled down only after the specified number of LSP ping packets are lost. This feature is supported for Layer 2 Circuit, Layer 2 VPN, and VPLS technologies.

To configure the LSP ping multiplier feature, include the `ping-multiplier number-of-packets` statement at the `[edit protocols l2circuit neighbor neighbor-address interface interface-name oam]`, `[edit routing-instances routing-instances-name protocols l2vpn oam]`, and `[edit routing-instances routing-instances-name protocols vpls oam]` hierarchy levels for Layer 2 circuit, Layer 2 VPN, and VPLS, respectively.

**Related Documentation**

- Changes in Behavior and Syntax on page 151
- Known Behavior on page 154
- Known Issues on page 155
- Resolved Issues on page 157
- Documentation Updates on page 156
- Migration, Upgrade, and Downgrade Instructions on page 157
- Product Compatibility on page 161

**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 in Junos OS Release 16.1R1 for the PTX Series.

- Hardware on page 152
- Forwarding and Sampling on page 152
• Interfaces and Chassis on page 152
• Routing Policy and Firewall Filters on page 153
• Routing Protocols on page 153
• Software Installation and Upgrade on page 153
• System Logging on page 153
• User Interface and Configuration on page 153

Hardware

• Powering on offline FPCs (PTX5000)—Beginning in Junos OS Release 16.1, offline FPCs do not come online during reboots or other power management events. To bring such an FPC online:
  1. Delete the `fpc fpc-slot power off` statement from the `[edit chassis]` hierarchy level, if that statement is configured, and commit the configuration.
  2. Either issue the `request chassis fpc online slot fpc-slot` operational-mode CLI command or press and hold the FPC ONLINE/OFFLINE button for about 5 seconds until the green OK LED next to the button lights steadily.

Forwarding and Sampling

• Deprecation of disable option (PTX3000)—Beginning in Junos OS Release 16.1, the disable option has been deprecated at the `[forwarding-options sampling instance instance-name family (inet | inet6 | mpls)]` hierarchy level on PTX3000 routers. When configured, the option does not take effect, so packets continue to be sampled. Instead of the disable option, use the `deactivate forwarding-options sampling instance instance-name family (inet | inet6 | mpls)` command to prevent sampling.

[See disable (Forwarding Options).]

Interfaces and Chassis

• Modified the default temperature threshold for FPC-SFF-PTX-P1-A (PTX Series)—In Junos OS Release 16.1R1 and later, the default temperature threshold value for FPC-SFF-PTX-P1-A is decreased to prevent yellow alarm, as shown in the following example:

<table>
<thead>
<tr>
<th>Item</th>
<th>C</th>
<th>Normal Fan Speed</th>
<th>Normal High</th>
<th>Normal Bad Fan</th>
<th>Normal Fire Shutdown</th>
<th>Normal Bad Fire Shutdown</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 0 PMB CPU</td>
<td>C</td>
<td>80</td>
<td>90</td>
<td>95</td>
<td>85</td>
<td>105</td>
</tr>
<tr>
<td>FPC 0 Exhaust</td>
<td>C</td>
<td>75</td>
<td>85</td>
<td>95</td>
<td>85</td>
<td>105</td>
</tr>
<tr>
<td>FPC 0 Intake</td>
<td>C</td>
<td>80</td>
<td>90</td>
<td>95</td>
<td>85</td>
<td>105</td>
</tr>
<tr>
<td>FPC 0 TL0</td>
<td>C</td>
<td>75</td>
<td>85</td>
<td>95</td>
<td>85</td>
<td>105</td>
</tr>
<tr>
<td>FPC 0 TQ0</td>
<td>C</td>
<td>75</td>
<td>85</td>
<td>95</td>
<td>85</td>
<td>105</td>
</tr>
<tr>
<td>FPC 0 TL1</td>
<td>C</td>
<td>75</td>
<td>85</td>
<td>95</td>
<td>85</td>
<td>105</td>
</tr>
<tr>
<td>FPC 0 TQ1</td>
<td>C</td>
<td>75</td>
<td>85</td>
<td>95</td>
<td>85</td>
<td>105</td>
</tr>
</tbody>
</table>
A yellow alarm is raised whenever the component temperature crosses the configured
temperature threshold value.

Routing Policy and Firewall Filters

- Support for logical queue-depth in the PFE for IP options packets for a given protocol
  (PTX Series) — Starting with Junos OS Release 16.1R1, you can configure logical
  queue-depth in the PFE for IP options packets for a given protocol. The queue-depth
  indicates the number of IP options packets which can be enqueued in the PFE logical
  queue, beyond which it would start dropping the packets.

Routing Protocols

- BGP advertises inactive routes when advertise-inactive statement is not
  configured — When BGP advertises a network layer reachability information (NLRI)
  with a label, and the advertised route resides in an xxx.xxx.3 routing table such as inet.3,
  Junos OS automatically advertises such inactive routes even if you have not configured
  the advertise-inactive statement.

Software Installation and Upgrade

- request system software add command options updated (PTX Series) — As of Junos
  OS Release 16.1, the upgrade-with-config-format option in the request system software
  add command is removed. The upgrade-with-config option applies to the file indicated.
  Specify .text or .xml. The upgrade-with-config option does not accept files with the
  extension .txt.

System Logging

- Support for system log message: UI_SKIP_SYNC_OTHER_RE (PTX Series) — Starting
  with Junos OS Release 16.1R1, configuration synchronization with a remote Routing
  Engine is skipped when the configuration is already in sync with another Routing Engine
  with database revision.

  **NOTE:** This system log message is generated when the graceful Routing
  Engine switchover feature is enabled.

  This system log message reports an event, not an error, and has notice as Severity and
  LOG_AUTH as Facility.

User Interface and Configuration

- output-file-name option for show system schema command is deprecated (PTX
  Series) — Starting with Junos OS Release 16.1, the output-file-name option for the show
  system schema operational command is deprecated. To direct the output to a file, use
  the output-directory option and specify the directory. By default, the filename for
  the output file uses the module name as the filename base and the format as the filename
  extension. If you also include the module-name option in the command, the specified
module name is used for both the name of the generated module and for the filename base for the output file.

[See show system schema.]

- New default implementation for serialization for JSON configuration data (PTX Series)—Starting with Junos OS Release 16.1, the default implementation for serialization for configuration data emitted in JavaScript Object Notation (JSON) has changed. The new default is as defined in internet drafts draft-ietf-netmod-yang-json-09, JSON Encoding of Data Modeled with YANG, and draft-ietf-netmod-yang-metadata-06, Defining and Using Metadata with YANG.

[See Mapping Junos OS Configuration Statements to JSON.]

### Related Documentation

- New and Changed Features on page 143
- Known Behavior on page 154
- Known Issues on page 155
- Resolved Issues on page 157
- Documentation Updates on page 156
- Migration, Upgrade, and Downgrade Instructions on page 157
- Product Compatibility on page 161

### Known Behavior

This section contains the known behavior, system maximums, and limitations in hardware and software in Junos OS Release 16.1R1 for PTX Series.

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

- General Routing on page 154

### General Routing

- The temperature conditions of the Routing Engine FRU for RE-PTX-X8 are now displayed correctly. The `show chassis zones` command now displays the accurate temperature conditions.

- The date and time zones are synchronized from the admin guest Junos OS to host OS on the PTX5000 router and use the same time zones. Therefore, there is no difference in the timestamp in system log files of Junos OS and the host OS.
Known Issues

This section lists the known issues in hardware and software in Junos OS Release 16.1R1 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.

• General Routing on page 155
• Routing Protocols on page 156

General Routing

• On PTX Series platforms with PIM configured and traffic flows, the following harmless error messages might be seen continuously on restarting routing or clearing PIM join:
  [LOG: Err] jbwy_fw_plct_free_cntr: 1117 Not able to find the cntr from list [LOG: Err]
  bwy_rt_free_stats_counters: jbwy_fw_plct_free_cntr failed 7 [LOG: Err]
  jbwy_fw_plct_free_cntr: 1117 Not able to find the cntr from list [LOG: Err]
  bwy_rt_free_stats_counters: jbwy_fw_plct_free_cntr failed 7 [LOG: Err]
  bwy_rt_cntr_stats_alloc: counter allocation failed for prefix 225.0.11.11.1.12/64 for sgif status 7. PR1004510

• On PTX Series platforms, if there are scaling configurations (for example 5,000 routes and each of them with 64 ECMP paths configured) on a single interface and an L2 rewrite profile is applied for the interface, the FPC may crash when deactivating and then activating the CoS configuration of the interface. PR1096958

• The "clear services accounting flow" command should not be used in Junos OS Release 15.1F4 or Junos OS Release 15.1F5 on inline J-flow on PTX5000 router for PTX Series. This command is specific to J-flow and is not supported in these releases. PR1117181

• DA mac filter is missing on Child link of AE after FPC restart. PR1184310
Routing Protocols

- When we have two paths for the same route, the route gets pointed to Unilist NH, which in turn gets pointed to two separate Unicast NHs. The route is determined by OSPF and we have BFD enabled on one of the paths, which runs through an l2circuit path. When the link on the l2circuit gets cut, the link flap is informed by BFD as well as through OSPF LSAs. Ideally the BFD should inform the link down event before the OSPF LSA. But at the current situation, the OSPF LSAs update the current event a second before BFD. Due to this reason, we do get the route to be pointing to a new Unilist NH with the weights swapped. But the Unicast NH for which the L3 link is down gets added to the Unilist NH, the BFD assumes the link to be up, and hence updates the weights inappropriately and hence we do see traffic loss. Once the BFD link down event is processed at OSPF protocol level, now the route points to only Unicast NH and hence we do see traffic flowing through the currently active link. The traffic outage would be hardly for less than a second during FRR. Also, this can be avoided if the BFD keepalive intervals are maintained around 50 ms with multiplier of 3 as opposed to 100 ms with a multiplier of 3. PR1119253

Related Documentation
- New and Changed Features on page 143
- Changes in Behavior and Syntax on page 151
- Known Behavior on page 154
- Resolved Issues on page 157
- Documentation Updates on page 156
- Migration, Upgrade, and Downgrade Instructions on page 157
- Product Compatibility on page 161

Documentation Updates

This section lists the errata and changes in Junos OS Release 16.1R1 documentation for the PTX Series.

- NETCONF XML Management Protocol Developer Guide on page 156

NETCONF XML Management Protocol Developer Guide

- The NETCONF XML Management Protocol Developer Guide incorrectly states that you can load custom YANG modules and action scripts on devices running Junos OS to augment the operational command hierarchy with non-native YANG RPCs. Junos OS does not support loading custom RPCs on devices running Junos OS.

Related Documentation
- New and Changed Features on page 143
- Changes in Behavior and Syntax on page 151
- Known Behavior on page 154
- Known Issues on page 155
Resolved Issues

This section lists the issues fixed in the Junos OS main release and the maintenance releases. The identifier following the description is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

- Forwarding and Sampling on page 157

Forwarding and Sampling

SRRD (Sampling Route-Record Daemon) process does not delete routes when the DELETE is received from RPD in few configuration cases. This results in buildup of memory in SRRD daemon, and once SRRD reaches the limit, it crashes and restarts itself. This happens only when one certain family is not configured on all of the FPC clients (e.g., FPC with inline J-Flow enabled or PIC with PIC-based sampling enabled is one client). For example, only IPv4 family is configured in all the clients and IPv6 and MPLS families are not configured for sampling in any of the clients. PR1180158

Related Documentation

- New and Changed Features on page 143
- Changes in Behavior and Syntax on page 151
- Known Behavior on page 154
- Known Issues on page 155
- Documentation Updates on page 156
- Migration, Upgrade, and Downgrade Instructions on page 157
- Product Compatibility on page 161

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 on page 157
- Upgrading a Router with Redundant Routing Engines on page 158
- Basic Procedure for Upgrading to Release 16.1 on page 158

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 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 16.1**

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

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

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

**NOTE:** The installation process rebuilds the file system and completely reinstall 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 16.1R1 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 16.1R1 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-16.1R.SPIN-domestic-signed.tgz
```
All other customers, use the following command:

```
user@host> request system software add validate reboot source /jinstall-16.1 R.SPIN-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:** You need to install the Junos OS software package and host software package on the routers with the RE-PTX-X8 Routing Engine. For upgrading the host and Junos OS on this router with VM host support, use the `junos-vmhost-install-x.tgz` image and specify the name of the regular package in the request `vmhost software add` command. For more information see VM Host Installation topic in *Installation and Upgrade Guide*.

---

**NOTE:** After you install a Junos OS Release 16.1 `jinstall` package, you cannot issue the `request system software rollback` command to return to the previously installed software. Instead you must issue the `request system software add validate` command and specify the `jinstall` package that corresponds to the previously installed software.

---

**NOTE:** A few of the existing `request system` commands are not supported on routers with RE-PTX-X8 Routing Engines. See the VM Host Software Administrative Commands in the Installation and Upgrade Guide.

---

**Related Documentation**

- New and Changed Features on page 143
- Changes in Behavior and Syntax on page 151
Product Compatibility

- Hardware Compatibility on page 161

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 143
- Changes in Behavior and Syntax on page 151
- Known Behavior on page 154
- Known Issues on page 155
- Resolved Issues on page 157
- Documentation Updates on page 156
- Migration, Upgrade, and Downgrade Instructions on page 157
Junos OS Release Notes for the QFX Series

These release notes accompany Junos OS Release 16.1R1 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

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

- New and Changed Features on page 162
- Changes in Behavior and Syntax on page 164
- Known Behavior on page 165
- Known Issues on page 166
- Documentation Updates on page 168
- Migration, Upgrade, and Downgrade Instructions on page 169
- Product Compatibility on page 172

New and Changed Features

This section describes the new features for the QFX Series switches in Junos OS Release 16.1R1.

**NOTE:** Junos OS Release 16.1R1 supports QFX5100 switches. Juniper Networks does not recommend using Junos OS Release 16.1Rx with QFX10002 switches.

- Junos OS XML API and Scripting on page 163
- Routing Protocols on page 163
- Routing Policy and Firewall Filters on page 163
- User Interface and Configuration on page 163
Junos OS XML API and Scripting

- Support for Python language for commit, event, op, and SNMP scripts (QFX5100, QFX10002) — Starting in Junos OS Release 16.1, you can author commit, event, op, and SNMP scripts in Python on devices that include the Python extensions package in the software image. Creating automation scripts in Python enables you to take advantage of Python features and libraries, as well as leverage Junos PyEZ APIs supported in Junos PyEZ Release 1.3.1 and earlier releases to perform operational and configuration tasks on devices running Junos OS. To enable execution of Python automation scripts, which the root user must own, configure the `language python` statement at the [edit system scripts] hierarchy level, and configure the filename for the Python script under the hierarchy level appropriate to that script type. Supported Python versions include Python 2.7.x.

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

Routing Protocols

- BGP link state distribution (QFX Series) — Junos OS Release 16.1 introduces a new mechanism to distribute topology information across multiple areas and autonomous systems (ASs) by extending the BGP protocol to carry link state information. Earlier, this information was acquired using an IGP, which has scaling limitations when it comes to distributing a large database. Using BGP provides a policy-controlled and scalable means of distributing the multi-area and multi-AS topology information. This information is used for computing paths for MPLS LSPs spanning multiple domains, such as inter-area TE LSP, and enables external path computing entities, such as ALTO and PCE, to acquire network topology.

Routing Policy and Firewall Filters

- Support for flexible-match-mask match condition (QFX5100 switches) — Starting with Junos OS Release 16.1, QFX5100 switch firewall filters support the `flexible-match-mask` match condition. The match condition can be enabled for both inet and Ethernet-switching families.

User Interface and Configuration

- Support for JSON format for configuration data (QFX5100, QFX10002) — Starting with Junos OS Release 16.1, you can configure devices running Junos OS using configuration data in JavaScript Object Notation (JSON) format in addition to the existing text, Junos XML, and Junos OS `set` command formats. You can load configuration data in JSON format in the Junos OS CLI by using the `load (merge | override | update) json` command or from within a NETCONF or Junos XML protocol session by using the `<load-configuration format="json">` operation. You can load JSON configuration data either from an existing file or as a data stream. Configuration data that is provided as a data stream must be enclosed in a `<configuration-json>` element.

[See load, Defining the Format of Configuration Data to Upload in a Junos XML Protocol Session, and Mapping Junos OS Configuration Statements to JSON.]
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 16.1R1 for the QFX Series.

- General Routing on page 164
- Security on page 165
- Software Installation and Upgrade on page 165
- User Interface and Configuration on page 165

General Routing

- Enhancement to request support information command—Starting in Junos OS Release 16.1R1, the request support information command is enhanced to capture the following additional details:
  - file list detail /var/run/db/—Displays the size of the configuration databases.
  - show system configuration database usage—Displays the actual usage of the configuration databases.

  NOTE: This information will be displayed only if the show system configuration database usage command is supported in the release.

- file list detail /config/—Contains the db_ext file and shows the size of it to indicate whether extend_size is enabled or disabled.

- New option introduced under show | display xml | display—Starting in Junos OS 16.1R1, you can use the show | display xml | display | mark-changed statement to view the "mark-changed" status of the nodes. This is useful for debugging purposes.

- Modified output of the clear services sessions | display xml command (MX Series)—In Junos OS Release 16.1, the output of the clear services sessions | display xml command is modified to include the <sess-marked-for-deletion> tag instead of the <sess-removed> tag. In releases before Junos OS Release 14.1X55-D30, the output of this command includes the <sess-removed> tag. The replacement of the <sess-removed> tag with the <sess-marked-for-deletion> tag aims at establishing consistency with the output of the clear services sessions command that includes the field Sessions marked for deletion.
Security

- Changes to DDoS protection packet type support (QFX Series)—Starting in Junos OS Release 16.1, the unclassified packet type in the mcast-snoop protocol group has been removed from the protocols statement at the [edit system ddos-protection] hierarchy level and from the output of the show ddos-protection protocols command.

Software Installation and Upgrade

- request system software add command options updated (QFX Series)—As of Junos OS Release 16.1, the upgrade-with-config-format option in the request system software add command is removed. The upgrade-with-config option applies to the file indicated. Specify .text or .xml. The upgrade-with-config option does not accept files with the extension .txt.

User Interface and Configuration

- output-file-name option for show system schema command is deprecated (QFX5100, QFX10002)—Starting with Junos OS Release 16.1, the output-file-name option for the show system schema operational command is deprecated. To direct the output to a file, use the output-directory option and specify the directory. By default, the filename for the output file uses the module name as the filename base and the format as the filename extension. If you also include the module-name option in the command, the specified module name is used for both the name of the generated module and for the filename base for the output file.

  [See show system schema.]

- New default implementation for serialization for JSON configuration data (QFX5100, QFX10002)—Starting with Junos OS Release 16.1, the default implementation for serialization for configuration data emitted in JavaScript Object Notation (JSON) has changed. The new default is as defined in Internet drafts draft-ietf-netmod-yang-json-09, JSON Encoding of Data Modeled with YANG, and draft-ietf-netmod-yang-metadata-06, Defining and Using Metadata with YANG.

  [See Mapping Junos OS Configuration Statements to JSON.]

Related Documentation

- New and Changed Features on page 162
- Known Behavior on page 165
- Known Issues on page 166
- Documentation Updates on page 168
- Migration, Upgrade, and Downgrade Instructions on page 169
- Product Compatibility on page 172

Known Behavior

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 16.1R1 for the QFX Series.
For the most complete and latest information about known Junos OS problems, use the Juniper Networks online Junos Problem Report Search application.

- Software Installation and Upgrade on page 166

**Software Installation and Upgrade**

- Option upgrade-with-config accepts only configuration files with extension .text or .xml (QFX Series)—In the request system software add command, the upgrade-with-config option does not apply the configuration if the configuration file has the extension .txt. This option accepts only files with the extension .text or .xml.

**Related Documentation**

- New and Changed Features on page 162
- Changes in Behavior and Syntax on page 164
- Known Issues on page 166
- Documentation Updates on page 168
- Migration, Upgrade, and Downgrade Instructions on page 169
- Product Compatibility on page 172

**Known Issues**

This section lists the known issues in hardware and software for the QFX Series switches in Junos OS Release 16.1R1.

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

- Authentication, Authorization, and Accounting on page 167
- High Availability and Resiliency on page 167
- Interfaces and Chassis on page 167
- IP Address Management on page 167
- Layer 2 Features on page 167
- Multicast on page 167
- Network Analytics on page 168
- Port Security on page 168
- Software Defined Networking on page 168
- Software Installation and Upgrade on page 168
- Spanning Tree Protocols on page 168
- System Management on page 168
Authentication, Authorization, and Accounting

- On QFX5100 switches, 802.1X authentication might not work after the dot1x protocol is restarted. PR1197446

High Availability and Resiliency

- On QFX5100 switches, after disabling MC-LAG member interfaces, more than 3 seconds of traffic loss might occur. PR1164228

Interfaces and Chassis

- On QFX5100 Virtual Chassis, DHCPv6 binding might fail if the server and the client are in different virtual routing and forwarding (VRF) instances. PR1167693
- With 100 or more Layer 2 circuit configurations in standby mode on a QFX5100 switch, the Layer 2 circuits might go down after issuing the restart routing operational mode command. PR1169575
- Layer 2 circuits on QFX5100 switches might not come up if 100 or more Layer 2 circuit connections are configured in no-standby mode. PR1169659
- On QFX Series switches, a Packet Forwarding Engine (PFE) or device-control process (dcd) restart might result in traffic loss. PR1188120
- After deactivating interfaces on a QFX5100 switch that is configured as a primary neighbor of a provider edge router, the backup Layer 2 circuit might not get activated as expected. PR1198191

IP Address Management

- On QFX5100 switches, a long ICMP delay might occur when attempting to ping a directly connected integrated routing and bridging (IRB) interface. PR966905

Layer 2 Features

- On QFX10002 switches, MAC addresses associated with a VLAN might be inadvertently deleted if the VLAN is configured as a native VLAN and is associated with an MC-LAG interface. PR1193881

Multicast

- On a QFX10002 switch that functions as a peer in a multicast group, multicast traffic entering a Layer 3 VLAN-tagged interface might be inadvertently dropped. PR1198502
- On QFX10002 switches, when IGMPv2 and IGMPv3 receivers for the same multicast group are in a VLAN, multicast traffic might not flow to any or a few of the IGMPv2 receivers. PR1190736
Network Analytics

- Despite the QFX5100 switch's being configured with the network analytics feature, the analytics daemon might not run. As a result, the network analytics feature might be unable to collect traffic and queue statistics and generate reports. PR1165768

Port Security

- On QFX5100 Virtual Chassis, the DHCP snooping database might be cleared if you change the configuration of the LACP mode from fast to slow. PR1191404

Software Defined Networking

- Deleted VLAN configurations provided by an OVSDB controller might be erroneously retained by QFX5100 switches. PR1176592
- On QFX5100 switches, OVSDB traffic might be dropped after Layer 2 learning is restarted. PR1177012

Software Installation and Upgrade

- After a unified ISSU upgrade from Junos OS Release 15.1R3 to Junos OS Release 16.1 on QFX5100 switches, LLDP neighbor discovery might fail. PR1187729

Spanning Tree Protocols

- On QFX5100 VC interfaces on which the flexible-vlan-tagging statement is specified, STP, RSTP, MSTP, and VSTP are not supported. PR1075230

System Management

- On QFX5100 switches, the amount of time that it takes for Zero Touch Provisioning to complete might be lengthy because TFTP might take a long time to fetch required data. PR980530

Related Documentation

- New and Changed Features on page 162
- Changes in Behavior and Syntax on page 164
- Known Behavior on page 165
- Documentation Updates on page 168
- Migration, Upgrade, and Downgrade Instructions on page 169
- Product Compatibility on page 172

Documentation Updates

This section lists the errata and changes in Junos OS Release 16.1R1 for the QFX Series switches documentation.

NETCONF XML Management Protocol Developer Guide

- The NETCONF XML Management Protocol Developer Guide incorrectly states that you can load custom YANG modules and action scripts on devices running Junos OS to augment the operational command hierarchy with non-native YANG RPCs. Junos OS does not support loading custom RPCs on devices running Junos OS.

Related Documentation
- New and Changed Features on page 162
- Changes in Behavior and Syntax on page 164
- Known Behavior on page 165
- Known Issues on page 166
- Migration, Upgrade, and Downgrade Instructions on page 169
- Product Compatibility on page 172

Migration, Upgrade, and Downgrade Instructions

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

- Performing an In-Service Software Upgrade (ISSU) on page 169
- Preparing the Switch for Software Installation on page 169
- Upgrading the Software Using ISSU on page 170

Performing an In-Service Software Upgrade (ISSU)

You can use ISSU to upgrade the software running on the switch with minimal traffic disruption during the upgrade.

NOTE: ISSU is supported in Junos OS Release 13.2X51-D15 and later.

Perform the following tasks:

- Preparing the Switch for Software Installation on page 169
- Upgrading the Software Using ISSU on page 170

Preparing the Switch for Software Installation

Before you begin software installation using ISSU:

- Ensure that nonstop active routing (NSR), nonstop bridging (NSB), and graceful Routing Engine switchover (GRES) are enabled. NSB and GRES enable NSB-supported Layer 2 protocols to synchronize protocol information between the master and backup Routing Engines.

To verify that nonstop active routing is enabled:
NOTE: If nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

user@switch> show task replication
   Stateful Replication: Enabled
   RE mode: Master

If nonstop active routing is not enabled (Stateful Replication is Disabled), see Configuring Nonstop Active Routing on Switches for information about how to enable it.

- Enable nonstop bridging (NSB). See Configuring Nonstop Bridging on Switches (CLI Procedure) for information on how to enable it.
- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the request system snapshot command.

Upgrading the Software Using ISSU

This procedure describes how to upgrade the software running on a standalone switch.

To upgrade the switch using ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in Upgrading Software.
2. Copy the software package or packages to the switch. We recommend that you copy the file to the /var/tmp directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Start the ISSU:
   - On the switch, enter:
     
     user@switch> request system software in-service-upgrade /var/tmp/package-name.tgz
     
     where package-name.tgz is, for example, jinstall-132_x51_vjunos.domestic.tgz.

NOTE: During the upgrade, you cannot access the Junos OS CLI.

The switch displays status messages similar to the following messages as the upgrade executes:

warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get lost!
ISSU: Validating Image
ISSU: Preparing Backup RE
Prepare for ISSU
ISSU: Backup RE Prepare Done
Extracting jinstall-qfx-5-13.2X51-D15.4-domestic ...
Install jinstall-qfx-5-13.2XS1-D1S.4-domestic completed
Spawning the backup RE
Spawn backup RE, index 0 successful
GRES in progress
GRES done in 0 seconds
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
<table>
<thead>
<tr>
<th>Item</th>
<th>Status</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>FPC 0</td>
<td>Online (ISSU)</td>
<td></td>
</tr>
</tbody>
</table>
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff

NOTE: An ISSU might stop, instead of abort, if the FPC is at the warm boot stage. Also, any links that go down and up will not be detected during a warm boot of the Packet Forwarding Engine (PFE).

NOTE: If the ISSU process stops, you can look at the log files to diagnose the problem. The log files are located at /var/log/vjunos-log.tgz.

5. Log in after the reboot of the switch completes. To verify that the software has been upgraded, enter the following command:

   user@switch> show version

6. To ensure that the resilient dual-root partitions feature operates correctly, copy the new Junos OS image into the alternate root partitions of all of the switches:

   user@switch> request system snapshot slice alternate

   Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

Related Documentation
- New and Changed Features on page 162
- Changes in Behavior and Syntax on page 164
- Known Behavior on page 165
- Known Issues on page 166
- Documentation Updates on page 168
Product Compatibility

- Hardware Compatibility on page 172

Hardware Compatibility

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

To determine the features supported on QFX 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 162
- Changes in Behavior and Syntax on page 164
- Known Behavior on page 165
- Known Issues on page 166
- Documentation Updates on page 168
- Migration, Upgrade, and Downgrade Instructions on page 169

Third-Party Components

This product includes third-party components. To obtain a complete list of third-party components, see Overview for Routing Devices.

For a list of open source attributes for this Junos OS release, see Open Source: Source Files and Attributions.

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/.
We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- **Online feedback rating system**—On any page at the Juniper Networks Technical Documentation site at [http://www.juniper.net/techpubs/index.html](http://www.juniper.net/techpubs/index.html), simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at [http://www.juniper.net/techpubs/feedback/](http://www.juniper.net/techpubs/feedback/).

- **E-mail**—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).
**Requesting Technical Support**

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.

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

1 September 2016—Revision 7, Junos OS Release 16.1R1—EX Series, MX Series, PTX Series, QFX Series, T Series, and Junos Fusion.


29 June 2016—Revision 1, Junos OS Release 16.1R1—MX Series, and Junos Fusion.