

Release Notes: Junos[®] OS Release 15.1X53-D592 for EX2300 and EX3400 Switches

November 14, 2019
Revision 1

Contents	Junos OS Release Notes for EX Series Switches 3
	What's New 3
	New Features in Release 15.1X53-D592 4
	New Features in Release 15.1X53-D591 4
	New Features in Release 15.1X53-D590 4
	New Features in Release 15.1X53-D58 4
	New Features in Release 15.1X53-D57 4
	New Features in Release 15.1X53-D55 4
	New Features in Release 15.1X53-D51 7
	New Features in Release 15.1X53-D50 7
	What's Changed 11
	Layer 2 Features 12
	Network Management and Monitoring 12
	Security 13
	System Management 13
	Known Limitations 13
	Class of Service 14
	Forwarding and Sampling 14
	Interfaces and Chassis 14
	Platform and Infrastructure 14

Routing Policy and Firewall Filters	15
Software Installation and Upgrade	15
Virtual Chassis	15
Open Issues	16
Infrastructure	16
Interfaces and Chassis	16
Network Management and Monitoring	17
Platform and Infrastructure	17
Virtual Chassis	18
Resolved Issues	18
Resolved Issues: Release 15.1X53-D592	19
Resolved Issues: Release 15.1X53-D591	19
Resolved Issues: Release 15.1X53-D590	20
Resolved Issues: Release 15.1X53-D59	22
Resolved Issues: Release 15.1X53-D58	25
Resolved Issues: Release 15.1X53-D57	27
Resolved Issues: Release 15.1X53-D55	29
Resolved Issues: Release 15.1X53-D52	31
Resolved Issues: Release 15.1X53-D51	31
Documentation Updates	33
Migration, Upgrade, and Downgrade Instructions	33
Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases	34
Finding More Information	35
Documentation Feedback	35
Requesting Technical Support	36
Self-Help Online Tools and Resources	36
Creating a Service Request with JTAC	37
Revision History	37

Junos OS Release Notes for EX Series Switches

IN THIS SECTION

- [What's New | 3](#)
- [What's Changed | 11](#)
- [Known Limitations | 13](#)
- [Open Issues | 16](#)
- [Resolved Issues | 18](#)
- [Documentation Updates | 33](#)
- [Migration, Upgrade, and Downgrade Instructions | 33](#)

These release notes accompany Junos OS Release 15.1X53-D592 for EX2300 and EX3400. They describe new and changed features, limitations, and known problems in the hardware and software.

What's New

IN THIS SECTION

- [New Features in Release 15.1X53-D592 | 4](#)
- [New Features in Release 15.1X53-D591 | 4](#)
- [New Features in Release 15.1X53-D590 | 4](#)
- [New Features in Release 15.1X53-D58 | 4](#)
- [New Features in Release 15.1X53-D57 | 4](#)
- [New Features in Release 15.1X53-D55 | 4](#)
- [New Features in Release 15.1X53-D51 | 7](#)
- [New Features in Release 15.1X53-D50 | 7](#)

Learn about new features introduced in Junos OS Release 15.1X53-D592 for the EX Series.

NOTE: The following EX Series platforms are supported in Junos OS Release 15.1X53-D5x: EX2300 and EX3400.

New Features in Release 15.1X53-D592

There are no new features or enhancements to existing features for EX Series in Junos OS Release 15.1X53-D592.

New Features in Release 15.1X53-D591

There are no new features or enhancements to existing features for EX Series in Junos OS Release 15.1X53-D591.

New Features in Release 15.1X53-D590

There are no new features or enhancements to existing features for EX Series in Junos OS Release 15.1X53-D590.

New Features in Release 15.1X53-D58

There are no new features or enhancements to existing features for EX Series in Junos OS Release 15.1X53-D58.

New Features in Release 15.1X53-D57

There are no new features or enhancements to existing features for EX Series in Junos OS Release 15.1X53-D57.

New Features in Release 15.1X53-D55

IN THIS SECTION

- [Hardware | 5](#)
- [Authentication and Access Control | 5](#)
- [Port Security | 7](#)
- [Virtual Chassis | 7](#)

Hardware

- **48-port EX2300 switch models**—Starting with Junos OS Release 15.1X53-D55, EX2300 switch models EX2300-48T and EX2300-48P with 48 built-in network ports with 10/100/1000 BASE-T connectors are available as fixed configuration switches that provide connectivity for low-density environments. The ports in EX2300-48P provide Power over Ethernet (PoE) or Power over Ethernet Plus (PoE+) on all network ports.

Authentication and Access Control

- **Central Web authentication (EX2300 and EX3400)**—Starting with Junos OS Release 15.1RX53-D55, you can configure central web authentication to redirect Web browser requests to a login page that requires the user to input a username and password. Upon successful authentication, the user is allowed to access the network. The login process is handled by a central Web authentication server, which provides scaling benefits over local Web authentication, also known as *captive portal*.

Central Web authentication is useful for providing network access to temporary users, such as visitors to a corporate site who are trying to access the network using devices that are not 802.1X-enabled. Web authentication can also be used as a fallback authentication method for regular network users who have 802.1X-enabled devices that fail authentication because of other issues, such as expired network credentials.

[See [Understanding Central Web Authentication](#).]

- **RADIUS-initiated changes to an authorized user session (EX2300 and EX3400)**—Starting with Junos OS Release 15.1X53-D55, EX2300 and EX3400 switches support changes to an authorized user session that are initiated by the authentication server. The server can send the switch a disconnect message to terminate the session or a Change of Authorization (CoA) message to modify the session authorization attributes. CoA messages are typically used to change data filters or VLANs for an authenticated host.

[See [Understanding RADIUS-Initiated Changes to an Authorized User Session](#).]

- **Flexible authentication order (EX2300 and EX3400)**—Starting with Junos OS Release 15.1RX53-D55, you can configure the order of authentication methods that the switch will use to authenticate an end device. By default, the switch will first attempt to authenticate using 802.1X authentication, then MAC RADIUS authentication, and then captive portal. You can override the default order of authentication methods by configuring the **authentication-order** statement to specify that the switch use either 802.1X authentication or MAC RADIUS authentication first. Captive portal must always be last in the order of authentication methods.

[See [Understanding Authentication on EX Series Switches](#).]

- **RADIUS accounting interim updates (EX2300 and EX3400)**—Starting with Junos OS Release 15.1RX53-D55, you can configure the switch to send periodic updates for a user accounting session at a specified interval to the accounting server. Interim accounting updates are included in the exchange of messages between the client and the accounting server. In RADIUS accounting, the client sends Accounting-Request messages to the server, which acknowledges receipt of the requests with

Accounting-Response messages. Interim accounting updates are sent in Accounting-Request messages with the Acct-Status-Type set to Interim-Update.

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

- **Support for multiple terms in a filter sent from the RADIUS server (EX2300 and EX3400)**—Starting with Junos OS Release 15.1X53-D55, you can use RADIUS server attributes to implement dynamic firewall filters with multiple terms on a RADIUS authentication server. These filters can be dynamically applied on all switches that authenticate supplicants through that server, eliminating the need to configure the same filter on multiple switches. You can define the filters directly on the server by using the Juniper-Switching-Filter attribute, which is a RADIUS attribute specific to Juniper Networks, also known as a *vendor-specific attribute (VSA)*. Filter terms are configured using one or more match conditions and a resulting action.

[See [Understanding Dynamic Filters Based on RADIUS Attributes.](#)]

- **EAP-PAP protocol support for MAC RADIUS authentication (EX2300 and EX3400)**—Starting with Junos OS Release 15.1X53-D55, you can configure the switch to use the Password Authentication Protocol (PAP) when authenticating clients with the MAC RADIUS authentication method. PAP transmits plaintext passwords over the network without encryption. It is required for use with Lightweight Directory Access Protocol (LDAP), which supports plaintext passwords for client authentication. This feature is configured by using the **authentication- protocol** CLI statement at the **[edit protocols dot1x authenticator interface interface-name mac-radius]** hierarchy level.

[See [Understanding Authentication on EX Series Switches.](#)]

Port Security

- **IPv6 router advertisement (RA) guard (EX3400)**—Starting with Junos OS Release 15.1X53-D55 for EX Series switches, IPv6 RA guard is supported on EX3400 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 are 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](#)].

Virtual Chassis

- **NSSU (EX3400)**—Starting with Junos OS Release 15.1X53-D55 for EX Series switches, EX3400 switches support the Non-Stop Software Upgrade feature. This support enables an NSSU upgrade from 15.1X53-D55 to a future release. You cannot upgrade from previous versions of 15.1X53 to 15.1X53-D55 using NSSU.

New Features in Release 15.1X53-D51

IN THIS SECTION

- [Hardware | 7](#)

Hardware

- Starting with Junos OS Release 15.1X53-D51, the DC-powered EX2300 switch model EX2300-24T-DC with 24 built-in network ports with 10/100/1000 BASE-T connectors is also available as a fixed configuration switch that provides connectivity for low-density environments.
- Starting with Junos OS Release 15.1X53-D51, the DC-powered EX3400 model EX3400-24T-DC switch with 24 built-in network ports with 10/100/1000 BASE-T connectors is also available as a fixed configuration switch that provides connectivity for low-density environments.

New Features in Release 15.1X53-D50

IN THIS SECTION

- [Hardware | 8](#)
- [High Availability | 9](#)

●	Interfaces and Chassis 9
●	Layer 2 Features 9
●	Layer 3 Features 9
●	Multicast Protocols 9
●	Network Management and Monitoring 10
●	Security 10
●	System Management 10
●	Traffic Management 11

Hardware

- **EX2300 switches**—Starting with Junos OS Release 15.1X53-D50, EX2300 switches are available as fixed configuration switches that provide connectivity for low-density environments. They are available in models with 12 or 24 built-in network ports with 10/100/1000 BASE-T connectors that provide Power over Ethernet (PoE) or Power over Ethernet Plus (PoE+) on all network ports (in PoE-capable models). The compact, fanless EX2300-C switches have 12 network ports.

EX2300-C switches have two 10-Gigabit Ethernet uplink ports that support 1-gigabit small form-factor pluggable (SFP) transceivers and 10-gigabit small form-factor pluggable plus (SFP+) transceivers. EX2300 switches except the EX2300-C switch model have four 10-Gigabit Ethernet uplink ports that support SFP and SFP+ transceivers. You can use these uplink ports as network ports or configure these ports as Virtual Chassis ports (VCPs) and use them to connect up to four switches by using SFP+ transceivers to form a *Virtual Chassis*.

- **EX3400 switches**—Starting with Junos OS Release 15.1X53-D50, EX3400 switches are available as fixed configuration switches that provide connectivity for low-density environments. They are available in models with 24 or 48 built-in network ports with 10/100/1000 BASE-T connectors that provide Power over Ethernet (PoE) or Power over Ethernet Plus (PoE+) on all network ports (in PoE-capable models).

EX3400 switches have four 10-Gigabit Ethernet uplink ports that support SFP transceivers and SFP+ transceivers and two 40-Gigabit Ethernet uplink ports that support quad small form-factor pluggable plus (QSFP+) transceivers. You can use these ports as network ports or as VCPs to connect up to ten switches to form one Virtual Chassis. The 40-Gigabit Ethernet uplink ports are configured as VCPs by default. To use these uplink ports as network ports, you must configure them as network ports. The 10-Gigabit Ethernet uplink ports are configured as network ports by default. To use these uplink ports as VCPs, you must configure them as VCPs.

High Availability

- **Graceful Routing Engine switchover (GRES), nonstop active routing and nonstop bridging**—High availability features refer to the hardware and software components that provide redundancy and reliability for network communications. EX2300 switches support GRES. EX3400 switches support GRES, nonstop active routing, and nonstop bridging.
- **Virtual Router Redundancy Protocol (VRRP) support**—VRRP enables you to provide alternative gateways for end hosts that are configured with static default routes. You can implement VRRP to provide a high availability default path to a gateway without the need to configure dynamic routing or router discovery protocols on end hosts.

Interfaces and Chassis

- **Link aggregation**—Link aggregation enables you to use multiple network cables and ports in parallel to increase link speed and redundancy.

Layer 2 Features

- **VLAN support**—VLANs enable you to divide one physical broadcast domain into multiple virtual domains.
- **Link Layer Discovery Protocol (LLDP) support**—LLDP enables a switch to advertise its identity and capabilities on a LAN, as well as receive information about other network devices.
- **Q-in-Q tunneling support**—This feature enables service providers on Ethernet access networks to extend a Layer 2 Ethernet connection between two customer sites. By using Q-in-Q tunneling, providers can also segregate or bundle customer traffic into fewer VLANs or different VLANs by adding another layer of 802.1Q tags. Q-in-Q tunneling is useful when customers have overlapping VLAN IDs, because the customer's 802.1Q (dot1Q) VLAN tags are prepended by the service VLAN (S-VLAN) tag.
- **Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP) support**—These protocols enable a switch to advertise its identity and capabilities on a LAN and receive information about other network devices.

Layer 3 Features

- **OSPF support**—The IPv4 OSPF protocol is an interior gateway protocol (IGP) for routing traffic within an autonomous system (AS). EX2300 and EX3400 switches support OSPFv1 and OSPFv2. You can configure OSPF at the **[edit protocols ospf]** hierarchy level.
- **Bidirectional Forwarding Detection (BFD) support for static routes and the OSPF, PIM, and RIP protocols**—BFD 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.

You can configure BFD for static routes and for the OSPF, PIM, and RIP protocols.

Multicast Protocols

- **Internet Group Management Protocol (IGMP) support**—IGMP manages the membership of hosts and routers in multicast groups. IP hosts use IGMP to report their multicast group memberships to any

immediately neighboring multicast routers. Multicast routers use IGMP to learn, for each of their attached physical networks, which groups have members.

- **IGMP snooping support**—IGMP snooping regulates multicast traffic in a switched network. With IGMP snooping enabled, a LAN switch monitors the IGMP transmissions between a host (a network device) and a multicast router, keeping track of the multicast groups and associated member interfaces. The switch uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces.

Network Management and Monitoring

- **SNMP support**—SNMP support includes versions 1, 2, and 3 for monitoring system activity.
- **System logging (syslog) support**—Syslog enables you to log system messages into a local directory on the switch or to a syslog server.
- **sFlow technology support**—This feature provides monitoring technology for high-speed switched or routed networks. You can configure sFlow technology to monitor traffic continuously at wire speed on all interfaces simultaneously. sFlow technology also collects samples of network packets, providing visibility into network traffic information. You configure sFlow monitoring at the **[edit protocols sflow]** hierarchy level. sFlow operational commands include **show sflow** and **clear sflow collector statistics**.
- **Port mirroring support**—Port mirroring copies packets entering or exiting a port or entering a VLAN and sends the copies to a local interface for local monitoring. You can use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on.

Security

- **Firewall filter support**—You can provide rules that define whether to accept or discard packets. You can use firewall filters on interfaces, VLANs, integrated routing and bridging (IRB) interfaces, link aggregation groups (LAGs), and loopback interfaces.
- **Policing support**—You can use policing to apply limits to traffic flow and to set consequences for packets that exceed those limits.
- **Storm control support**—You can enable the switch to monitor traffic levels and take a specified action when a specified traffic level—called the *storm control level*—is exceeded, preventing packets from proliferating and degrading service. You can configure a switch to drop broadcast and unknown unicast packets, shut down interfaces, or temporarily disable interfaces when a traffic storm occurs.

System Management

- **Login authentication using RADIUS and TACACS+**—You can use RADIUS and TACACS+ authentication to validate users who attempt to access the switch.
- **System utilization alarms support**—This feature provides system alarms to alert you of high disk usage in the **/var** partition on the switch. You can display these alarm messages by issuing the **show system alarms** operational mode command if the **/var** partition usage is higher than 75 percent. A usage level

between 76 and 90 percent indicates high usage and triggers a minor alarm condition, whereas a usage level over 90 percent indicates that the partition is full and triggers a major alarm condition.

Traffic Management

- **Class of service (CoS)**—When a packet traverses a switch, the switch provides the appropriate level of service to the packet using either default class-of-service(CoS) settings or CoS settings that you configure. On ingress ports, the switch classifies packets into appropriate forwarding classes and assigns a loss priority to the packets. On egress ports, the switch applies packet scheduling and any rewrite rules to re-mark packets.
- **Class-of-service (CoS) rewrite rules and classifier support**—You can use rewrite rules to set the value of the CoS bits within a packet header, and thereby alter the CoS settings of incoming packets. Packet classification maps incoming packets to a particular class-of-service (CoS) servicing level. You can use classifiers to map packets to a forwarding class and a loss priority and to assign packets to output queues based on the forwarding class.
- **Port scheduling with queue shaping support**—You can manage excess traffic and avoid congestion on a network interface where traffic might exceed the maximum port bandwidth. You can manage parameters such as transmit rate, shaping rate, and priority on each queue.

SEE ALSO

[Changes in Behavior and Syntax | 11](#)

[Known Behavior | 13](#)

[Known Issues | 16](#)

[Resolved Issues | 18](#)

[Documentation Updates | 33](#)

[Migration, Upgrade, and Downgrade Instructions | 33](#)

What's Changed

IN THIS SECTION

- [Layer 2 Features | 12](#)
- [Network Management and Monitoring | 12](#)
- [Security | 13](#)
- [System Management | 13](#)

See what changed in Junos OS Release 15.1X53-D592 for EX Series switches.

Layer 2 Features

- **Layer 2 Protocol Tunneling (L2PT) (EX2300 and EX3400 switches)**—Starting in Junos OS Release 15.1X53-D55, EX2300 and EX3400 switches support Layer 2 protocol tunneling (L2PT) using the **set protocols layer2-control mac-rewrite interface *interface-name* protocol** command. The CLI includes options to configure an interface to tunnel any of the following Layer 2 protocols: CDP, GVRP, IEEE 802.3AH, LACP, LLDP, MVRP, STP (as well as RSTP and MSTP), VSTP, and VTP.

See [Understanding Layer 2 Protocol Tunneling on EX Series Switches](#).

- **Configuration option for LLDP VLAN name type, length, and value (TLV) (EX3400)**—Starting in Junos OS Release 15.1X53-D59, you can configure the **vlan-name-tlv-option (name | vlan-id)** statement at the **[edit protocols lldp]** hierarchy level to select whether to transmit the VLAN name or simply the VLAN ID for the Link Layer Discovery Protocol (LLDP) VLAN name TLV when exchanging LLDP messages. By default, EX Series switches running Enhanced Layer 2 Software (ELS) transmit the VLAN ID for the LLDP VLAN name TLV, and the **show lldp detail** command displays the default string **vlan-vlan-id** for an interface's VLAN name in the **Vlan-name** output field. Switches that support the **vlan-name-tlv-option** statement behave the same as the default if you configure the **vlan-id** option with this statement. If you configure the **name** option, the switch transmits the VLAN name instead, and the **show lldp detail** command displays the VLAN name in the **Vlan-name** output field.

Network Management and Monitoring

- **Hard-coded RFC 3635 MIB OIDs updated (EX2300 and EX3400 switches)**—In Junos OS Release 15.1X53-D57, the following RFC 3635 MIB OIDs have been updated as default values:
 - dot3StatsFCSErrors and dot3HCStatsFCSErrors, framing errors
 - dot3StatsInternalMacReceiveErrors and dot3HCStatsInternalMacReceiveErrors, MAC statistics: Total errors (Receive)
 - dot3StatsSymbolErrors and dot3HCStatsSymbolErrors, code violations
 - dot3ControlFunctionsSupported, flow control
 - dot3PauseAdminMode, flow control
 - dot3PauseOperMode, auto-negotiation

See the [SNMP Explorer](#).

Security

- **Firewall warning message (EX2300 switches)**—Starting in Junos OS Release 15.1X53-D590, a warning message is displayed whenever a firewall term includes log or syslog with the accept filter action.

System Management

- **Increase in length of TACACS messages**—Starting in Junos OS Release 15.1X53-D59, the length of TACACS messages allowed on Junos OS devices has been increased from 8150 to 65535 bytes.

SEE ALSO

New and Changed Features	 3
Known Behavior	 13
Known Issues	 16
Resolved Issues	 18
Documentation Updates	 33
Migration, Upgrade, and Downgrade Instructions	 33

Known Limitations

IN THIS SECTION

- [Class of Service](#) | 14
- [Forwarding and Sampling](#) | 14
- [Interfaces and Chassis](#) | 14
- [Platform and Infrastructure](#) | 14
- [Routing Policy and Firewall Filters](#) | 15
- [Software Installation and Upgrade](#) | 15
- [Virtual Chassis](#) | 15

Learn about known limitations in this release for EX2300 and EX3400 switches. For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Class of Service

- EX2300 switches do not support CoS over integrated routing and bridging (IRB) interfaces.
- EX2300 switches support only TCP as a loss-priority protocol. The **any** option is not supported.
- On EX2300 and EX3400 switches, the **drop-profile-map loss-priority** statement does not display the **medium-low loss-priority** option.

Forwarding and Sampling

- On EX2300 and EX3400, SFLOW sampling does not work on egress traffic when the polling interval is configured as 0. [PR1185677](#)

Interfaces and Chassis

- On EX2300, when a filter having reject action is hit(IRACLv6), interface flaps could be seen. [PR1156553](#)
- Previously, the same IP address could be configured on different logical interfaces from different physical interfaces in the same routing instance (including master routing instance), but only one logical interface was assigned with the identical address after commit. There was no warning during the commit, only syslog messages indicating incorrect configuration. This issue is fixed and it is now not allowed to configure the same IP address (the length of the mask does not matter) on different logical interfaces. [PR1221993](#)

Platform and Infrastructure

- EX2300 switches do not support virtual routing and forwarding (VRF) instances on VPNs.
- On EX2300 and EX3400 switches, protocol hello interval for LACP, VRRP, and BFD must be configured to 2 seconds or more with dead interval not less than 6 seconds to prevent protocol flaps during CPU intensive operations events such as Routing Engine switchover, interface flaps and exhaustive data collection from the Packet Forwarding Engine.
- EX2300 switches do not support unicast RPF (uRPF).
- EX2300 switches do not support neighbor discovery inspection.
- On EX2300-48T switches, traffic loss is expected for line rate traffic with 64 byte frames on 10-gigabit interfaces.

- On EX2300 and EX3400 switches, when you perform multiple CLI upgrades, sometimes the upgrade fails with an **insufficient space** error. [PR1344512](#)
- In EX2300, transit ARP requests entering a port can get trapped to the CPU even if no IRB is configured on the VLAN. This can result in unnecessary ARP requests to the CPU and in extreme cases result in drops of genuine ARP requests in the ARP queue to CPU. [PR1365642](#)

Routing Policy and Firewall Filters

- EX3400 switches do not support filter-based forwarding (FBF) of IPv6 traffic.
- On EX3400, filter bind fails due to unavailability of tcam in the following scenario:
 - Filter with terms more than supported terms is configured and applied on ingress/egress of an interface.
 - Extra terms are removed and committed again.

Software Installation and Upgrade

- When the image is copied through FTP from a server to a switch, sometimes the ftpd WCPU might go high, causing the CLI to freeze for approximately 10 seconds. [PR1306286](#)
- On EX2300 and EX3400 switches, when you perform multiple CLI upgrades, sometimes the upgrade fails with an "insufficient space" error. [PR1344512](#)

Virtual Chassis

- **Automatic software update limitations (EX2300 and EX3400 Virtual Chassis)**—Automatic software updates are not supported on EX2300 or EX3400 Virtual Chassis running Junos OS Releases 15.1X53-D50 through 15.1X53-D52 when the target update release is Junos OS Release 15.1X53-D55 or later releases. Automatic software updates are supported within the range of release versions Junos OS Releases 15.1X53-D50 through 15.1X53-D52, or from Junos OS Release 15.1X53-D55 to later releases.

[See [Understanding Automatic Software Update on Virtual Chassis Member Switches.](#)]

- On an EX2300 Virtual Chassis, the **request system reboot all-members at now** command might reboot only that particular switch in the Virtual Chassis from which the command is issued. [PR1188016](#)

SEE ALSO

[New and Changed Features | 3](#)

[Changes in Behavior and Syntax | 11](#)

[Known Issues | 16](#)

[Resolved Issues | 18](#)

[Documentation Updates | 33](#)

[Migration, Upgrade, and Downgrade Instructions | 33](#)

Open Issues

IN THIS SECTION

- [Infrastructure | 16](#)
- [Interfaces and Chassis | 16](#)
- [Network Management and Monitoring | 17](#)
- [Platform and Infrastructure | 17](#)
- [Virtual Chassis | 18](#)

Learn about open issues in Junos OS Release 15.1X53-D592 for EX2300 and EX3400. For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

Infrastructure

- On EX3400 or EX2300 during ZTP with configuration and image upgrade with FTP as file transfer , image upgrade is successful but sometimes VMcore is observed. [PR1377721](#)

Interfaces and Chassis

- You might be unable to commit your configuration if you modify the subnet of an IP address on an IRB interface by using the **replace pattern** command. [PR1119713](#)
- On GRES switchover, VSTP port cost on AE interfaces might get changed, leading to topology change. [PR1174213](#)

Network Management and Monitoring

- On a EX2300 switch, the IfSpeed and IfHighSpeed MIB values might be incorrectly displayed during an SNMP get operation. [PR1326902](#)

Platform and Infrastructure

- If one interface configured with SP type (encapsulation extended-vlan-bridge/flexible-vlan-tagging) and another interface with Enterprise type (interface-mode) with same vlan-id, the traffic might not forward as expected through these two interfaces. [PR1309448](#)
- On EX3400 when me0 ports are connected between two EX3400 switches, the link does not come up. The link comes up when me0 is connected to network port. [PR1351757](#)
- On EX2300, when there is high rate of ARP request coming on a port, and same port has IRB enabled for multicast traffic , user might experience high latency while adding, deleting, and updating Multicast routes. [PR1358107](#)
- On EX2300, when watchdog is induced, the last reboot reason is shown as Swizzle Reboot. [PR1369924](#)
- On EX3400 switches, when LAG/LACP is configured with auto-negotiation disabled and speed is set 1G for links, a switch reboot might result in ports down on EX3400 side. [PR1369965](#)
- On Junos OS platforms with supporting dot1x, the dot1xd core-dumps might be seen when it receives the reply from the authd and reply length is less than 28 bytes. [PR1372421](#)
- On EX3400 Virtual Chassis -MACSEC does not come up after link flap where link is part of LACP and MACSEC is enabled on member link. [PR1378710](#)
- On rare occasions in EX2300-VC while performing GRES with a typical access security profile in campus/enterprise deployment we might see fxpc core. [PR1380451](#)
- EX2300 - pki-service daemon gets terminated on trying to clear security pki local-certificate system-generated. [PR1382774](#)
- Sometimes in EX2300-Virtual Chassis, uplink port with speed configured to 100m and auto-negotiation disabled, might not forward traffic after switch reboot. [PR1386906](#)
- EX3400 - SFP Rx power hi alarm/warning thresh is showing incorrect value in show interfaces diagnostics optics. [PR1395434](#)
- Occasionally, PKID might generate core files during **clear security pki local-certificate system-generated**. However, PKID is a stateless daemon that comes right back up after the core files and a new system self-signed certificate is generated as part of the PKI init process. So there is no loss of functionality due to the core files. [PR1461194](#)

Virtual Chassis

- On an EX2300 switch in a Virtual Chassis, a VCCP daemon restart might result in existing OSPF sessions over link aggregation interfaces being struck in init state. [PR1180055](#)

SEE ALSO

New and Changed Features	 3
Changes in Behavior and Syntax	 11
Known Behavior	 13
Resolved Issues	 18
Documentation Updates	 33
Migration, Upgrade, and Downgrade Instructions	 33

Resolved Issues

IN THIS SECTION

- [Resolved Issues: Release 15.1X53-D592](#) | [19](#)
- [Resolved Issues: Release 15.1X53-D591](#) | [19](#)
- [Resolved Issues: Release 15.1X53-D590](#) | [20](#)
- [Resolved Issues: Release 15.1X53-D59](#) | [22](#)
- [Resolved Issues: Release 15.1X53-D58](#) | [25](#)
- [Resolved Issues: Release 15.1X53-D57](#) | [27](#)
- [Resolved Issues: Release 15.1X53-D55](#) | [29](#)
- [Resolved Issues: Release 15.1X53-D52](#) | [31](#)
- [Resolved Issues: Release 15.1X53-D51](#) | [31](#)

Learn which issues were resolved in this release for EX2300 and EX3400 switches. For the most complete and latest information about known Junos OS defects, use the Juniper Networks online [Junos Problem Report Search](#) application.

This section lists the issues fixed in the Junos OS 15.1X53 releases for the EX2300 and EX3400 switches.

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

Resolved Issues: Release 15.1X53-D592

IN THIS SECTION

- [Infrastructure](#) | 19
- [Platform and Infrastructure](#) | 19

Infrastructure

- The dot1x might not work when dot1x is configured with isolated VLAN on one interface. [PR1404664](#)

Platform and Infrastructure

- [SIRT] Certain QFX and EX Series devices are vulnerable to 'Etherleak' memory disclosure in Ethernet padding data (CVE-2017-2304). [PR1063645](#)
- Ping does not go through device after WTR timer expires in ERPS scenario. [PR1132770](#)
- The TCP connection between ppmd and ppman might be dropped due to a kernel issue. [PR1401507](#)
- The upgrade of the PoE firmware might fail on EX3400. [PR1413802](#)
- Virtual Chassis might become unstable and FXPC core files when there are a lot of configured filter entries. [PR1422132](#)
- The delay in transmission of BPDUs after GRES might result in loss of traffic on EX2300 or EX3400 Virtual Chassis. [PR1428935](#)
- LED turns on even after power-off the Virtual Chassis members. [PR1438252](#)
- The DHCP snooping table might be cleared for VLAN ID 1 after adding a new VLAN ID to it. [PR1438351](#)

Resolved Issues: Release 15.1X53-D591

IN THIS SECTION

- [Layer 2 Features](#) | 20
- [Platform and Infrastructure](#) | 20
- [Routing Protocols](#) | 20

Layer 2 Features

- On EX2300/EX3400, if L2PT is configured and user wants to enable LLDP, then user needs configure LLDP individually on the port. Interface all option does not work. [PR1361114](#)

Platform and Infrastructure

- IGMP general query packets destined to 224.0.0.1 are sent back on the received interface, breaking the unicast connectivity. [PR1262723](#)
- EX2300 and EX3400 SFP-T interfaces might display an incorrect Half-Duplex mode status in the Link-partner field in **show interfaces extensive** output. [PR1357770](#)
- On EX3400-Virtual Chassis getting logs **Error tvp_status_led_set** and **Error:tvp_optics_diag_eeprom_read** for pic 1 and pic 2. [PR1389407](#)
- EX3400 Virtual Chassis - When an interface in a VC-member switch which is not master, is flapped, IGMP query packets 224.0.0.1 are sent to all the members ports except the master fpc. This causes the interface MAC for the flapped interface to be learned upstream. [PR1393405](#)
- EX2300 - Sometimes when interface-mode of a port is changed from Access to Trunk and reverted back to Access with switch options interface enabled for voip, Ethernet switching table does not populate. [PR1396422](#)

Routing Protocols

- On EX2300 and EX3400 Series, **firewall filter** configuration cannot perform packet matching on any IPv6 extension headers. This issue may allow IPv6 packets that should have been blocked to be forwarded. IPv4 packet filtering is unaffected by this vulnerability. See <https://kb.juniper.net/JSA10905> for details. [PR1346052](#)

Resolved Issues: Release 15.1X53-D590

IN THIS SECTION

- [Layer 2 Features | 20](#)
- [Network Management and Monitoring | 21](#)
- [Platform and Infrastructure | 21](#)

Layer 2 Features

- On EX2300 and EX3400 platforms, if L2TP is configured, protocol specific MACs are not displayed in the Ethernet switching table. There is no functional impact. [PR1361131](#)

- On EX2300 or EX3400, While configuring L2PT for tunneling LLDP, it is observed the LLDP packets are dropped at the L2PT NNI interface. Issue seen only first time the configuration is done and recovers with reboot. [PR1362173](#)

Network Management and Monitoring

- Event-policy generated traps are sent with UTC, even though time zone is defined under system hierarchy. [PR1380777](#)

Platform and Infrastructure

- Netconf syntax error reported if the resync character is split in multiple streams. [PR1161167](#)
- In Junos environment, after invoked or execution this RPC: `<rpc><get-configuration compare="rollback" format="text" rollback="0"/></rpc>`, the management daemon (MGD) might crash, SSH/console need to be reconnected. [PR1271024](#)
- On EX2300 and EX3400 platforms, all the DHCP-Reply or DCHP-Offer packets might be discarded in a VLAN which DHCP snooping is not enabled while DHCP snooping is running on other VLANs. As a result, all the DHCP client will not get an IP address from the DHCP server in that VLAN. [PR1345426](#)
- On EX2300 and EX3400 Series switches with SFP used, when the actual receiver signal power exceeds 0.21 mW, the output of the command **show interfaces diagnostics optics** might display an incorrect value for the field "Receiver signal average optical power". [PR1326642](#)
- On EX3400 and EX2300 Series platforms, IP directed broadcast traffic forwarding does not work (the statement **targeted-broadcast** is configured). This might result in some applications not working. [PR1331326](#)
- On EX2300 and EX3400 Series platforms, all the DHCP-Reply or DCHP-Offer packets might be discarded in a VLAN which DHCP snooping is not enabled while DHCP snooping is running on other VLANs. As a result, all the DHCP clients will not get an IP address from the DHCP server in that VLAN. [PR1345426](#)
- When EX2300 and EX3400 platforms are used as transit switches, the traffic sent out of an IRB interface might use original MAC address instead of the configured MAC address for the IRB. [PR1359816](#)
- The l2cpd process might crash and generate a core file if MVRP is configured and RSTP is enabled with **interface all** command. [PR1365937](#)
- Multicast router advertisement (RA) packets coming on a VLAN need to be flooded to interfaces of all FPCs belonging to the same VLAN. Packets when traversing through HighGig port (that connects different FPCs) need to hit hardware filter to transmit packets in other FPCs. In issue state, the filter is not applicable for the HighGig ports, so multicast RA packets do not traverse through other FPCs. [PR1370329](#)
- On EX2300 and EX3400 platform, unicast ARP packets loop might be observed on the interface where both destination and source MAC of the ARP packets are learned and have Dynamic ARP inspection (DAI) enabled. [PR1370607](#)
- On EX2300 and EX3400 Series switches which are acted as transit switches, NTP broadcast packet with source port 123 might hit the default firewall rule and be trapped to CPU but not flooded to VLANs. [PR1371035](#)

- When issuing command **>show pfe filter hw summary** there might be an issue where counters are showing negative values Group Group-ID Allocated Used Free
----- > Ingress filter groups: iRACL group 33
128 64 64 iVACL group 29 256 173 83 iPACL group 25 128 168 -40 <- This issue is cosmetic as hardware programming for port based access list is working fine, TCAM slices were allocated but the counter was not updated properly causing negative value to appear. [PR1375022](#)
- In EX2300/EX3400 Virtual-Chassis environment, all interfaces belonging to certain FPC might go down after multiple GRES. When this happens, all the ports on the FPC are not seen or usable. [PR1379790](#)
- EX2300 interface configured with Q-in-Q (flexible-vlan-tagging) might experience issues with **host bound traffic** (traffic ingressing the interface destined to the Routing Engine / CPU) after the EX has been rebooted. [PR1387039](#)
- EX2300 - VOIP vlan are not sent through MVRP protocol and when the interface is configured for VOIP vlan, it also stops sending the DATA vlan that is configured under the same interface. [PR1394846](#)

Resolved Issues: Release 15.1X53-D59

IN THIS SECTION

- [Layer 2 Features | 22](#)
- [High Availability \(HA\) and Resiliency | 24](#)
- [Infrastructure | 24](#)
- [Interfaces and Chassis | 24](#)
- [Platform and Infrastructure | 24](#)
- [Routing Protocol | 25](#)
- [Subscriber Access Management | 25](#)
- [User Interface and Configuration | 25](#)

Layer 2 Features

- On EX2300, EX3400 switches, if a trunk port is deleted and then reconfigured as an access port in the same commit, the Layer 2 address learning daemon (l2ald) might generate a core file. [PR1105255](#)
- Customer might see JDHCP core file generated with DHCP relay configured. The issue can be seen after the ungraceful reboot of the VC. The DHCP service shall work normal after restarting the DHCP process currently running. [PR1190258](#)
- Memory leak in JDHCP during dhcp session RELEASE/BIND. [PR1181723](#)

- After the MACsec session flaps, data traffic sent over the MACsec-enabled link might not be properly received and the receiving device might report the received frames as "framing errors" in the output of show interfaces command. [PR1269229](#)
- On EX Series standalone switches or their Virtual Chassis with dot1x configured, there will be memory leaks for PNACAUTH in dot1xd. Once the memory block of PNACAUTH used by dot1xd grows to its limit size, the switch may not process clients' authentication further and results in dot1x clients reauthenticating constantly. The dot1xd process always runs irrespective of configuration and as part of its initialization it tries connection with authd; if authd is not running, then there is a memory leak in dot1xd. [PR1313578](#)
- When the switch is configured for dot1x multiple supplicant mode, a MAC move within the VLAN will result in traffic getting dropped till the MAC learned on the previous port ages out. [PR1329654](#)
- IP Directed broadcast traffic forwarding does not work on EX3400/EX2300. Applications such as Wakeup-on-lan. [PR1331326](#)
- On an EX2300-48P and EX2300-48T, the port ge-0/0/16-23 does not advertise a 10-Mbps speed. It advertises only 100 and 1000-Mbps speeds. [PR1331357](#)
- EX3400/EX2300 switches incorrectly flood unicast ARP replies in the VLAN when Dynamic ARP inspection is configured. [PR1331928](#)
- On an EX2300-48T switch, the output of the command **show chassis power-budget-statistics** might display an incorrect value for the Base power reserved field. [PR1333032](#)
- Redirect message sent from EX Switch even when no-redirect is set for the specified interface [PR1333153](#)
- On the EX2300, sFlow sampling is not accurate if the sample-rate is configured less than 256. This might cause the inaccurate monitoring to network traffic. [PR1333765](#)
- On EX2300/EX3400 platforms, when the bulk of MAC notifications are received along with 'interface-mac-limit' configuration changes, the device might stop learning the MAC address, and the MAC address might display with the "Hit Pending" status. [PR1341518](#)
- On EX2300/EX3400 platforms, the Packet Forwarding Engine manager (fxpc) process might crash when a firewall filter is applied on a VLAN. [PR1342783](#)
- On EX2300/EX3400 platforms, Packet Forwarding Engine manager (FXPC) might spike to 90% on an idle chassis if you enable accept-source-mac on an interface. [PR1345978](#)
- Over temperature traps erroneously sent by EX2300/EX3400. [PR1348836](#)
- There is a difference in the behavior of tagging once you remove an interface previously configured in an interface range and part of a VLAN. When the removed interface is configured with another VLAN and is configured as an access port, it still shows up as a tagged interface and drops all untagged traffic. [PR1349712](#)
- An EX2300 or EX3400 L2PT LACP MAC rewrite might send duplicate LACP BPDUs with both GBPT and LACP destination MACs exiting the PE. There is no service impact. [PR1350329](#)

- On EX2300-48T/48P platforms with Equal Cost Multipath (ECMP) next-hops configured, after a switch reboots, the ECMP group might only be created on Packet Forwarding Engine (PFE) unit 0. The transit traffic will only be forwarded towards that next-hop and it will not be forwarded if the traffic ingress on Packet Forwarding Engine (PFE) unit 1. [PR1351418](#)
- EX2300s may incorrectly drop OSPF traffic when the following are configured: Q-in-Q tunneling is configured; an lo0 interface is configured and a firewall filter is applied to the lo0 interface. [PR1355111](#)

High Availability (HA) and Resiliency

- In a rare scenario, GRES might not reach the ready state and might fail to start, because the Routing Engine does not receive the state ack message from the Packet Forwarding Engine after performing GRES. This is a timing issue. It might also stop Routing Engine resource releasing and then cause resource exhausting. [PR1236882](#)

Infrastructure

- When a VLAN is configured on all switches in a ring topology, a traffic loop might occur after the VLAN is removed from one of the switches. [PR1229744](#)
- On EX Series switches, CoS (for example: rewrite rules) are unbound from the IFL (logical interface) when deleting ISIS interface and hence device is not marking traffic correctly. [PR1239827](#)
- On EX3400 switches, even if an interface is disabled or a cable is unplugged, the interface LED status might still stay green. [PR1329903](#)

Interfaces and Chassis

- When clients are authenticated with dynamic VLAN assignment on an 802.1X-enabled interface, if they are connected/disconnected within a short time (within sub-seconds), the logical interface and the bridge domain or VLAN might remain in a problematic state, thus cause the clients to be denied when accessing the network. [PR1230073](#)
- After adding or deleting a VLAN to an interface an FXPC generates a core file followed by an FPC restart. [PR1334850](#)
- Some PoE devices may not receive PoE power from an EX2300 or an EX3400 due to a false report of Underload Latch. [PR1345234](#)

Platform and Infrastructure

- An unauthenticated root login may allow upon reboot when a commit script is used. A commit script allows a device administrator to execute certain instructions during commit, which is configured under the [system scripts commit] stanza. Please Refer to <https://kb.juniper.net/JSA10835> for more information. [PR1179601](#)
- Junos: Unauthenticated Remote Code Execution through J-Web interface (CVE-2018-0001); Refer to <https://kb.juniper.net/JSA10828> for more information. [PR1269932](#)
- An l2cpd core-dump might be seen if the interface is disabled under VSTP and enabled under RSTP causing inconsistency in spanning-tree. [PR1317908](#)

- EX3400 CPU might hog when continuous Telnet EC commands are sent on more than 75 concurrent telnet sessions. This may lead to slowness in CLI response. [PR1331234](#)
- On EX2300 and EX3400 switches, unicast ARP packets that are not destined to the switch routed interfaces are copied to CPU in addition to forwarding in HW. This will update the ARP cache on the routing engine. [PR1332463](#)
- In an MSTP scenario when the character size of MSTP region name exceeds 31 characters, any commit may trigger MSTP work abnormally even if the configuration change does not relate to MSTP. [PR1342900](#)

Routing Protocol

- RPD might crash on the routers with a core file. [PR1144112](#)

Subscriber Access Management

- On EX2300 and EX3400 switches, the dot1x user might fail to authenticate with a RADIUS server if the connection to the RADIUS server bounced. [PR1338993](#)

User Interface and Configuration

- The mgd process might crash when you execute **load override** command. [PR1153392](#)
- The mgd might crash if an IRB interface is included as part of an interface-range configuration. [PR1186156](#)

Resolved Issues: Release 15.1X53-D58

IN THIS SECTION

- [Infrastructure | 25](#)
- [Interfaces and Chassis | 26](#)
- [Layer 2 Features | 26](#)
- [Platform and Infrastructure | 26](#)
- [Port Security | 26](#)
- [Routing Protocols | 27](#)
- [Software Installation and Upgrade | 27](#)

Infrastructure

- The statistics info of em0 is 0 when checking by SNMP or CLI show command. [PR1188103](#)
- On an EX2300-48 switch that has two Packet Forwarding Engine forwarding ASICs (unit-0 for ports ge-0/0/24-47 and unit-1 for ports ge-0/0/0-23), MAC addresses learned on ports ge-0/0/24-47 are correctly updated in the Ethernet-switching table on the Routing Engine, but the hardware table on the

Packet Forwarding Engine unit-1 is not updated. Therefore, packets destined to the MAC address learned via ports ge-0/0/24–47 and traffic ingressing on ports ge-0/0/0–23 are treated as unknown unicast and flooded in the respective VLAN. However, packets destined for these MAC addresses but ingressing on ports ge-0/0/24–47 are correctly forwarded as unicast.

[PR1321612](#)

Interfaces and Chassis

- On EX3400 VC, the port with PoE enabled (i.e., 'set poe interface ge-1/0/1') may not come up after reboot of the Line card member. [PR1312983](#)

Layer 2 Features

- On EX2300 and EX3400 switches, access ports might incorrectly send VLAN tagged traffic. The problem is usually triggered by PVLAN configuration or having VLAN re-write configuration. [PR1315206](#)
- MAC moves might not happen on an EX2300 VC when a client moves from one port to another port within the VLAN. [PR1321835](#)

Platform and Infrastructure

- A sustained sequence of different types of normal transit traffic can trigger a high CPU consumption denial of service condition in the Junos OS register and schedule software interrupt handler subsystem when a specific command is issued to the device. [PR1145306](#)
- During a reboot of an EX2300 or EX3400 switch, the boot logs are not displayed on the mini-USB console even though the CLI command **set system ports auxiliary port-type mini-usb** is configured. The logs are displayed only on the serial console. The mini-USB console becomes active only when the system reaches the login prompt. [PR1192388](#)
- On EX3400 Virtual Chassis, issuing a **load replace terminal** CLI command and attempting to replace the interface stanza in the same operation might terminate the user CLI session. [PR1293587](#)
- Transit ARP traffic is sent to the host CPU when Dynamic ARP Inspection is configured and can potentially drop ARP replies destined to the switch when there is a large VLAN with multiple hosts. [PR1319891](#)
- The PHP process on the switch might run at a high CPU utilization when the configuration is committed via J-Web. [PR1328323](#)

Port Security

- Malicious LLDP crafted packet leads to privilege escalation, denial of service (CVE-2018-0007). Refer to <https://kb.juniper.net/JSA10830> for more information. [PR1252823](#)
- On an EX2300-48 port switch the syslog messages might contain messages like "fpc0 ifd null, port 28". These messages do not have any functional impact since port 28 is not the front panel port but the internal port on each forwarding ASIC. [PR1295711](#)

Routing Protocols

- Junos OS: The rpd might crash due to malformed Border Gateway Protocol (BGP) UPDATE packet (CVE-2018-0020). Refer to <https://kb.juniper.net/JSA10848> for more information. [PR1299199](#)

Software Installation and Upgrade

- On EX3400-VC, CLI image upgrade from Junos OS Release 15.1X53 to Junos OS Release 18.1R1 might fail with the error message "ERROR: Failed to add Junos-". [PR1317425](#)

Resolved Issues: Release 15.1X53-D57

IN THIS SECTION

- [Authentication and Access Control | 27](#)
- [Infrastructure | 27](#)
- [Interfaces and Chassis | 28](#)
- [J-Web | 28](#)
- [Layer 2 Features | 28](#)
- [Multicast Protocols | 28](#)
- [Network Management and Monitoring | 28](#)
- [Platform and Infrastructure | 28](#)
- [Port Security | 28](#)
- [Routing Protocols | 29](#)
- [Software Installation and Upgrade | 29](#)
- [Virtual Chassis | 29](#)

Authentication and Access Control

- An EX3400 Virtual Chassis might stop communicating with the RADIUS server when a large number of subscribers log in or log out. [PR1287442](#)

Infrastructure

- On EX2300, output of **show ethernet-switching table persistent-learning | display json or xml** is malformed. [PR1271144](#)
- During a commit sequence on EX2300, a log message with an incorrect number for available space for TCAM entries is displayed. [PR1287860](#)
- Issues are seen during conversion from Junos OS Release 15.1X53-D56 to SNOS. [PR1289809](#)

- EX2300 and EX3400 switches get an invalid system date when powered on. [PR1289924](#)
- On EX2300 and EX3400 Virtual Chassis, IP routing fails for destination routes with prefix length 32 or 128 when they point to ECMP next-hops. [PR1305462](#)

Interfaces and Chassis

- On EX2300, the **interface-range** command cannot be used to set speed and auto-negotiation properties for a group of interfaces. [PR1258851](#)

J-Web

- On EX2300 and EX3400 J-Web allows configuration of **source-address-filter**. [PR1281290](#)
- On EX3400, the PHP process consumes 100% of the CPU load during VLAN-ID list creation via a J-Web session. [PR1289943](#)

Layer 2 Features

- VLAN configuration changes causing EX2300 and EX3400 instability and traffic loss. [PR1282438](#)
- MAC addresses learned on AE interfaces do not age out on EX2300 Virtual Chassis running Junos OS Release 15.1X53-D55.5. [PR1288109](#)
- On EX3400, L2PT **mac re-write** is not supported for other vendor's PVST protocol. [PR1294340](#)

Multicast Protocols

- EX3400 Virtual Chassis has tail drops on multicast queues due to incorrect shared buffer programming. [PR1269326](#)

Network Management and Monitoring

- Real-time performance monitoring (RPM) probe-clients for ICMP or UDP might not work for EX2300 and EX3400 switches. [PR1188841](#)

Platform and Infrastructure

- On EX3400 and EX2300, after creation of recovery snapshot, SSH/Telnet login is unsuccessful from OAM volume. [PR1191356](#)

Port Security

- If an EX2300 switch is configured with the **interface-mac-limit** statement, the switch does not forward DHCP Offer packets from the server to the client. [PR1239633](#)
- JDHCPD cores frequently on EX3400 Virtual Chassis with **dhcp-security option-82** enabled. [PR1271427](#)
- DHCP relay over IRB can generate a jdhcpd core file while the switch is performing IP binding. [PR1272646](#)
- On EX3400, MACsec may not work on a 10G interface after a switch reboot. [PR1276730](#)
- EX3400 Virtual Chassis DHCP relay functionality might be affected when multiple monitoring sessions are opened through Junos Space. [PR1292112](#)

Routing Protocols

- OSPF neighbors might not converge when using MD5 on EX2300 and EX3400 switches. [PR1269572](#)

Software Installation and Upgrade

- On an EX3400 Virtual Chassis, during a nonstop software upgrade (NSSU), traffic drop might drop for more than 5 seconds for both Layer 2 and Layer 3 for the following protocols: multicast, Multiple Spanning Tree Protocol, Ethernet Ring Protection, and OSPFv3. [PR1224987](#)
- On an EX2300 Virtual Chassis, when you upgrade the software using the CLI, the device might go into the debug (DB) mode with the following error message: **Fatal kernel mode data abort: 'Alignment Fault' on read**. [PR1237863](#)

Virtual Chassis

- On an EX2300 switch in a Virtual Chassis, a VCCP daemon restart might result in existing OSPF sessions over link aggregation interfaces being struck in the Init state. [PR1180055](#)

Resolved Issues: Release 15.1X53-D55

IN THIS SECTION

- [Class of Service | 30](#)
- [High Availability | 30](#)
- [Layer 2 Features | 30](#)
- [Layer 3 Features | 30](#)
- [Platform and Infrastructure | 30](#)
- [Routing Protocols | 31](#)
- [Virtual Chassis | 31](#)

Class of Service

- On EX2300 switches, a packet loss priority (PLP) of medium-low is not supported for firewall filter configurations. [PR1180586](#)

High Availability

- DHCP renew or release packets might not be forwarded to the server when the EX2300 switch acts as a VRRP node. [PR1157056](#)

Layer 2 Features

- If MAC move limit is configured to drop traffic, EX Series switches might forward traffic instead of dropping traffic when the MAC move limit is exceeded. [PR1105372](#)
- On EX3400 and EX2300 switches, for the **mac-move-limit** statement, the **drop** and **drop-and-log** actions might not work. [PR1178693](#)
- On EX2300 and EX3400 switches, the **hash-mode** option is not available at the **[edit forwarding-options enhanced-hash-key]** hierarchy level. [PR1188866](#)
- On EX3400 and EX2300 switches, LLDP, LACP, and MVRP protocol options are not available under the **mac-rewrite** configuration statement. [PR1189353](#)

Layer 3 Features

- On an EX2300 switch, if the only configured route is a static default route, transit traffic destined to IP addresses that belong to subnets 128.0.0.1 to 191.255.255.254 are dropped. [PR1220078](#)

Platform and Infrastructure

- On an EX3400 switch, CLI upgrades might fail with an **insufficient space** error. [PR1148911](#)
- The EX3400 switch might shift to debug mode prompt or initiate an autoreboot after multiple reboots and switchovers. [PR1172524](#)
- EX2300 and EX3400 switches do not support VRRP authentication. [PR1172775](#)
- On EX3400 switches, the console response might become slow when ARP requests are sent at five percent of the line rate to the management interface. [PR1181891](#)
- On EX3400 switches, high CPU utilization caused by the fxpc process might also increase the latency (up to 100 ms) of traffic directed to the Routing Engine. [PR1230716](#)

Routing Protocols

- Unicast reverse-path forwarding is not supported on the EX2300 switch. [PR1151632](#)

Virtual Chassis

- In an EX3400 Virtual Chassis with two members, you might see the Routing Engine become unresponsive for up to 10 minutes while displaying the error message **kernel: jlock hog timer expired: jlock** acquired followed by additional kernel error messages; eventually the Virtual Chassis recovers on its own. [PR1235994](#)

Resolved Issues: Release 15.1X53-D52

IN THIS SECTION

- [Infrastructure | 31](#)

Infrastructure

- On EX2300 and EX3400 platforms, if the switch has been powered off for a couple of days, when you power it on, it boots with the default date of 1970-01-01. If NTP is configured on the switch at this time, the system clock might be set to an incorrect date—for example, 2038-01-01—which results in all protocols and timer-related functionality being affected. [PR1215296](#)

Resolved Issues: Release 15.1X53-D51

IN THIS SECTION

- [Class of Service | 32](#)
- [Infrastructure | 32](#)
- [Layer 2 Features | 32](#)
- [Layer 3 Protocols | 32](#)
- [Network Management | 32](#)
- [Virtual Chassis | 32](#)

Class of Service

- On EX3400 switches, CoS rewrite does not work on IRB interfaces. [PR1190361](#)

Infrastructure

- EX2300 switches do not support the Energy Efficient Ethernet (EEE) feature. [PR1178790](#)
- On EX3400 and EX2300 switches, the **request system zeroize media** command might not erase USB snapshot. [PR1183830](#)
- On EX3400 switches, the output of the **show macsec statistics** command might not display MACsec counter details. [PR1189042](#)
- On an EX3400 switch, if N+N PSU redundancy is configured, the switch might not revert to the N+0 mode. [PR1191731](#)
- On EX3400 and EX2300 switches, when the client is authenticated in either dynamic, server-fail, server-reject, or guest VLAN multiple supplicant modes, ping failures might be seen between the client and switch. [PR1192363](#)

Layer 2 Features

- On EX2300 switches, rate-limiting is observed on 10-gigabit ports after a storm control configuration is removed. [PR1189027](#)

Layer 3 Protocols

- On EX2300 and EX3400 switches, LLDP neighbors might not be formed over Layer 3 tagged interfaces. [PR1190585](#)

Network Management

- On EX2300 and EX3400 switches, sFlow sampling might not work for egress traffic. [PR1185677](#)

Virtual Chassis

- On an EX3400 switch, the virtual management Ethernet (VME) interface might not be reachable after a reboot or switchover. As a workaround, enter the **ifconfig me0 down** command at the shell prompt. [PR1187433](#)
- In an EX3400 Virtual Chassis with two members, you might see the Routing Engine become unresponsive for up to 10 minutes while displaying the error message **kernel: jlock hog timer expired: jlock** acquired followed by additional kernel error messages; eventually the Virtual Chassis recovers on its own. [PR1235994](#)

SEE ALSO

[New and Changed Features | 3](#)

[Changes in Behavior and Syntax | 11](#)

Known Behavior 13
Known Issues 16
Documentation Updates 33
Migration, Upgrade, and Downgrade Instructions 33

Documentation Updates

There are no errata or changes in Junos OS Release 15.1X53-D592 documentation for the EX Series.

SEE ALSO

New and Changed Features 3
Changes in Behavior and Syntax 11
Known Behavior 13
Known Issues 16
Resolved Issues 18
Migration, Upgrade, and Downgrade Instructions 33

Migration, Upgrade, and Downgrade Instructions

IN THIS SECTION

- [Upgrade and Downgrade Support Policy for Junos OS Releases and Extended End-Of-Life Releases | 34](#)

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 and Extended End-Of-Life Releases

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

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

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

For information about software installation and upgrade, see the [Installation and Upgrade Guide](#).

NOTE: : EX2300 or EX3400 switches running Junos OS Software Release 15.1X53-D57 or earlier revisions cannot be directly upgraded via CLI to Junos OS Software Release 18.1R1 because of configuration incompatibilities between the two releases related to the uplink port configurations. For example: Any configuration having interfaces on the uplink module (xe-0/2/*) will throw errors during the upgrade process. To work around this problem, please specify the validate option in the upgrade command to check for these errors, then remove the configuration that results in the errors, and use the no-validate option to do the upgrade.

Alternately, an intermediate upgrade to 15.1X53-D58 can be performed by keeping the configuration intact and then a subsequent upgrade to 18.1R1 is possible.

SEE ALSO

[New and Changed Features | 3](#)

[Changes in Behavior and Syntax | 11](#)

[Known Behavior | 13](#)

[Known Issues | 16](#)

[Resolved Issues | 18](#)

[Documentation Updates | 33](#)

Finding More Information

- **Feature Explorer**—Determine the features supported on MX Series, PTX Series, QFX Series devices. The Juniper Networks Feature Explorer is a Web-based app that helps you to explore and compare Junos OS feature information to find the right software release and hardware platform for your network. <https://pathfinder.juniper.net/feature-explorer/>
- **PR Search Tool**—Keep track of the latest and additional information about Junos OS open defects and issues resolved. prsearch.juniper.net.
- **Hardware Compatibility Tool**—Determine optical interfaces and transceivers supported across all platforms. apps.juniper.net/hct/home

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

- **Juniper Networks Compliance Advisor**—Review regulatory compliance information about [Common Criteria](#), [FIPS](#), [Homologation](#), [RoHS2](#), and [USGv6](#) for Juniper Networks products. apps.juniper.net/compliance/.

Documentation Feedback

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

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

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <https://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <https://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: <https://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <https://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <https://kb.juniper.net/>
- Download the latest versions of software and review release notes: <https://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <https://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <https://www.juniper.net/company/communities/>
- Create a service request online: <https://myjuniper.juniper.net>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Creating a Service Request with JTAC

You can create a service request with JTAC on the Web or by telephone.

- Visit <https://myjuniper.juniper.net>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <https://support.juniper.net/support/requesting-support/>.

Revision History

14 November 2019—Revision 1, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D592

20 May 2019—Revision 1, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D591

21 November 2018—Revision 1, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D590

24 July 2018—Revision 2, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D59—updates to Known Issues and Resolved Issues

25 June 2018—Revision 1, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D59

12 February 2018—Revision 1, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D58

17 November 2017—Revision 2, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D57—update to Known Issues

21 September 2017—Revision 1, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D57

11 July 2017—Revision 4, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D55—update to Changes in Behavior and Syntax

25 May 2017—Revision 3, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D55—update to Known Behavior

12 January 2017—Revision 2, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D55—update to Resolved Issues

5 January 2017—Revision 1, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D55

11 October 2016—Revision 1, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D52

28 September 2016—Revision 1, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D51

9 June 2016—Revision 1, Junos OS for EX2300 and EX3400 Switches, Release 15.1X53-D50

Copyright © 2019 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

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