

# Release Notes: Junos<sup>®</sup> OS Release 15.1X53-D58 for EX2300 and EX3400 Switches

February 12, 2018  
Revision 1

## Contents

Junos OS Release Notes for EX Series Switches . . . . .	3
New and Changed Features . . . . .	3
New Features in Release 15.1X53-D58 . . . . .	3
New Features in Release 15.1X53-D57 . . . . .	3
New Features in Release 15.1X53-D55 . . . . .	3
New Features in Release 15.1X53-D51 . . . . .	5
New Features in Release 15.1X53-D50 . . . . .	6
Changes in Behavior and Syntax . . . . .	10
Layer 2 Features . . . . .	10
Known Behavior . . . . .	10
Class of Service . . . . .	11
Platform and Infrastructure . . . . .	11
Routing Policy and Firewall Filters . . . . .	11
Software Installation and Upgrade . . . . .	11
Virtual Chassis . . . . .	11
Known Issues . . . . .	12
Authentication and Access Control . . . . .	13
EVPNs . . . . .	13
Forwarding and Sampling . . . . .	13
Infrastructure . . . . .	13
Interfaces and Chassis . . . . .	13
Layer 2 Features . . . . .	13
Platform and Infrastructure . . . . .	14
Port Security . . . . .	14
Routing Protocols . . . . .	14
Software Installation and Upgrade . . . . .	15
User Interface and Configuration . . . . .	15
Virtual Chassis . . . . .	15

Resolved Issues . . . . .	15
Resolved Issues: Release 15.1X53-D58 . . . . .	15
Resolved Issues: Release 15.1X53-D57 . . . . .	17
Resolved Issues: Release 15.1X53-D55 . . . . .	19
Resolved Issues: Release 15.1X53-D52 . . . . .	20
Resolved Issues: Release 15.1X53-D51 . . . . .	20
Documentation Updates . . . . .	21
Migration, Upgrade, and Downgrade Instructions . . . . .	22
Upgrade and Downgrade Support Policy for Junos OS Releases . . . . .	22
Product Compatibility . . . . .	23
Hardware Compatibility . . . . .	23
Documentation Feedback . . . . .	23
Requesting Technical Support . . . . .	24
Self-Help Online Tools and Resources . . . . .	24
Opening a Case with JTAC . . . . .	24
Revision History . . . . .	25

---

## Junos OS Release Notes for EX Series Switches

---

These release notes accompany Junos OS Release 15.1X53-D58 for EX2300 and EX3400. They describe new and changed features, limitations, and known problems in the hardware and software.

- [New and Changed Features on page 3](#)
- [Changes in Behavior and Syntax on page 10](#)
- [Known Behavior on page 10](#)
- [Known Issues on page 12](#)
- [Resolved Issues on page 15](#)
- [Documentation Updates on page 21](#)
- [Migration, Upgrade, and Downgrade Instructions on page 22](#)
- [Product Compatibility on page 23](#)

### New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Releases 15.1X53-D5x 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-D58 on page 3](#)
  - [New Features in Release 15.1X53-D57 on page 3](#)
  - [New Features in Release 15.1X53-D55 on page 3](#)
  - [New Features in Release 15.1X53-D51 on page 5](#)
  - [New Features in Release 15.1X53-D50 on page 6](#)

---

#### 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

---

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

### **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

- **Hardware**

### 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

---

- [Hardware](#)
- [High Availability](#)
- [Interfaces and Chassis](#)
- [Layer 2 Features](#)
- [Layer 3 Features](#)
- [Multicast Protocols](#)
- [Network Management and Monitoring](#)
- [Security](#)
- [System Management](#)
- [Traffic Management](#)

### 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 on page 10](#)
  - [Known Behavior on page 10](#)
  - [Known Issues on page 12](#)
  - [Resolved Issues on page 15](#)
  - [Documentation Updates on page 21](#)
  - [Migration, Upgrade, and Downgrade Instructions on page 22](#)

- [Product Compatibility on page 23](#)

## 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 15.1X53-D58 for EX2300 and EX3400 switches.

- [Layer 2 Features on page 10](#)

### 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](#).

- See Also**
- [New and Changed Features on page 3](#)
  - [Known Behavior on page 10](#)
  - [Known Issues on page 12](#)
  - [Resolved Issues on page 15](#)
  - [Documentation Updates on page 21](#)
  - [Migration, Upgrade, and Downgrade Instructions on page 22](#)
  - [Product Compatibility on page 23](#)

## Known Behavior

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 15.1X53-D58 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](#)
- [Platform and Infrastructure](#)
- [Routing Policy and Firewall Filters](#)
- [Software Installation and Upgrade](#)
- [Virtual Chassis](#)

---

### 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.

---

### Platform and Infrastructure

---

- EX2300 switches do not support virtual routing and forwarding (VRF) instances on VPNs.
- EX2300 and EX3400 switches do not support IPv4 or IPv6 source guard.
- On EX2300 and EX3400 switches, protocol hello timers for LACP, VRRP, and BFD must be configured to more than 2 seconds to prevent protocol flaps during system events such as Routing Engine switchover and interface flaps.
- 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.

---

### Routing Policy and Firewall Filters

---

- EX3400 switches do not support filter-based forwarding (FBF) of IPv6 traffic.
- EX2300 switches do not support a combination of (router) firewall filters, ingress port firewall filters, and ingress VLAN firewall filters on the same interface.
- On EX3400 switches, filter bind might fail because of TCAM unavailability when:
  - A filter that has more than the supported number of terms is applied on an ingress or egress interface
  - The extra terms are removed from such a filter and the configuration is committed again

As a workaround, unbind the filter and bind it again to the interface. [PR1181501](#)

---

### 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](#)

---

### 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 on page 3](#)
  - [Changes in Behavior and Syntax on page 10](#)
  - [Known Issues on page 12](#)
  - [Resolved Issues on page 15](#)
  - [Documentation Updates on page 21](#)
  - [Migration, Upgrade, and Downgrade Instructions on page 22](#)
  - [Product Compatibility on page 23](#)

## Known Issues

This section lists the known issues in hardware and software in Junos OS Release 15.1X53-D58 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.

- [Authentication and Access Control](#)
- [EVPNs](#)
- [Forwarding and Sampling](#)
- [Infrastructure](#)
- [Interfaces and Chassis](#)
- [Layer 2 Features](#)
- [Platform and Infrastructure](#)
- [Port Security](#)
- [Routing Protocols](#)
- [Software Installation and Upgrade](#)
- [User Interface and Configuration](#)
- [Virtual Chassis](#)

---

### Authentication and Access Control

---

- On an EX2300-48T switch when dot1x single supplicant mode is configured , intermittently other clients on the port like an IP Phone may fail to forward traffic because the MAC address of the IP phone is not programmed in the switch. [PR1334310](#)

### EVPNs

---

- EX3400/EX2300 switches incorrectly flood unicast ARP replies in the VLAN when Dynamic ARP inspection is configured. [PR1331928](#)

### Forwarding and Sampling

---

- On the EX2300 and EX3400 SFLOW sampling is not accurate when the sample-rate is less than 256. [PR1333765](#)

### Infrastructure

---

- The statistics information of em0 is 0 when checked with SNMP or CLI show command. [PR1188103](#)

### Interfaces and Chassis

---

- The output of the command **show interfaces diagnostics optics** might display an incorrect value for the field "Receiver signal average optical power". This is a display issue only and does not affect the functionality of the optic. [PR1326642](#)
- In a Highly scaled VSTP (6 Interfaces x 253 VLANs) and MSTP config, CPU utilization may go high and L2CPD may hog. [PR1331858](#)
- 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](#)

### Layer 2 Features

---

- When the switch is configured for dot1x multi-supplicant mode , MAC move within the VLAN results in traffic getting dropped till the MAC learnt on the previous port ages out. [PR1329654](#)
- EX3400 CPU have hog when Continuous Telnet EC command are sent on more than 75 concurrent telnet session. This may lead to slowness in CLI response. [PR1331234](#)
- On a EX2300 switch, the output of the command **show chassis routing-engine** might display an incorrect value of "mac reset" for the "last reboot reason" field. [PR1331264](#)
- IP Directed broadcast traffic forwarding does not work on EX3400/EX2300. Applications such as Wakeup-on-lan does not work without this support. [PR1331326](#)
- Redirect message sent from EX series switch even when no-redirect is set for the specified interface. [PR1333153](#)

### Platform and Infrastructure

---

- On EX3400 and EX2300 switches, Junos OS volume recovery might not work after the switch is booted from a USB recovery snapshot. [PR1186127](#)
- On an EX3400 Virtual Chassis, the master Routing Engine might reset in some cases with the message **kernel: %KERN-2: jlock hog timer expired**. [PR1285034](#)
- Junos: Unauthenticated Remote Code Execution through J-Web interface (CVE-2018-0001); Refer to <https://kb.juniper.net/JSA10828> for more information. [PR1269932](#)
- On a EX2300 switch, the IfSpeed and IfHighSpeed MIB values might be incorrectly displayed during an SNMP get operation. [PR1326902](#)
- 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](#)

### Port Security

---

- In a scaled configuration , It is observed access ports of a member in VC go offline when committing/decommting "reauthentication" configuration for large number of interfaces spread 4 Members of the VC. [PR1329012](#)
- On EX2300-48P port ge-0/0/16-23 does not advertise 10M speed. It advertise only 100/1000M speeds. [PR1331357](#)

### Routing Protocols

---

- When performing traceroute to a remote host for an MPLS (Multiprotocol Label Switching) label-switched path signaled by the LDP (Label Distribution Protocol), the rpd process might crash. [PR1299026](#)
- LLDP power negotiation with Cisco APs with EX3400/EX2300, as Juniper EX Switch sends Extended POE TLV and POE TLV as seperate TLVs, where as Cisco sends then as Single TLV. [PR1300945](#)

---

## Software Installation and Upgrade

---

- On EX3400 and EX2300, "request system zeroize media" does not erase usb snapshot. [PR1183830](#)

## User Interface and Configuration

---

- 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](#)

## Virtual Chassis

---

- On an EX3400 Virtual Chassis, the master Routing Engine might reset in some cases with the message kernel: %KERN-2: jlock hog timer expired. [PR1329259](#)

- See Also**
- [New and Changed Features on page 3](#)
  - [Changes in Behavior and Syntax on page 10](#)
  - [Known Behavior on page 10](#)
  - [Resolved Issues on page 15](#)
  - [Documentation Updates on page 21](#)
  - [Migration, Upgrade, and Downgrade Instructions on page 22](#)
  - [Product Compatibility on page 23](#)

## Resolved Issues

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-D58 on page 15](#)
- [Resolved Issues: Release 15.1X53-D57 on page 17](#)
- [Resolved Issues: Release 15.1X53-D55 on page 19](#)
- [Resolved Issues: Release 15.1X53-D52 on page 20](#)
- [Resolved Issues: Release 15.1X53-D51 on page 20](#)

---

## Resolved Issues: Release 15.1X53-D58

---

### Infrastructure

- 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. This issue is reported in Junos OS Release 15.1X53-D57 and is not seen in Release 15.1X53-D56. Note that this issue is not applicable on EX2300-24 port switches. As a workaround, configure **interface-mac-limit** in the **[edit vlans]** hierarchy. Add the **interface-mac-limit** configuration to all VLANs to ensure that the MAC limit is set to a higher value that the limit is not expected to exceed. For example:

```
set vlans VLAN-NAME switch-options interface-mac-limit 16383
set vlans VLAN-NAME switch-options interface-mac-limit packet-action drop-and-log
```

When **interface-mac-limit** is configured, packet forwarding does not happen till the MAC is updated in the Ethernet-switching table in software. This learning process is very fast usually and only the first packet that arrives with this new source-mac is dropped. In some cases, if there is a burst of traffic with the same source-mac-address, then a few additional packets might be dropped till the MAC is learned in software.

[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. This issue is specific to Junos OS Release 15.1X53-D57.3 and is not seen in the previous releases. [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](#)

### **Software Installation and Upgrade**

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

## **Resolved Issues: Release 15.1X53-D57**

### **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, EX3400, and EX4300, 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. Configuring IRB on the affected interface might prevent the problem. [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**

#### ***Class of Service***

- On EX2300 switches, a packet loss priority (PLP) of medium-low is not supported for firewall filter configurations. [PR1180586](#)
- EX2300 and EX3400 switches do not support weighted random early detection (WRED) profiles. [PR1187354](#)

#### ***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***

- 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. To work around this problem, configure specific routes in addition to the default route. [PR1220078](#)

#### ***Platform and Infrastructure***

- On an EX3400 switch, CLI upgrades might fail with an **insufficient space** error. As a workaround, if there is not enough space for an upgrade, use the **request system storage cleanup** command to clear up space. [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](#)

#### ***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**

- **Infrastructure**

##### ***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**

- **Class of Service**
- **Infrastructure**
- **Layer 2 Features**
- **Layer 3 Protocols**
- **Network Management**
- **Virtual Chassis**

##### ***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 on page 3](#)
  - [Changes in Behavior and Syntax on page 10](#)
  - [Known Behavior on page 10](#)
  - [Known Issues on page 12](#)
  - [Documentation Updates on page 21](#)
  - [Migration, Upgrade, and Downgrade Instructions on page 22](#)
  - [Product Compatibility on page 23](#)

## **Documentation Updates**

There are no errata or changes in Junos OS Release 15.1X53-D58 for the EX Series switches documentation.

- See Also**
- [New and Changed Features on page 3](#)
  - [Changes in Behavior and Syntax on page 10](#)

- [Known Behavior on page 10](#)
- [Known Issues on page 12](#)
- [Resolved Issues on page 15](#)
- [Migration, Upgrade, and Downgrade Instructions on page 22](#)
- [Product Compatibility on page 23](#)

## 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 22](#)

### 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 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 <https://www.juniper.net/support/eol/junos.html>.

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

- See Also**
- [New and Changed Features on page 3](#)
  - [Changes in Behavior and Syntax on page 10](#)
  - [Known Behavior on page 10](#)

- [Known Issues on page 12](#)
- [Resolved Issues on page 15](#)
- [Documentation Updates on page 21](#)
- [Product Compatibility on page 23](#)

## Product Compatibility

- [Hardware Compatibility on page 23](#)

### 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 <https://pathfinder.juniper.net/feature-explorer/>.

- See Also**
- [New and Changed Features on page 3](#)
  - [Changes in Behavior and Syntax on page 10](#)
  - [Known Behavior on page 10](#)
  - [Known Issues on page 12](#)
  - [Resolved Issues on page 15](#)
  - [Documentation Updates on page 21](#)
  - [Migration, Upgrade, and Downgrade Instructions on page 22](#)

## 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](mailto:techpubs-comments@juniper.net), or fill out the documentation feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>. If you are using e-mail, be sure to include the following information with your comments:

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

## Requesting Technical Support

---

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

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service 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://www2.juniper.net/kb/>
- 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/>
- Open a case online in the CSC Case Management tool: <https://www.juniper.net/cm/>

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

## 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 <https://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 <https://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/documentation/feedback/>.

---

## Revision History

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 © 2018 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.