

Release Notes: Junos[®] OS Release 14.1X53-D27 for the EX Series and QFX Series

Release 14.1X53-D27
July 29, 2016
Revision 2

Contents

Junos OS Release Notes for EX Series Switches	4
New and Changed Features	4
New Features in Release 14.1X53-D27	4
New Features in Release 14.1X53-D26	4
New Features in Release 14.1X53-D25	5
New Features in Release 14.1X53-D15	5
New Features in Release 14.1X53-D10	7
Changes in Behavior and Syntax	17
Authentication and Access Control	17
Interfaces and Chassis	17
Routing Policy and Firewall Filters	18
Known Behavior	19
Class of Service	20
Interfaces and Chassis	20
J-Web	20
Layer 3 Protocols	21
MPLS	21
Multicast Protocols	21
Network Management	22
Virtual Chassis and Virtual Chassis Fabric	22
Known Issues	22
High Availability	23
Interfaces and Chassis	23
J-Web	23
Layer 2 Protocols	23
MPLS	23
System Management	24

Virtual Chassis and Virtual Chassis Fabric	24
Resolved Issues	24
Resolved Issues: Release 14.1X53-D27	25
Issues: Release 14.1X53-D26	25
Resolved Issues: Release 14.1X53-D25	26
Resolved Issues: Release 14.1X53-D16	26
Resolved Issues: Release 14.1X53-D10	26
Documentation Updates	27
Bridging and Learning	27
Security	28
Migration, Upgrade, and Downgrade Instructions	28
Upgrade and Downgrade Support Policy for Junos OS Releases	28
Product Compatibility	29
Hardware Compatibility	29
Junos OS Release Notes for the QFX Series	29
New and Changed Features	30
New Features in Release 14.1X53-D27	30
New Features in Release 14.1X53-D26	31
New Features in Release 14.1X53-D25	32
New Features in Release 14.1X53-D15	33
New Features in Release 14.1X53-D10	38
Changes in Behavior and Syntax	49
SNMP	50
Open vSwitch Database (OVSDB)	50
Software Upgrade	50
Known Behavior	51
Interfaces and Chassis	51
Layer 3 Protocols	52
MPLS	52
Multicast Protocols	52
OVSDB	52
QFabric Systems	53
Routing Policy and Firewall Filters	53
Software Installation and Upgrade	53
System Management	54
Storage and Fibre Channel	54
Traffic Management	55
Virtual Chassis and Virtual Chassis Fabric	59
VXLAN	59
Known Issues	60
Interfaces and Chassis	60
MPLS	61
Multicast Protocols	61
Network Management and Monitoring	61
OVSDB	61
Platform and Infrastructure	62
QFabric System	62
System Management	62
Virtual Chassis and Virtual Chassis Fabric	62

VXLAN	63
Resolved Issues	63
Resolved Issues: Release 14.1X53-D27	64
Resolved Issues: Release 14.1X53-D26	64
Resolved Issues: Release 14.1X53-D25	64
Resolved Issues: Release 14.1X53-D16	66
Resolved Issues: Resolved Before Release 14.1X53-D16	67
Documentation Updates	68
Bridging and Learning	68
Network Management and Monitoring	69
Virtual Chassis and Virtual Chassis Fabric (VCF)	69
Migration, Upgrade, and Downgrade Instructions	69
Upgrading to a Controlled Version of Junos OS	69
Upgrading Software on QFX5100 Standalone Switches	70
Performing an In-Service Software Upgrade (ISSU)	71
Preparing the Switch for Software Installation	72
Upgrading the Software Using ISSU	72
Product Compatibility	74
Hardware Compatibility	74
Software Compatibility	74
Third-Party Components	75
Finding More Information	75
Documentation Feedback	75
Requesting Technical Support	76
Self-Help Online Tools and Resources	76
Opening a Case with JTAC	76
Revision History	77

Junos OS Release Notes for EX Series Switches

These release notes accompany Junos OS Release 14.1X53-D27 for the EX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

The following EX Series switches are supported in Junos OS Release 14.1X53-D27: EX4300 and EX4600.



NOTE: These release notes include information on all Junos OS Release 14.1X53 releases. Therefore, information about EX Series switches that are not supported in Junos OS Release 14.1X53-D27 but are supported on other Junos OS Release 14.1X53 releases are included in these release notes.

- [New and Changed Features on page 4](#)
- [Changes in Behavior and Syntax on page 17](#)
- [Known Behavior on page 19](#)
- [Known Issues on page 22](#)
- [Resolved Issues on page 24](#)
- [Documentation Updates on page 27](#)
- [Migration, Upgrade, and Downgrade Instructions on page 28](#)
- [Product Compatibility on page 29](#)

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 14.1X53 for the EX Series.

- [New Features in Release 14.1X53-D27 on page 4](#)
- [New Features in Release 14.1X53-D26 on page 4](#)
- [New Features in Release 14.1X53-D25 on page 5](#)
- [New Features in Release 14.1X53-D15 on page 5](#)
- [New Features in Release 14.1X53-D10 on page 7](#)

[New Features in Release 14.1X53-D27](#)

There are no new features for EX Series switches in Junos OS Release 14.1X53-D27.

[New Features in Release 14.1X53-D26](#)

Hardware

- **New optical transceivers support on EX4300 switches**—Starting with Junos OS Release 14.1X53-D26, EX4300 switches support the following optical transceivers:

- EX-SFP-GE10KT13R14 (1000BASE-BX-U, 10 km)
- EX-SFP-GE10KT14R13 (1000BASE-BX-D, 10 km)
- EX-SFP-GE10KT13R15 (1000BASE-BX-U, 10 km)
- EX-SFP-GE10KT15R13 (1000BASE-BX-D, 10 km)

New Features in Release 14.1X53-D25

Authentication and Access Control

- **Access control (mixed EX4300 and EX4600 Virtual Chassis)**—Starting with Junos OS Release 14.1X53-D25, EX4600 switches operating in a mixed Virtual Chassis with EX4300 switches support controlling access to your network by using several different authentication methods: 802.1X authentication, MAC RADIUS authentication, or **captive portal**. You enable the **authentication-whitelist** statement at the **[edit switching-options]** hierarchy level instead of at the **[edit ethernet-switching-options]** hierarchy level.

Access control features in a mixed EX4300 and EX4600 Virtual Chassis are supported only on EX4300 switch interfaces.

[See [Access Control on a Mixed EX4300-EX4600 Virtual Chassis](#).]

MPLS

- **MPLS stitching for virtual machine connections (EX4600)**—By using MPLS, the stitching feature of Junos OS provides connectivity between virtual machines on opposite sides of data center routers. An external controller, programmed in the data-plane, assigns MPLS labels to both virtual machines and servers. Then, the signaled MPLS labels are used between the data center routers, generating static link switched paths (LSPs), resolved over RSVP or LDP, to provide the routes dictated by the labels. The new CLI command **stitch**, located under the LSP transit command, provides this capability. [See [MPLS Stitching For Virtual Machine Connection](#).]

New Features in Release 14.1X53-D15

Interfaces and Chassis

- **Default logging for Ethernet ring protection switching (ERPS) EX2200, EX3200, EX3300, EX4200, EX4500, EX4550, EX8200 standalone switches; EX2200, EX3300, EX4200, EX4500, EX4550, EX8200 Virtual Chassis)**—Starting with Junos OS Release 14.1X53-D15, the listed EX Series switches automatically log basic state transitions for the ERPS protocol. No configuration is required to initiate this logging. Basic state transitions include ERPS interface transitions from up to down, and down to up; and ERPS state transitions from idle to protection, and protection to idle.

The basic state transitions are logged in a single file named **erp-default**, which resides in the **/var/log** directory of the switch. The maximum size of this file is 15 MB.

Default logging for ERPS can capture initial ERPS interface and state transitions, which can help you troubleshoot issues that occur early in the ERPS protocol startup process. However, if more robust logging is needed, you can enable traceoptions for ERPS by

entering the **traceoptions** statement in the **[edit protocols protection-group]** hierarchy level.

Be aware that for ERPS, only default logging or traceoptions can be active at a time on the switch. That is, default logging for ERPS is automatically enabled and if you enable traceoptions for ERPS, the switch automatically disables default logging. Conversely, if you disable traceoptions for ERPS, the switch automatically enables default logging.

- **Power over Ethernet (EX4600 switches)**—Starting with Junos OS Release 14.1X53-D15, EX4600 switches support Power over Ethernet (PoE) when operating in a mixed-mode Virtual Chassis with an EX4300 switch. You can enable PoE configuration statements and run PoE operational commands on an EX4600 switch only when the switch is operating in a mixed-mode Virtual Chassis.

You can configure PoE at the **[edit poe]** hierarchy level.

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

MPLS

- **MPLS enhancements (EX4600 switches)**—Starting with Junos OS Release 14.1X53-D15, a set of procedures is provided for augmenting network layer packets with label stacks, thereby turning them into labeled packets. MPLS has emerged as an elegant solution to meet the bandwidth-management and service requirements for next-generation IP-based backbone networks.

The following MPLS features have been added to EX4600:

- BGP L3 VPN Carrier-over-Carrier and Interprovider

BGP is an exterior gateway protocol (EGP) that is used to exchange routing information among routing devices in different autonomous systems (ASs). Instead of using the label distribution protocols LDP or RSVP, MPLS can piggyback on routing protocols such as BGP and OSPF.

- Ethernet over MPLS pseudowire based on LDP (draft Martini / L2 Circuit)

Ethernet-over-MPLS supports sending Layer 2 Ethernet frames transparently over MPLS using a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core. Pseudowire is a software mechanism for emulating various networking or telecommunications services across packet-switched networks that use Ethernet, IP, or MPLS. An Ethernet pseudowire is used to carry Ethernet or 802.3 PDUs over an MPLS network enabling service providers to offer emulated Ethernet services over existing MPLS networks. There are several label distribution protocols used such as Label Distribution Protocol (LDP) or RSVP; another technique is piggybacking on routing protocols such as BGP and OSPF.

- Static and dynamic Ethernet pseudowire over LDP and RSVP tunnels

Pseudowire is a software mechanism for emulating various networking or telecommunications services across packet-switched networks that use Ethernet, IP, or MPLS. Label Distribution Protocol (LDP) and RSVP are label distribution protocols used by MPLS.

- Pseudowire over aggregated Ethernet on core-facing interfaces

Pseudowire is a software mechanism for emulating various networking or telecommunications services across packet-switched networks that use Ethernet, IP, or MPLS.

- RSVP fast-reroute including link-protection and node-link-protection

One label distribution protocol used for MPLS data transmission is RSVP.

[See [MPLS Feature Support on the QFX Series and the EX4600 Switch](#).]

Security

- **Media Access Control Security (MACsec) support (EX4600 switches)**—Starting with Junos OS Release 14.1X53-D15, MACsec is supported on all built-in SFP+ interfaces on an EX4600 switch. MACsec is also supported on all eight SFP+ interfaces on the EX4600-EM-8F expansion module when it is installed in an EX4600 switch. MACsec is an industry-standard security technology that provides secure communication for all traffic on point-to-point Ethernet links. MACsec is capable of identifying and preventing most security threats, and can be used in combination with other security protocols to provide end-to-end network security. MACsec is standardized in IEEE 802.1AE. See also *Documentation Updates*.

[See [Understanding Media Access Control Security \(MACsec\)](#).]

New Features in Release 14.1X53-D10

Authentication and Access Control

- **IPv6 for RADIUS AAA (EX3300, EX4200, EX4300, EX4500, and EX8200 switches and EX4300 Virtual Chassis)**—Starting with Junos OS Release 14.1X53-D10, EX3300, EX4200, EX4300, EX4500, and EX8200 switches and EX4300 Virtual Chassis support IPv6, along with the existing IPv4 support, for user authentication, authorization, and accounting (AAA) using RADIUS servers.

RADIUS authentication is a method of authenticating users who attempt to access the router or switch. To use RADIUS authentication on the switch, configure information about one or more RADIUS servers on the network by including one **radius-server** statement at the **[edit system]** hierarchy level for each RADIUS server.

When you configure a source address for each configured RADIUS server, each RADIUS request sent to a RADIUS server uses the specified source address.

- **Authentication**—Specify which source address Junos OS uses when accessing your network to contact an external RADIUS server for authentication. You configure the IPv6 source address for RADIUS authentication at the **[edit system radius-server server-address source-address]** hierarchy level.
- **Accounting**—Specify which source address Junos OS uses when contacting a RADIUS server for sending accounting information. You configure the IPv6 source address for RADIUS authentication at the **[edit system accounting destination radius server server-address source-address]** hierarchy level.

[See [source-address](#).]

Bridging and Learning

- **RVI support for private VLANs (EX8200 switches and EX8200 Virtual Chassis)**—Starting with Junos OS Release 14.1X53-D10, you can configure a routed VLAN interface (RVI) on an EX8200 switch or EX8200 Virtual Chassis to handle the Layer 3 traffic of intersecondary VLANs (community VLANs and isolated VLANs) in a private VLAN (PVLAN). By using an RVI to handle the routing within the PVLAN, you eliminate the need for an external router with a promiscuous port connection to perform this function.

One RVI serves the entire PVLAN domain regardless of whether the domain consists of one or more switches. After you configure the RVI, Layer 3 packets received by the secondary VLAN interfaces are mapped to and routed by the RVI.

[See [Configuring a Routed VLAN Interface in a Private VLAN \(CLI Procedure\)](#).]

- **Support for private VLANs (EX4300)**—Starting with Junos OS Release 14.1X53-D10, EX4300 switches support private VLANs (PVLANS). PVLANS are useful for restricting the flow of broadcast and unknown unicast traffic and for limiting the known communication between known hosts. PVLANS can be used to help ensure the security of service providers sharing a server farm, or to provide security to subscribers of various service providers sharing a common metropolitan area network.



NOTE: An interface can belong to only one PVLAN domain.

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

- **Support for Layer 2 protocol tunneling (EX4300)**—Starting with Junos OS Release 14.1X53-D10, EX4300 switches support Layer 2 protocol tunneling (L2PT). L2PT enables service providers to send Layer 2 protocol data units (PDUs) across the provider's cloud and deliver them to Juniper Networks EX Series Ethernet Switches that are not part of the local broadcast domain. This feature is useful when you want to run Layer 2 protocols on a network that includes switches located at remote sites that are connected across a service provider network. For example, it can help you provide transparent LAN services over a metropolitan Ethernet infrastructure. L2PT operates under the Q-in-Q tunneling configuration; therefore, you must enable Q-in-Q tunneling before you can configure L2PT.

The Layer 2 protocol to be tunneled can be one of the following: 802.3AH, CDP, LACP, LLDP, MVRP, STP, VTP, GVRP, or VSTP.



NOTE: L2PT does not support the following on EX4300 switches:

- drop-threshold or shutdown-threshold statements
- The all option for setting the Layer 2 protocol
- 802.1X authentication

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

- **MAC notification (EX4300 and EX4600)**—Starting with Junos OS Release 14.1X53-D10, MAC notification is supported on EX4300 and EX4600 switches. The switches track clients on a network by storing MAC addresses in the Ethernet switching table on the switch. When switches learn or unlearn a MAC address, SNMP notifications can be sent to the network management system at regular intervals to record the addition or removal of the MAC address. This process is known as MAC notification.

The MAC Notification MIB controls MAC notification for the network management system.

The MAC notification interval defines how often these SNMP notifications are sent to the network management system. The MAC notification interval works by tracking all MAC address additions or removals on the switch over a period of time and then sending all tracked MAC address additions or removals to the network management server at the end of the interval.

Enabling MAC notification allows you to monitor the addition and removal of MAC addresses from the Ethernet switching table remotely using a network management system. The advantage of setting a high MAC notification interval is that the amount of network traffic is reduced because updates are sent less frequently. The advantage of setting a low MAC notification interval is that the network management system is better synchronized with the switch.

Two new MIBs related to MAC notification are provided at Junos OS Release 14.1X53-D10. See *Documentation Updates*.

[See [Configuring MAC Notification \(CLI Procedure\)](#).]

- **Default VLAN and multiple VLAN range support (EX4300)**—Starting with Junos OS Release 14.1X53-D10, the default VLAN and multiple VLAN range are supported on EX4300 switches. They provide the ability for the switch to operate as a *plug and play* device and connect to various Ethernet-enabled devices in a small, scaled enterprise network. When the switch boots, a VLAN named **default** is created. The default VLAN is automatically created for the default routing instance named **default-switch**. All interfaces on the switch are automatically configured as access interfaces and are part of the default VLAN.

The default VLAN accepts and forwards untagged packets only and is preconfigured with a VLAN ID (**vlan-id**) of 1. The default VLAN does not support a VLAN ID list (**vlan-id-list**), **vlan-id** set to **all**, or **vlan-id** set to **none**. You can configure the VLAN ID to be another value, but the value must be between 1 and 4093.

Access interfaces that are enabled for VoIP or 802.1X are internally converted to trunk interfaces, so that the interfaces can belong to multiple VLANs. If the interfaces do not belong to a valid VLAN, the interfaces automatically become part of the default VLAN.

You can configure more than one VLAN range, and each range can contain unique VLAN properties.



NOTE: Virtual Chassis interfaces cannot be preconfigured to belong to the default VLAN or any other VLAN.



NOTE: For interfaces to be part of the default VLAN, you must configure the interfaces to be part of the Ethernet switching family. You can configure Ethernet switching at the [edit interfaces *interface-name* unit family] hierarchy level.

Class of Service

- **Explicit congestion notification (ECN) support (EX4300)**—Starting with Junos OS Release 14.1X53-D10, ECN marking is supported on EX4300 switches—you enable it for packets in scheduler queues. Explicit congestion notification (ECN) enables end-to-end congestion notification between two endpoints on TCP/IP based networks. The two endpoints are an ECN-enabled sender and an ECN-enabled receiver. ECN must be enabled on both endpoints and on all intermediate devices between the endpoints for ECN to work properly. Any device in the transmission path that does not support ECN breaks the end-to-end ECN functionality.

ECN notifies networks about congestion with the goal of reducing packet loss and delay by making the sending device decrease the transmission rate until the congestion clears, without dropping packets.

To enable ECN, issue the **set class-of-service schedulers *name* explicit-congestion-notification** command.

Infrastructure

- **Licensing enhancements (EX Series)**—Starting with Junos OS Release 14.1X53-D10, licensing enhancements on EX Series switches enable you to configure and delete license keys in a Junos OS CLI configuration file. The license keys are validated and installed after a successful commit of the configuration file. If a license key is invalid, the commit fails and issues an error message. You can configure individual license keys or multiple license keys by issuing Junos OS CLI commands or by loading the license key configuration contained in a file. All installed license keys are stored in the **/config/license/** directory.

To install an individual license key in the Junos OS CLI, issue the **set system license keys key *name*** command, and then issue the **commit** command.

For example:

```
[edit]
root@switch# set system license keys key "JUNOS_TEST_LIC_FEAT aeaqeb qbmqds
qwwsxe okyvou 6v57u5 zt6ie6 uwl3zh assvnu e2ptl5 soxawy vtfh7k axwnno m5w54j
6z"
root@switch# commit
commit complete
```

To verify that the license key was installed, issue the **show system license** command.

For example:

```
root@switch> show system license
License usage:
Licenses  Licenses  Licenses  Expiry
```


Feature name	used	installed	needed
sdk-test-feat1	0	1	0 permanent

Licenses installed:

License identifier: JUNOS_TEST_LIC_FEAT

License version: 2

Features:

 sdk-test-feat1 - JUNOS SDK Test Feature 1
 permanent

To install multiple license keys in the Junos OS CLI, issue the **set system license keys key *name*** command, and then issue the **commit** command.

For example:

```
[edit]
root@switch# set system license keys key "key_1"
set system license keys key "key_2"
set system license keys key "key_2"
set system license keys key "key_4"
root@switch# commit
commit complete
```

To verify that the license key was installed, issue the **show system license** command.

To install an individual license key configuration in a file, issue the **cat** command:

For example:

```
[edit]
root@switch%cat license.conf
system {
  license {
    keys {
      key "JUNOS_TEST_LIC_FEAT aeaqeb qbmqds qwwsxe okyvou 6v57u5 zt6ie6
uwl3zh assvnu e2ptl5 soxawy vtfh7k axwnno m5w54j 6z";
    }
  }
}
```

Load and merge the license configuration file.

For example:

```
[edit]
root@switch# load merge license.conf
load complete
```

Issue the **show | compare** command to see the configuration, and then issue the **commit** command.

For example:

```
[edit]
root@switch# show | compare
[edit system]
+ license {
+   keys {
+     key "JUNOS_TEST_LIC_FEAT aeaqeb qbmqds qwwsxe okyvou 6v57u5 zt6ie6
uwl3zh assvnu e2ptl5 soxawy vtfh7k axwnno m5w54j 6z";
```



```
+   }
+   }
[edit]
root@switch# commit
```

To verify that the license key was installed, issue the **show system license** command.

For example:

```
root@switch> show system license
License usage:

```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
sdk-test-feat1	0	1	0	permanent

```

Licenses installed:
License identifier: JUNOS_TEST_LIC_FEAT
License version: 2
Features:
  sdk-test-feat1 - JUNOS SDK Test Feature 1
  permanent
```

To install multiple license keys in a file, issue the **cat** command:

For example:

```
[edit]
root@switch%cat license.conf
system
{
  license
  {
    keys
    {
      key "key_1"
      key "key_2"
      key "key_3"
      ...
      key "key_n"
    }
  }
}
```

Load and merge the license configuration file, and then issue the **commit** command.

For example:

```
[edit]
root@switch# load merge license.conf
load complete
[edit]
root@switch# commit
```

To verify that the license key was installed, issue the **show system license** command.

You can also delete or deactivate individual and multiple license keys in the Junos OS CLI by issuing the **delete system license keys** or **deactivate system license keys** commands. Do not use the **request system license delete** command to delete the license keys.

For example, to issue the **delete system license keys** command:

```
[edit]
root@switch# delete system license keys
root@switch# commit
```

Interfaces and Chassis

- **Support for aggregated Ethernet link protection enhancements (EX4500)**—Starting with Junos OS Release 14.1X53-D10, aggregated Ethernet link protection is enhanced on EX4500 switches to support a collection of Ethernet links within a LAG bundle. Link protection could previously be used to protect a single link within a LAG bundle only. The ability to provide link protection for a collection of links in a LAG bundle is provided using link protection subgroups, which are introduced as part of this feature.

[See [Configuring LACP Link Protection of Aggregated Ethernet Interfaces \(CLI Procedure\)](#).]

J-Web

- **J-Web interface available in two packages (EX2200, EX3200, EX3300, EX4200, EX4300, EX4500, EX4550, EX6200)**—Prior to this release, the J-Web interface was available as a single package as part of Junos OS. Starting with Junos OS Release 14.1X53-D10, the J-Web interface is available in two packages:
 - The Platform package is installed as part of Junos OS, which provides basic functionalities of J-Web. You can use the Platform package to create a basic configuration and maintain your EX Series switch.
 - The Application package is an optionally installable package, which provides complete functionalities of J-Web that enable you to configure, monitor, maintain, and troubleshoot your switch. You must download the Application package and install it over the Platform package on your switch.

For detailed information about the J-Web packages, see [Release Notes: J-Web Application Package Release 14.1X53-A1 for Juniper Networks EX Series Ethernet Switches](#).

- **Browser support enhancements for the J-Web interface (EX2200, EX3200, EX3300, EX4200, EX4300, EX4500, EX4550, EX6200)**—Starting with Junos OS Release 14.1X53-D10, the J-Web interface supports the following browsers:
 - Microsoft Internet Explorer versions 9 and 10
 - Mozilla Firefox versions 24 through 30
 - Google Chrome versions 27 through 36



TIP: For best viewing of the J-Web application, set the screen resolution to 1440 X 900.

Layer 3 Protocols

- **IS-IS protocol (EX3300)**—EX3300 switches now support the Intermediate System-to-Intermediate System (IS-IS) protocol. On EX3300 switches, the IS-IS configuration is available at the **[edit protocols]** hierarchy level.

[See [Layer 3 Protocols Supported on EX Series Switches.](#)]

MPLS

- **Ethernet-over-MPLS (L2 circuit) (EX4600)**—Starting with Junos OS Release 14.1X53-D10, Ethernet-over-MPLS is supported on EX4600 switches. Ethernet-over-MPLS enables you to send Layer 2 Ethernet frames transparently over an MPLS cloud. Ethernet-over-MPLS uses a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core. It encapsulates Ethernet protocol data units (PDUs) inside MPLS packets and forwards the packets, using label stacking, across the MPLS network.

This technology has applications in service provider, enterprise, and data center environments. For disaster recovery purposes, data centers are hosted in multiple sites that are geographically distant and interconnected using a WAN network. These data centers require Layer 2 connectivity between them for the following reasons:

- To replicate the storage over Fibre Channel over IP (FCIP). FCIP works only on the same broadcast domain.
 - To run a dynamic routing protocol between the sites.
 - To support high availability clusters that interconnect the nodes hosted in the various data centers.
- **MPLS-based Layer 3 VPNs (EX4600)**—Starting with Junos OS Release 14.1X53-D10, MPLS-based Layer 3 VPNs are supported on EX4600 switches.

Customer networks are private and can use either public addresses or private addresses. When customer networks that use private addresses connect to the public Internet infrastructure, the private addresses might overlap with private addresses being used by other network users. MPLS BGP VPNs solve this problem by adding the route distinguisher prefix to the route.

You can configure the switch as a CE or PE device using Layer 3 MPLS/BGP VPN for interprovider and carrier-of-carrier VPNs. The key difference between interprovider and carrier-of-carriers VPNs is whether the customer sites belong to the same autonomous system (AS) or to a separate AS:

 - Interprovider VPNs—The customer sites belong to different ASs. You need to configure EBGP to exchange the customer's external routes.
 - Carrier-of-carriers VPNs—The customer sites belong to the same AS. You need to configure IBGP to exchange the customer's external routes.
 - **MPLS LSP protection (EX4600)**—Starting with Junos OS Release 14.1X53-D10, the following types of MPLS LSP protection are supported on EX4600 switches:
 - Fast reroute (FRR)

- Link protection
- Node link protection

[See [MPLS Overview](#).]

Network Management and Monitoring

- **Chef for Junos OS (EX4300)**—Starting with Junos OS Release 14.1X53-D10, Chef for Junos OS is supported on EX4300 switches.
- **Puppet for Junos OS (EX4300)**—Starting with Junos OS Release 14.1X53-D10, Puppet for Junos OS is supported on EX4300 switches.
- **Network analytics (EX4300)**—Starting with Junos OS Release 14.1X53-D10, EX4300 switches support the network analytics feature. The network analytics feature provides visibility into the performance and behavior of the data center infrastructure. This feature collects data from the switch, analyzes the data by using sophisticated algorithms, and captures the results in reports. Network administrators can use the reports to help troubleshoot problems, make decisions, and adjust resources as needed. The analytics manager (analyticsm) in the Packet Forwarding Engine collects traffic and queue statistics, and the analytics daemon (analyticsd) in the Routing Engine analyzes the data and generates reports. You can enable network analytics by configuring microburst monitoring and high-frequency traffic statistics monitoring.

[See [Network Analytics Overview](#).]

- **Ethernet frame delay measurement (EX2200)**—Starting with Junos OS Release 14.1X53-D10, you can obtain Ethernet frame delay measurements (ETH-DM) on an EX2200 switch. You can configure Operation, Administration, and Maintenance (OAM) statements for connectivity fault management (IEEE 802.1ag) to provide on-demand measurements of frame delay and frame delay variation (jitter). You configure the feature under the **[edit protocols oam ethernet connectivity-fault-management]** hierarchy level.
- **Support for native analyzers and remote port-mirroring capabilities (EX4300)**—Starting with Junos OS Release 14.1X53-D10, native analyzers and remote port mirroring are supported on EX4300 switches. A native analyzer configuration contains both an input stanza and an output stanza in the analyzer hierarchy for mirroring packets. In remote port mirroring, the mirrored traffic is flooded into a remote mirroring VLAN that can be specifically created for the purpose of receiving mirrored traffic. On EX4300 switches, the analyzer configuration is available under the **[edit forwarding-options]** hierarchy level.

Port Security

- **IPv6 access security (EX2200 and EX3300)**—Starting with Junos OS Release 14.1X53-D10, the following IPv6 access security features are supported on EX2200 and EX3300 switches: DHCPv6 snooping, IPv6 Neighbor Discovery Inspection, IPv6 source guard, and RA guard. DHCPv6 snooping enables a switch to process DHCPv6 messages between a client and a server and build a database of the IPv6 addresses assigned to the DHCPv6 clients. The switch can use this database, also known as the binding table, to stop malicious traffic. DHCPv6 includes the relay agent Remote-ID option, also known as Option 37, to optionally append additional information to the messages sent by the client towards the server. This information can be used by the server to assign addresses and configuration parameters to the client. IPv6 Neighbor Discovery inspection analyzes neighbor discovery messages sent between IPv6 nodes on the same link and verifies them against the DHCPv6 binding table. IPv6 source guard inspects all IPv6 traffic from the client and verifies the source IPv6 address and source MAC address against the entries in the DHCPv6 binding table. If no match is found, the traffic is dropped. RA guard examines incoming Router Advertisement (RA) messages and decides whether to forward or block them based on statically configured IPv6/MAC address bindings. If the content of the RA message does not match the bindings, the message is dropped.

Starting with this release, Remote-ID (Option-37) is not added by default on when you enable **dhcpv6-snooping**.

You configure DHCPv6 snooping, IPv6 Neighbor Discovery Inspection, and IPv6 source guard at the **[edit ethernet-switching-options secure-access-port vlan *vlan-name*]** hierarchy level. You configure RA guard at the **[edit ethernet-switching-options secure-access-port interface *interface-name*]** hierarchy level.

[See [Port Security Overview](#).]

- **IPv6 access security (EX4300)**—Starting with Junos OS Release 14.1X53-D10, DHCPv6 snooping supports a configuration to optionally append the relay agent Remote ID (Option-37), Interface-ID (Option-18), and Vendor-Class (Option-16) to the DHCPv6 packets sent by a client. You can configure these options under the **[edit vlans *vlan-name* forwarding-options dhcp-security dhcpv6-options]** hierarchy level.
- **Media Access Control Security (MACsec) support for switch to host connections (EX4200, EX4300, and EX4550)**—Starting with Junos OS Release 14.1X53-D10, MACsec is supported on links connecting EX4200, EX4300, and EX4550 switches to host devices, such as phones, servers, personal computers, or other endpoint devices. This feature also introduces MACsec dynamic mode and the ability to retrieve MACsec Key Agreement (MKA) keys from a RADIUS server, which are required to enable MACsec on a switch to host link.

[See [Understanding Media Access Control Security \(MACsec\)](#) .]

Virtual Chassis and Virtual Chassis Fabric

- **Alias support for Virtual Chassis and Virtual Chassis Fabric (VCF) nodes**—Starting with Junos OS Release 14.1X53-D10, an alias can be used to label nodes in a Virtual Chassis and VCF. An alias enables you to more clearly identify a member switch in your Virtual Chassis or VCF by assigning a text label to it. The text label appears alongside the switch's serial number whenever operational commands, such as **show virtual-chassis**, are used to monitor Virtual Chassis status.

[See [aliases](#).]

Related Documentation

- [Changes in Behavior and Syntax on page 17](#)
- [Known Behavior on page 19](#)
- [Known Issues on page 22](#)
- [Resolved Issues on page 24](#)
- [Documentation Updates on page 27](#)
- [Migration, Upgrade, and Downgrade Instructions on page 28](#)
- [Product Compatibility on page 29](#)

Changes in Behavior and Syntax

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 14.1X53 for the EX Series.

- [Authentication and Access Control](#)
- [Interfaces and Chassis](#)
- [Routing Policy and Firewall Filters](#)

[Authentication and Access Control](#)

- Starting with Junos OS Release 14.1X53-D25 for EX Series switches, the **accounting-port** CLI statement is now supported at the **[edit access radius-server server-address]** hierarchy level on all EX Series switches. This command was supported only on EX4300, EX4600, and EX9200 switches in earlier Junos OS releases. The **accounting-port** statement enables you to specify the port on which to contact the RADIUS accounting server. The default port number is 1813, as specified in RFC 2866.

[Interfaces and Chassis](#)

- On EX4300 switches, when you configure the DHCP **relay-option-82** option, the circuit ID is added by default. In the case of an IRB interface, the DHCP relay option 82 will contain a description or name of the physical layer interface instead of the name of the IRB interface. To include the name of the IRB interface, you can use the **include-irb-and-l2** statement. To display only the IRB interface without the names of the Layer 2 interface and VLAN, use the **no-vlan-interface-name** statement.

default	VLAN-tagged interface	ge-1/2/3:10
	Dual-tagged interface	ge-1/2/3:10-20
	Pure Layer 3 interface	ge-1/2/3.0
	IRB interface	ge-1/2/3.0:v10
use-vlan-id		ge-1/2/3.0:10
include-irb-and-l2		ge-1/2/3.0:v10+irb.10
include-irb-and-l2 and use-vlan-id		ge-1/2/3.0:10+irb.10
no-vlan-interface-name		irb.10
no-vlan-interface-name and use-vlan-id		Mutually exclusive
no-vlan-interface-name and include-irb-and-l2		ge-1/2/3.0+irb.10
use-interface-description		l2_descr:v10
	If no description found	ge-1/2/3.0:v10
use-interface-description and use-vlan-id		Mutually exclusive
use-interface-description and include-irb-and-l2		l2_descr:v10+irb.10
	If no description found	ge-1/2/3.0:v10+irb.10
use-interface-description and no-vlan-interface-name		irb_descr
	If no description found	irb.10
use-interface-description, no-vlan-interface-name, and include-irb-and-l2		l2_descr+irb.10
	If no description found	ge-1/2/3.0+irb.10

Routing Policy and Firewall Filters

- **Support for enhanced mask length on IPv6 destination-address match conditions for loopback filters (EX Series switches)**—Starting with Junos OS Release 14.1X53-D15, the maximum mask length of IPv6 destination-address match conditions in loopback (lo0) filters on EX Series switches is /128.

- Related Documentation**
- [New and Changed Features on page 4](#)
 - [Known Behavior on page 19](#)
 - [Known Issues on page 22](#)
 - [Resolved Issues on page 24](#)
 - [Documentation Updates on page 27](#)
 - [Migration, Upgrade, and Downgrade Instructions on page 28](#)
 - [Product Compatibility on page 29](#)

Known Behavior

The following are changes in known behavior in Junos OS Releases 14.1X53 for the EX Series.

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

- [Class of Service](#)
- [Interfaces and Chassis](#)
- [J-Web](#)
- [Layer 3 Protocols](#)
- [MPLS](#)
- [Multicast Protocols](#)
- [Network Management](#)
- [Virtual Chassis and Virtual Chassis Fabric](#)

Class of Service

- On EX4550 switches, 128-byte packets are dropped if the CPU is at 97 percent load or greater. Packets of different sizes are not dropped under these conditions. [PR1057408](#)

Interfaces and Chassis

- On 40-gigabit links between EX4300 and QFX5100 switches, you must disable **auto-negotiation** on both ends of the link for the interfaces to remain up. On each switch, issue the **set interface et-x/y/z ether-options no-auto-negotiation** command. Also, because **auto-negotiation** is disabled, you must also explicitly configure the **link-mode** and **speed** options on those interfaces. [PR1118318](#)

J-Web

- On an EX4300 Virtual Chassis, if you use the J-Web user interface to request support information for all members at the same time, the switch might not be able to retrieve the information. As a workaround, request support information for each member one at a time.
- In the J-Web interface, you cannot commit some configuration changes in the Ports Configuration page or the VLAN Configuration page because of the following limitations for port-mirroring ports and port-mirroring VLANs:
 - A port configured as the output port for an analyzer cannot be a member of any VLAN other than the default VLAN.
 - A VLAN configured to receive analyzer output can be associated with only one interface.

This is a known software limitation. [PR400814](#)

- In the J-Web interface for EX4500 switches, the Ports Configuration page (Configure > Interfaces > Ports), the Port Security Configuration page (Configure > Security > Port Security), and the Filters Configuration page (Configure > Security > Filters) display features that are not supported on EX4500 switches. [PR525671](#)
- The J-Web interface does not support role-based access control; it supports only users in the super-user authorization class. Therefore, a user who is not in the super-user class, such as a user with view-only permission, is able to launch the J-Web interface and can configure everything, but the configuration fails on the switch, and the switch displays access permission error messages. [PR604595](#)
- On an EX3300 Virtual Chassis, if you use the J-Web interface to request support information for all members at the same time, the switch might not be able to retrieve the information. As a workaround, request support information for each member one at a time. [PR911551](#)
- In the Maintain > Update J-Web page, Select Application package > Update J-Web > local file does not work in Microsoft IE9 and later releases, due to default security options set on IE9 and later releases. As a workaround, increase the security level by using one of the following methods:

Method 1:

1. Navigate to **Internet Options > Security**.
2. Select the zone **Local intranet**.
3. Click the custom level button.
4. Disable the option **Include local directory Path when uploading file to the server** in the **Settings > miscellaneous** section.
5. Repeat Steps 3 and 4 for the zone **Internet**.

Method 2:

- Navigate to **Internet Options > Security > Custom level...** and set **Reset custom settings** to **Medium-High** or **High**. This automatically disables the option **Include local directory Path when uploading file to the server** under the **Settings > miscellaneous** section.

[PR1029736](#)

Layer 3 Protocols

- On EX3300 switches, when there are multiple open Telnet or SSH sessions, the switch might become unresponsive. [PR1029340](#)

MPLS

- FRR convergence times over pseudo interfaces (aggregate) might be larger than over physical interfaces. [PR976737](#)
- In a scaled configuration for MPLS FRR and L2 circuit, the convergence time for FRR might increase. For L2 circuit, there might be packet drops. [PR1016146](#)

Multicast Protocols

- On EX4300 switches, executing the **show igmp snooping membership** CLI command continuously while IGMP groups are being processed results in some groups not being displayed in the output. CPU utilization also increases significantly when this command is executed when there are more than 1000 groups. As a workaround, issue the **show igmp snooping membership** command with filters such as **group** or **interface**. This is a known software limitation. [PR914908](#)
- On an EX4550 switch, if you configure IGMP on all interfaces and create a large number of multicast groups, the maximum scale for IGMP can be achieved on some interfaces, but not on all interfaces. [PR1025169](#)

Network Management

- On EX2200 switches, remote MEP flaps might occur every 30 to 200 seconds because of processing delays and lead to iterator delay measurement statistic resets. All delay system measurements remain valid when this issue occurs. As a workaround, use an iterator count of less than 30. [PR1005819](#)

Virtual Chassis and Virtual Chassis Fabric

- When an EX4300 switch is removed from a Virtual Chassis by deleting the Virtual Chassis port (VCP) connecting the switch to the Virtual Chassis, the EX4300 switch splits from the Virtual Chassis. To add the EX4300 switch back into the Virtual Chassis, enter the **request virtual-chassis reactivate** command to take the switch out of linecard mode and then enter the **request virtual-chassis vc-port set pic-slot slot-number port port-number** command to create the VCP. [PR1013386](#)
- On a mixed Virtual Chassis Fabric (VCF), a Virtual Chassis port (VCP) link between two members might disappear after you perform a nonstop software upgrade (NSSU). The **show virtual-chassis protocol adjacency member** command output shows the state of the VCP link as **Initializing**. [PR1031296](#)

Related Documentation

- [New and Changed Features on page 4](#)
- [Changes in Behavior and Syntax on page 17](#)
- [Known Issues on page 22](#)
- [Resolved Issues on page 24](#)
- [Documentation Updates on page 27](#)
- [Migration, Upgrade, and Downgrade Instructions on page 28](#)
- [Product Compatibility on page 29](#)

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 14.1X53 for the EX Series.

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

- [High Availability](#)
- [Interfaces and Chassis](#)
- [J-Web](#)
- [Layer 2 Protocols](#)
- [MPLS](#)
- [System Management](#)
- [Virtual Chassis and Virtual Chassis Fabric](#)

High Availability

- On an EX4300 Virtual Chassis that has performed a nonstop software upgrade (NSSU), multicast traffic is dropped for approximately ten minutes immediately after the NSSU because multicast groups do not immediately refresh. [PR1033594](#)

Interfaces and Chassis

- On EX Series switches, except for the EX4600 switch, if you configure an IPv4 GRE interface on an IPv6 interface, the GRE tunnel might not work properly. Traffic is not forwarded through the tunnel. [PR1008157](#)
- In a mixed QFX3500 and EX4300 Virtual Chassis configured for persistent MAC and MAC limiting, traffic is not received on aggregated Ethernet interfaces on EX4300 switches when the EX4300 switches are operating in the linecard role. [PR1033618](#)
- When a transceiver on a QFX5100, QFX3600, QFX3500, or EX4300 switch is removed and reinserted into an interface within 30 seconds after you issued the **set virtual-chassis vc-port set** command to convert the interface into a Virtual Chassis port (VCP), the VCP is not created. [PR1029829](#)
- An EX4600-EM-8F expansion module installed in a QFX5100-24Q switch or an EX4600 switch does not support the 100 Mbps speed on the 10-Gigabit Ethernet interfaces. [PR1032257](#)
- When an EX4600 or QFX5100 switch is downgraded from Junos OS Release 14.1X53-D15 or later to Junos OS Release 14.1X53-D10 or earlier, the 40-Gbps Ethernet interfaces on QSFP+ transceivers might not return to the up state. As a workaround, power cycle the switch after the Junos OS upgrade. [PR1061213](#)

J-Web

- On an EX Series switch using the J-Web interface, the J-web interface might pause indefinitely after STP, RSTP, or MSTP is selected from the Configure>Switching>Spanning tree menu. [PR1046051](#)

Layer 2 Protocols

- On an EX4300 switch, a MAC address that is specified as part of a MAC-based VLAN is authenticated on an interface, for example, xe-1/1/1, on which 802.1X authentication in multiple supplicant mode is configured. However, the same MAC address might not be authenticated on another interface, for example, xe-2/1/1, if the MAC address moves to interface xe-2/1/1 from interface xe-1/1/1. [PR1007589](#)

MPLS

- Up to 100 pseudowires are supported in active/backup configuration (cold standby). When more than 100 pseudowires are configured, traffic might not be forwarded correctly under certain scenarios. [PR1048500](#)
- When link-protection, node-link-protection, or fast-reroute is configured on high-traffic MPLS label-switched paths (LSPs), a traffic convergence delay of 680ms to 1.5 seconds

can occur. Link protection provides protection against a link failure along an RSVP label-switched path. Node-link protection establishes a bypass label-switched paths (LSP) through a different device. Fast reroute provides redundancy for an LSP path. [PR1039717](#)

System Management

- On EX Series and QFX Series switches that are configured with the **include-option-82 nak** option so that DHCP servers include option 82 information in NAK messages, two copies of option-82 might be appended to DHCP ACK packets. [PR1064969](#)

Virtual Chassis and Virtual Chassis Fabric

- On a Virtual Chassis with three EX2200 switch members, if you configure nine link aggregation groups and eight interfaces per LAG bundle, the LACP links might transition down and up continuously. As a workaround, configure eight link aggregation groups and eight interfaces per LAG bundle instead. [PR1030809](#)
- In a mixed QFX3500 and EX4300 Virtual Chassis with a QFX3500 switch acting in the master role, the Virtual Chassis mastership might change when the Virtual Chassis receives multicast traffic. A mixed QFX3500 and EX4300 Virtual Chassis with a QFX3500 switch acting in the master role is not a supported configuration in this release of Junos OS because of this issue. [PR1126216](#)

Related Documentation

- [New and Changed Features on page 4](#)
- [Changes in Behavior and Syntax on page 17](#)
- [Known Behavior on page 19](#)
- [Resolved Issues on page 24](#)
- [Documentation Updates on page 27](#)
- [Migration, Upgrade, and Downgrade Instructions on page 28](#)
- [Product Compatibility on page 29](#)

Resolved Issues

This section lists the issues fixed in the Junos OS main release and the maintenance releases.

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

- [Resolved Issues: Release 14.1X53-D27 on page 25](#)
- [Issues: Release 14.1X53-D26 on page 25](#)
- [Resolved Issues: Release 14.1X53-D25 on page 26](#)
- [Resolved Issues: Release 14.1X53-D16 on page 26](#)
- [Resolved Issues: Release 14.1X53-D10 on page 26](#)

Resolved Issues: Release 14.1X53-D27

No issues that were previously reported in any version of the Junos OS Release 14.1X53 release notes have been resolved in Junos OS Release 14.1X53-D27 for the EX Series switches.

Issues: Release 14.1X53-D26

Interfaces and Chassis

- On a mixed EX4300 and EX4600 Virtual Chassis, MAC learning sometimes stops happening on an interface after 802.1x is disabled. As a workaround, disable and re-enable the interface. [PR1070885](#)
- On EX4600 and QFX5100 switches, the 100Mbps LED functionality is not working. The LED does not glow when 100Mbps traffic is sent or received on the switch, and no output is displayed when the **show chassis led** command is entered to gather information on the 100Mbps interface. [PR1025359](#)

Resolved Issues: Release 14.1X53-D25

MPLS

- Layer 2 tagged traffic sent over an MPLS L2 circuit from one local customer edge (CE1) switch to another (CE2) might be dropped after an in-service software upgrade occurs in the provider edge (PE1) switch. However, traffic from CE2 to CE1 is not affected. In addition to the traffic loss, OSPF neighbors might be lost. OSPF is an interior gateway protocol (IGP) that routes packets within a single autonomous system (AS). [PR1044999](#)

Resolved Issues: Release 14.1X53-D16

Authentication and Access Control

- On EX4300 switches with 802.1X authentication configured, when an 802.1X-enabled interface flaps, the dot1x daemon (dot1xd) might generate frequent core files due to a memory leak. [PR1049635](#)

Interfaces and Chassis

- On EX4600 switches, disabling a member link of an AE interface might cause packets to be sent to a port that is down, which results in traffic loss. As a workaround, to restore service, bring the port that is down back up again. [PR1050260](#)

MPLS

- On EX Series switches, issuing a ping command does not work after disabling and re-enabling the interface. [PR1039743](#)

Port Security

- In a mixed-mode Virtual Chassis Fabric with storm control enabled, if autonegotiation is enabled on a 1-gigabit interface (the default setting), the storm-control value for allowed bandwidth might be set to 0, which would cause traffic to be dropped. As a workaround, manually configure the link speed instead of using autonegotiation. [PR1051756](#)

Spanning-Tree Protocols

- On EX4300 switches with VLAN Spanning Tree Protocol (VSTP) running on aggregated Ethernet interfaces, the root port might receive VSTP BPDUs that are intended for other interfaces (port IDs). This issue can cause the root bridge to flap. The issue can also cause the root bridge to dispute the BPDUs and not converge. [PR1066137](#)

Virtual Chassis and Virtual Chassis Fabric

- On the EX4600 and EX4300 Virtual Chassis, disabling and re-enabling LAG interfaces causes traffic failure. You must reboot for the interface to recover. [PR1044580](#)

VLAN Infrastructure

- On EX4300 switches, naming a VLAN "vlan-rewrite" causes an error when you commit the configuration. [PR1054996](#)

Resolved Issues: Release 14.1X53-D10

MPLS

- In certain scenarios, the pseudowire redundancy feature might not work as expected. [PR1013686](#)
- For MPLS FRR and L2 circuit, certain scenarios after an ISSU might not work as expected. As a workaround, restart the Packet Forwarding Engine. [PR1016513](#)

Port Security

- On an EX2200 or EX3300 Virtual Chassis, when DHCP snooping is enabled and 1000 or more IPv4 and 500 or more IPv6 DHCP bindings occur simultaneously, the software forwarding daemon (sfid) might create a core file. There might be a traffic impact because of the core file creation. [PR1019136](#)

Related Documentation

- [New and Changed Features on page 4](#)
- [Changes in Behavior and Syntax on page 17](#)
- [Known Behavior on page 19](#)
- [Known Issues on page 22](#)
- [Documentation Updates on page 27](#)
- [Migration, Upgrade, and Downgrade Instructions on page 28](#)
- [Product Compatibility on page 29](#)

Documentation Updates

This section lists changes and errata in Junos OS Release 14.1X53 for the EX Series switches documentation.

- [Bridging and Learning on page 27](#)
- [Security on page 28](#)

Bridging and Learning

- Two new MIBs related to MAC notification are provided at Junos OS Release 14.1X53-D10:
 - `jnxL2aldMacHistoryEntry`
 - `jnxL2aldMacNotificationMIBGlobalObjects`

These MIBs are not yet described in the documentation.

Security

- Media Access Control Security (MACsec) support (EX4600 switches) was added in Junos OS Release 14.1X53-D15, but that feature was not listed in the first versions of the Junos OS Release 14.1X53-D15 release notes. We have added the feature listing in revision 3 of the release notes. See *New and Changed Features*.

Related Documentation

- [New and Changed Features on page 4](#)
- [Changes in Behavior and Syntax on page 17](#)
- [Known Behavior on page 19](#)
- [Known Issues on page 22](#)
- [Resolved Issues on page 24](#)
- [Migration, Upgrade, and Downgrade Instructions on page 28](#)
- [Product Compatibility on page 29](#)

Migration, Upgrade, and Downgrade Instructions

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

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

- [Upgrade and Downgrade Support Policy for Junos OS Releases on page 28](#)

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

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

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

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

**Related
Documentation**

- [New and Changed Features on page 4](#)
- [Changes in Behavior and Syntax on page 17](#)
- [Known Behavior on page 19](#)
- [Known Issues on page 22](#)
- [Resolved Issues on page 24](#)
- [Documentation Updates on page 27](#)
- [Product Compatibility on page 29](#)

Product Compatibility

- [Hardware Compatibility on page 29](#)

Hardware Compatibility

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

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

<http://pathfinder.juniper.net/feature-explorer/>

**Related
Documentation**

- [New and Changed Features on page 4](#)
- [Changes in Behavior and Syntax on page 17](#)
- [Known Behavior on page 19](#)
- [Known Issues on page 22](#)
- [Resolved Issues on page 24](#)
- [Documentation Updates on page 27](#)
- [Migration, Upgrade, and Downgrade Instructions on page 28](#)

Junos OS Release Notes for the QFX Series

These release notes accompany Junos OS Release 14.1X53-D27 for the QFX Series. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

The following QFX Series platforms are supported in Junos OS Release 14.1X53-D27: QFX3500, QFX3600, and QFX5100.



NOTE: These release notes include information on all Junos OS Release 14.1X53 releases. Therefore, information about QFX Series platforms that are not supported in Junos OS Release 14.1X53-D27 but are supported in other Junos OS Release 14.1X53 releases are included in these release notes.

- [New and Changed Features on page 30](#)
- [Changes in Behavior and Syntax on page 49](#)
- [Known Behavior on page 51](#)
- [Known Issues on page 60](#)
- [Resolved Issues on page 63](#)
- [Documentation Updates on page 68](#)
- [Migration, Upgrade, and Downgrade Instructions on page 69](#)
- [Product Compatibility on page 74](#)

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 14.1X53 for the QFX Series. To view the entire set of software information in PDF format, see the [Complete Software Guide for Junos OS for the QFX Series](#).

- [New Features in Release 14.1X53-D27 on page 30](#)
- [New Features in Release 14.1X53-D26 on page 31](#)
- [New Features in Release 14.1X53-D25 on page 32](#)
- [New Features in Release 14.1X53-D15 on page 33](#)
- [New Features in Release 14.1X53-D10 on page 38](#)

New Features in Release 14.1X53-D27

Hardware

- **QFX5100-24Q-AA switch**—This low-latency, high-performance, top-of-rack switch provides 2.56 Tbps throughput. Each QSFP+ port supports 40-Gigabit Ethernet but can be configured as four independent 10-Gigabit Ethernet ports using breakout cables (channelization mode). The switch can also be configured to support 96 10-Gigabit Ethernet ports using breakout cables (channelization mode) with 1280-Gbps total throughput.

The switch can be ordered with either ports-to-FRUs or FRUs-to-ports airflow and with AC or DC power supplies.

The QFX5100-24Q-AA module bay can accommodate a single double-wide expansion module (QFX-PFA-4Q) and two single-wide optional expansion modules (two or one each of QFX-EM-4Q and EX4600-EM-8F).

- **QFX-PFA-4Q expansion module (QFX5100-24Q-AA switch)**—Starting with Junos OS Release 14.1X53-D27, the QFX5100-24Q-AA switch supports the QFX-PFA-4Q expansion module. This double-wide expansion module provides four additional 40-Gigabit Ethernet QSFP+ ports, a dedicated FPGA, and support for the Precision Time Protocol (PTP).

New Features in Release 14.1X53-D26

Network Management and Monitoring

- **DHCP smart relay (QFX5100)**—Starting with Junos OS Release 14.1X53-D26, you can configure alternative IP addresses for the gateway interface so that if the server fails to reply to the requests sent from the primary gateway address, the switch can resend the requests using alternative gateway addresses. To use this feature, you must configure an IRB interface or Layer 3 subinterface with multiple IP addresses and configure that interface as a relay agent.

Open vSwitch Database (OVSDB)

- **New OVSDB Command Summaries (QFX5100, QFX5100VC)**—Starting with Junos OS Release 14.1X53-D26, the **show ovssdb commit failures** and **clear ovssdb commit failures** commands are introduced.

If you suspect a problem has occurred with the configuration of an OVSDB-managed Virtual Extensible LAN (VXLAN) and associated logical interface(s), you can enter the **show ovssdb commit failures** command. This command describes the OVSDB-managed VXLANs and associated logical interface(s) that the Juniper Networks switch automatically configured but was unable to commit.

After you resolve the problem, you can remove the configuration from the queue and retry committing the configuration by using the **show ovssdb commit failures** command.

- **Storm control on OVSDB-managed interfaces (QFX5100)**—Starting with Junos OS Release 14.1X53-D26, you can configure storm control on VXLAN interfaces that are managed by an OVSDB controller. By default, Layer 2 BUM traffic that originates in an OVSDB-managed VXLAN is replicated and forwarded by a service node in the same VXLAN. Because service nodes can be overloaded if too much BUM traffic is received, you can manually configure storm control on server-facing VXLAN interfaces to control how much of this traffic is allowed into a VXLAN.

New Features in Release 14.1X53-D25

MPLS

- **MPLS stitching for virtual machine connections (QFX5100, QFX3500)**—By using MPLS, the stitching feature provides connectivity between virtual machines on opposite sides of data center routers. An external controller, programmed in the data plane, assigns MPLS labels to both virtual machines and servers. Then, the signaled MPLS labels are used between the data center routers, generating static label-switched paths (LSPs), resolved over RSVP or LDP, to provide the routes dictated by the labels. The new CLI command **stitch**, located under the LSP **transit** command, provides this capability.

[See [MPLS Stitching For Virtual Machine Connection](#).]

Open vSwitch Database (OVSDB)

- **OVSDB schema updates (QFX5100 switch, QFX5100 Virtual Chassis)**—Starting with Junos OS Release 14.1X53-D25, the Open vSwitch Database (OVSDB) schema for physical devices version that is implemented on QFX5100 switches is version 1.3.0. In addition, this schema now supports the multicast MACs local table.

[See [Open vSwitch Database Schema for Physical Devices](#).]

Software Installation and Upgrade

- **Preboot eXecution Environment (PXE) software for Junos Fusion satellite devices (QFX5100 switches)**—Enables you to convert a Junos Fusion satellite device back into a standalone QFX5100 switch. For more information on this feature, please see the Junos OS 14.2R3 Release Notes and the Junos Fusion documentation.

System Management

- **DHCP relay with DHCP server and DHCP client in separate routing instances**—You can use a stateless DHCP relay agent between a client and server in different virtual routing instances. This feature uses cross-message exchange between the virtual routing instances and supports both DHCPv4 and DHCPv6 packets. This method ensures that:
 - DHCP server network is isolated from the DHCP clients, because there is no direct routing between the client's and server's routing instances.
 - Only DHCP packets, not routine traffic, are relayed across the two routing instances.

[See [DHCP Message Exchange Between DHCP Clients and DHCP Server in Different Virtual Routing Instances](#).]

- **Precision Time Protocol (PTP) transparent clock (QFX5100 switch)**—PTP synchronizes clocks throughout a packet-switched network. With a transparent clock, the PTP packets are updated with residence time as the packets pass through the switch. There is no master/slave designation. With an end-to-end transparent clock, only the residence time is included. The residence time can be sent in a one-step process, which means that timestamps are sent in one packet. In a two-step process, estimated timestamps are sent in one packet, and additional packets contain updated

timestamps. In addition, user UDP over IPv4 and IPv6, and unicast and multicast transparent clocks are supported. You can configure the transparent clock at the [edit protocols ptp] hierarchy level.

[See [Understanding Transparent Clocks in Precision Time Protocol.](#)]

VXLAN

- **Configurable VXLAN UDP Port (QFX5100)**—Starting with Junos OS 14.1X53-D25, you can configure the UDP port used as the destination port for VXLAN traffic on a QFX5100 switch. To configure the VXLAN destination port to be something other than the default UDP port of 4789, enter **set protocols l2-learning destination-udp-port port-number**. The port you configure will be used for all VXLANs configured on the switch. [See [Understanding VXLANs.](#)]



NOTE: If you make this change on one switch in a VXLAN, you must make the same change on all the devices that terminate the VXLANs configured on your switch. If you do not do so, traffic will be disrupted for all the VXLANs configured on your switch. When you change the UDP port, the previously learned remote VTEPs and remote MACs are lost and VXLAN traffic is disrupted until the switch relearns the remote VTEPs and remote MACs.

New Features in Release 14.1X53-D15

Hardware

- **Extended node support (QFX5100-24Q and QFX5100-48T switches)**—Enables you to include a QFX5100-24Q switch and a QFX5100-48T switch as a Node device in a QFabric System. To add the device, first install the QFabric “5” family software package (jinstall-qfabric-5-release.tgz) on the switch, and attach two management ports to the QFabric system control plane. For copper-based control plane systems, use the RJ-45 fixed management port and one SFP management port on the QFX5100 Node device with a copper module. For fiber-based control plane systems, use two SFP management ports on the QFX5100 Node device with fiber modules.

[See [Understanding the QFabric System Hardware Architecture .](#)]

- **Improved online insertion and replacement procedures (QFabric systems)**—Allows for non-disruptive insertion or replacement of server Node groups, network Node groups, redundant server Node groups, Interconnect devices, and front and rear cards of the Interconnect devices.

[See [Powering Off an Existing QFabric Node Device .](#)]

- **QFX5100 Interconnect Device (QFabric Systems)** Allows a QFX5100-24Q switch to operate as a QFX3000-M interconnect device. The interconnect acts like a backplane for data plane traffic traversing the QFX3000-M QFabric System between Node devices. The QFX5100 interconnect device has 24 40-Gigabit QSFP+ ports, but only 16 are available as fte ports. The QFX5100 interconnect device features two RJ-45

management ports and two SFP managements ports, which allow connection to either copper-based or fiber-based control plane networks.

[See [Understanding Interconnect Devices](#) .]

Class of Service

- **Mitigating fate sharing on Interconnect devices by remapping forwarding classes (QFabric systems)**—Enables you to remap traffic assigned to a forwarding class into different, separate forwarding classes to mitigate fate sharing as the traffic crosses the Interconnect device. Separating the traffic into multiple forwarding classes spreads the flows across multiple output queues instead of using one output queue for all of the traffic. (Each forwarding class uses a different output queue, and each output queue has its own dedicated bandwidth resources.) Fate sharing occurs when flows in the same forwarding class (flows that have the same IEEE 802.1p priority code point) use the same output queue on an interface, because the flows share the same path and resources. When one flow becomes congested, the congestion can affect the other flows that use the same output queue even if they are not experiencing congestion, because when the congested flow is paused, the other flows that use the same code point are also paused. Because flows from many Node devices cross the Interconnect device, the flows are aggregated at egress interfaces, which increases the chance of fate sharing. Forwarding class remapping mitigates fate sharing on the Interconnect device by separating the traffic into different forwarding classes that use different output queues, so pausing one congested flow does not affect uncongested flows that have been mapped to different forwarding classes and therefore to different output queues.

[See [Understanding How to Mitigate Fate Sharing on a QFabric System Interconnect Device by Remapping Traffic Flows \(Forwarding Classes\)](#) and [Understanding Default CoS Scheduling on QFabric System Interconnect Devices \(Junos OS Release 13.1 and Later Releases\)](#) .]

- **Scheduler configuration on Interconnect device fabric ports (QFabric systems)**—Enables you to configure scheduling on the fabric (fte and bfte) ports of the QFabric system Interconnect devices. (This complements the Junos OS Release 13.1 feature that provides scheduler configuration on Node device fabric ports. The combination of access port, Node device fabric port, and Interconnect device fabric port scheduling gives you complete control of scheduling across a QFabric system.) In earlier Junos OS releases, Interconnect device fabric port scheduling was done by default, with no user configuration. In Junos OS Release 14.1X53-D15, the default fabric port scheduler on Interconnect devices is the same as it was in earlier releases.

[Understanding CoS Scheduling Across the QFabric System](#) and [Understanding Default CoS Scheduling on QFabric System Interconnect Devices \(Junos OS Release 13.1 and Later Releases\)](#) .]

Multicast Features

- **IGMP querier (QFabric Systems)**—Enables multicast traffic to be forwarded between connected switches in pure Layer 2 networks. If you enable IGMP snooping in a Layer 2 network without a multicast router, the IGMP snooping reports are not forwarded between connected switches. This means that if hosts connected to different switches in the network join the same multicast group and traffic for that group arrives on one of the switches, the traffic is not forwarded to the other switches that have hosts that should receive the traffic. If you enable IGMP querying for a VLAN, multicast traffic is forwarded between switches that participate in the VLAN if they are connected to hosts that are members of the relevant multicast group.

[See [Using a Switch as an IGMP Querier](#) .]

- **IGMPv3 (QFabric Systems)**—Introduces support for IGMP (Internet Group Management Protocol) version 3 (IGMPv3). IGMPv3 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 routing devices. Multicast routing devices use IGMP to learn which groups have members for each of their attached physical networks.

[See [Understanding IGMP](#) .]

- **IGMPv3 snooping (QFabric systems)**—With IGMP snooping enabled (the default setting), a switch monitors the IGMP traffic between hosts and multicast routers and uses what it learns to forward multicast traffic to only the downstream interfaces that are connected to interested receivers. This conserves bandwidth by allowing the switch to send multicast traffic to only those interfaces that are connected to devices that want to receive the traffic (instead of flooding the traffic to all the downstream VLAN interfaces).

[See [IGMP Snooping Overview](#) .]

- **Multicast flow groups (QFabric systems)**—Node devices usually forward multicast traffic on all available interconnect devices to distribute the load balancing replication load. As a result, redundant multicast streams can flow through one interconnect device, making that interconnect device a potential single point of failure for the redundant flows. Some applications require that the redundant multicast streams flow through different interconnect devices to prevent a single interconnect device from potentially dropping both streams of multicast traffic during a failure. You can enforce this use of dual interconnect devices by using the QFabric flow segregation feature.

[See [Understanding QFabric Multicast Flow Groups](#) .]

- **PIM-SSM (QFabric systems)**—Protocol Independent Multicast source-specific multicast (PIM-SSM) uses a subset of PIM sparse mode and IGMP version 3 (IGMPv3) to enable a client to receive multicast traffic directly from the source. PIM SSM uses the PIM sparse-mode functionality to create a shortest-path tree (SPT) between the client and the source, but builds the SPT without the help of a rendezvous point.

[See [PIM SSM](#) .]

Network Management and Monitoring

- **Cloud Analytics Engine (QFX5100 switches)**—Uses network data analysis to improve application performance and availability. Cloud Analytics Engine includes data collection, analysis, correlation, and visualization, helping you better understand the behavior of workloads and applications across the physical and virtual infrastructure. Cloud Analytics Engine provides an aggregated and detailed level of visibility, tying applications and the network together, and an application-centric view of network status, improving your ability to quickly roll out new applications and troubleshoot problems.

[See [Cloud Analytics Engine](#) .]

Open vSwitch Database (OVSDB)

- **Automatic configuration of OVSDB-managed VXLANs with trunk interfaces (QFX5100 switches)**—In a VMware NSX for Multi-Hypervisor environment for the data center, the QFX5100 switch can automatically configure an OVSDB-managed VXLAN and one or more interfaces associated with the VXLAN, thereby eliminating the need for you to perform these tasks, using the Junos OS CLI. The automatic configuration of the VXLAN and associated interfaces is based on the configuration of a logical switch in NSX Manager or in the NSX API. Starting in Junos OS Release 14.1X53-D15, the switch supports the automatic configuration of trunk interfaces and their association with an OVSDB-managed VXLAN. In this situation, trunk interfaces enable the support of multiple software applications running directly on a physical server that generate traffic that must be isolated by OVSDB-managed VXLANs.

[See [Understanding How to Set Up Virtual Extensible LANs in an Open vSwitch Database Environment](#) .]

QFabric Systems

- **QFabric system software downgrade support (QFabric systems)**—Starting with Junos OS 14.1X53-D15, downgrading software provides a quick recovery mechanism to a previous software version and configuration file in cases where a software upgrade or configuration changes have made the QFabric system unstable or inoperable. The recovery mechanism consists of a “restore-point,” which is a snapshot of the software on the QFabric system as well as the configuration that can be rolled back to. Downgrade support does not replace the existing backup and restore functionality.
 - To enable software downgrade:
 - Create a restore-point.



NOTE: You can only create one restore-point at a time. Creating a new restore-point deletes the existing restore-point if there is one. Also, all CLI commands are blocked while creating a restore-point.

To create a restore-point, issue the **request system software restore-point** command.

- To roll back to the restore-point, issue the **request system software recover-from-restore-point** command.
- To display the status of the Director group after creating a restore-point for the QFabric system, issue the **show system software restore-point status** command.

Security

- **Error message displayed when TCAM is full (QFX5100 switches)**—Firewall filters are stored in ternary content addressable memory (TCAM). With previous versions of Junos OS, if you configure a firewall filter that cannot fit into the available TCAM space, the filter defaults to "permit any," and no error message is displayed in the CLI. With Junos OS Release 14.1X53-D15, an error message is displayed in the CLI if this occurs.

[See [Planning the Number of Firewall Filters to Create](#) .]

- **Media Access Control Security (MACsec) support (QFX5100-24Q switches)**—Starting with Junos OS Release 14.1X53-D15, MACsec is supported on all eight SFP+ interfaces on the EX4600-EM-8F expansion module when it is installed in a QFX5100-24Q switch. MACsec is an industry-standard security technology that provides secure communication for all traffic on point-to-point Ethernet links. MACsec is capable of identifying and preventing most security threats, and can be used in combination with other security protocols to provide end-to-end network security. MACsec is standardized in IEEE 802.1AE.

[See [Understanding Media Access Control Security \(MACsec\)](#) .]

Virtual Chassis and Virtual Chassis Fabric

- **Increase vmember limit to 512k support (Virtual Chassis Fabric)**—Increases number of vmembers to 512k. For example, to calculate how many interfaces are required to support 4,000 VLANs, divide the maximum number of vmembers (512,000) by the number of configured VLANs (4,000). In this case, 128 interfaces are required.

[See [Understanding Bridging and VLANs.](#)]

VLAN Infrastructure

- **Support for private VLANs (QFX5100 switches)**—VLANs limit broadcasts to specified users. Private VLANs (PVLANS) take this concept a step further by splitting the broadcast domain into multiple isolated broadcast subdomains and essentially putting secondary VLANs inside a primary VLAN. PVLANS restrict traffic flows through their member switch ports (called “private ports”) so that these ports communicate only with a specified uplink trunk port or with specified ports within the same VLAN. The uplink trunk port is usually connected to a router, firewall, server, or provider network. Each PVLAN typically contains many private ports that communicate only with a single uplink, thereby preventing the ports from communicating with each other.

Just like regular VLANs, PVLANS are isolated on Layer 2 and require that a Layer 3 device be used to route traffic among them. PVLANS are useful for restricting the flow of broadcast and unknown unicast traffic and for limiting the communication between known hosts. Service providers use PVLANS to keep their customers isolated from one another.

[See [Understanding Private VLANs.](#)]

New Features in Release 14.1X53-D10

Authentication and Access Control

- **IPv6 for RADIUS AAA (QFX5100 switch and Virtual Chassis)**—Starting with Junos OS Release 14.1X53-D10, QFX5100 switches and QFX5100 Virtual Chassis support IPv6, along with the existing IPv4 support, for user authentication, authorization, and accounting (AAA) using RADIUS servers.

RADIUS authentication is a method of authenticating users who attempt to access the router or switch. To use RADIUS authentication on the switch, configure information about one or more RADIUS servers on the network by including one **radius-server** statement at the **[edit system]** hierarchy level for each RADIUS server.

When you configure a source address for each configured RADIUS server, each RADIUS request sent to a RADIUS server uses the specified source address.

- **Authentication**—Specify which source address Junos OS uses when accessing your network to contact an external RADIUS server for authentication. You configure the IPv6 source address for RADIUS authentication at the **[edit system radius-server server-address source-address]** hierarchy level.
- **Accounting**—Specify which source address Junos OS uses when contacting a RADIUS server for sending accounting information. You configure the IPv6 source address

for RADIUS authentication at the `[edit system accounting destination radius server server-address source-address]` hierarchy level.

[See [source-address](#).]

Bridging and Learning

- **MAC notification (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, MAC notification is supported on QFX5100 switches. The switches track clients on a network by storing MAC addresses in the Ethernet switching table on the switch. When switches learn or unlearn a MAC address, SNMP notifications can be sent to the network management system at regular intervals to record the addition or removal of the MAC address. This process is known as MAC notification.

The MAC Notification MIB controls MAC notification for the network management system.

The MAC notification interval defines how often these SNMP notifications are sent to the network management system. The MAC notification interval works by tracking all MAC address additions or removals on the switch over a period of time and then sending all tracked MAC address additions or removals to the network management server at the end of the interval.

Enabling MAC notification allows you to monitor the addition and removal of MAC addresses from the Ethernet switching table remotely using a network management system. The advantage of setting a high MAC notification interval is that the amount of network traffic is reduced because updates are sent less frequently. The advantage of setting a low MAC notification interval is that the network management system is better synchronized with the switch.

Two new MIBs related to MAC notification are provided at Junos OS Release 14.1X53-D10. See *Documentation Updates*.

[See [Configuring MAC Notification \(CLI Procedure\)](#).]

- **Default VLAN and multiple VLAN range support (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, the default VLAN and multiple VLAN range are supported on QFX5100 switches. They provide the ability for the switch to operate as a *plug and play* device and connect to various Ethernet-enabled devices in a small, scaled enterprise network. When the switch boots, a VLAN named **default** is created. The default VLAN is automatically created for every routing instance that belongs to a type of **virtual-switch** and for the default routing instance named **default-switch**. All interfaces on the switch are automatically configured as access interfaces and are part of the default VLAN.

The default VLAN accepts and forwards untagged packets only and is preconfigured with a VLAN ID (**vlan-id**) of 1. The default VLAN does not support a VLAN ID list (**vlan-id-list**), **vlan-id** set to **all**, or **vlan-id** set to **none**. You can configure the VLAN ID to be another value, but the value must be between 1 and 4093.

Access interfaces that are VoIP-enabled or 802.1X-enabled are internally converted to trunk interfaces, so that the interfaces can belong to multiple VLANs. If the interfaces do not belong to a valid VLAN, the interfaces automatically become part of the default VLAN.

You can configure more than one VLAN range, and each range can contain unique VLAN properties.



NOTE: Virtual Chassis interfaces cannot be preconfigured to belong to the default VLAN or any other VLAN.



NOTE: For interfaces to be part of the default VLAN, you must configure the interfaces to be part of the Ethernet switching family. You can configure Ethernet switching at the [edit interfaces *interface-name* unit family] CLI hierarchy level.

- **Ethernet ring protection switching (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, Ethernet ring protection switching (ERPS) is supported on QFX5100 switches. ERPS helps achieve high reliability and network stability. Links in the ring never form loops that fatally affect the network operation and services availability.

[See [Understanding Ethernet Ring Protection Switching Functionality](#).]

High Availability

- **Resilient hashing support for link aggregation groups and equal cost multipath routes (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, resilient hashing is now supported by link aggregation groups (LAGs) and equal cost multipath (ECMP) sets.

A LAG combines Ethernet interfaces (members) to form a logical point-to-point link that increases bandwidth, provides reliability, and allows load balancing. Resilient hashing enhances LAGs by minimizing destination remapping when a new member is added to or deleted from the LAG.

Resilient hashing works in conjunction with the default static hashing algorithm. It distributes traffic across all members of a LAG by tracking the flow's LAG member utilization. When a flow is affected by a LAG member change, the packet forwarding engine (PFE) rebalances the flow by reprogramming the flow set table. Destination paths are remapped when a new member is added to or existing members are deleted from a LAG.

Resilient hashing applies only to unicast traffic and supports a maximum of 1024 LAGs, with each group having a maximum of 256 members.

An ECMP group for a route contains multiple next-hop equal cost addresses for the same destination in the routing table. (Routes of equal cost have the same preference and metric values.)

Junos OS uses a hash algorithm to choose one of the next-hop addresses in the ECMP group to install in the forwarding table. Flows to the destination are rebalanced using resilient hashing.

Resilient hashing enhances ECMPs by minimizing destination remapping when a new member is added to or deleted from the ECMP group.

[See [Understanding the Use of Resilient Hashing to Minimize Flow Remapping in Trunk Groups](#).]

Infrastructure

- **Licensing enhancements (QFX Series)**—Starting with Junos OS Release 14.1X53-D10, licensing enhancements on QFX Series switches enable you to configure and delete license keys in a Junos OS CLI configuration file. The license keys are validated and installed after a successful commit of the configuration file. If a license key is invalid, the commit fails and issues an error message. You can configure individual license keys or multiple license keys by issuing Junos OS CLI commands or by loading the license key configuration contained in a file. All installed license keys are stored in the `/config/license/` directory.

To install an individual license key in the Junos OS CLI, issue the **set system license keys key *name*** command, and then issue the **commit** command.

For example:

[edit]


```
root@switch# set system license keys key "JUNOS_TEST_LIC_FEAT aeaqeb qbmqds
qwwsxe okyvou 6v57u5 zt6ie6 uwl3zh assvnu e2ptl5 soxawy vtfh7k axwnno m5w54j
6z"
root@switch# commit
commit complete
```

To verify that the license key was installed, issue the **show system license** command.

For example:

```
root@switch> show system license
License usage:

```

Feature name	Licenses used	Licenses installed	Licenses needed	Expiry
sdk-test-feat1	0	1	0	permanent

```

Licenses installed:
License identifier: JUNOS_TEST_LIC_FEAT
License version: 2
Features:
  sdk-test-feat1 - JUNOS SDK Test Feature 1
  permanent
```

To install multiple license keys in the Junos OS CLI, issue the **set system license keys key *name*** command, and then issue the **commit** command.

For example:

```
[edit]
root@switch# set system license keys key "key_1"
set system license keys key "key_2"
set system license keys key "key_2"
set system license keys key "key_4"
root@switch# commit
commit complete
```

To verify that the license key was installed, issue the **show system license** command.

To install an individual license key configuration in a file, issue the **cat** command:

For example:

```
[edit]
root@switch%cat license.conf
system {
  license {
    keys {
      key "JUNOS_TEST_LIC_FEAT aeaqeb qbmqds qwwsxe okyvou 6v57u5 zt6ie6
uwl3zh assvnu e2ptl5 soxawy vtfh7k axwnno m5w54j 6z";
    }
  }
}
```

Load and merge the license configuration file.

For example:

```
[edit]
root@switch# load merge license.conf
load complete
```


Issue the **show | compare** command to see the configuration, and then issue the **commit** command.

For example:

```
[edit]
root@switch# show | compare
[edit system]
+ license {
+   keys {
+     key "JUNOS_TEST_LIC_FEAT aeaqeb qbmqds qwwsxe okyvou 6v57u5 zt6ie6
uwl3zh assvnu e2ptl5 soxawy vtfh7k axwnno m5w54j 6z";
+   }
+ }
[edit]
root@switch# commit
```

To verify that the license key was installed, issue the **show system license** command.

For example:

```
root@switch> show system license
License usage:
           Licenses  Licenses  Licenses  Expiry
Feature name    used  installed  needed
sdk-test-feat1      0      1      0  permanent

Licenses installed:
License identifier: JUNOS_TEST_LIC_FEAT
License version: 2
Features:
  sdk-test-feat1 - JUNOS SDK Test Feature 1
  permanent
```

To install multiple license keys in a file, issue the **cat** command:

For example:

```
[edit]
root@switch%cat license.conf
system
{
  license
  {
    keys
    {
      key "key_1"
      key "key_2"
      key "key_3"
      ...
      key "key_n"
    }
  }
}
```

Load and merge the license configuration file, and then issue the **commit** command.

For example:

```
[edit]
```



```
root@switch# load merge license.conf
load complete
[edit]
root@switch# commit
```

To verify that the license key was installed, issue the **show system license** command.

You can also delete or deactivate individual and multiple license keys in the Junos OS CLI by issuing the **delete system license keys** or **deactivate system license keys** commands. Do not use the **request system license delete** command to delete the license keys.

For example, to issue the **delete system license keys** command:

```
[edit]
root@switch# delete system license keys
root@switch# commit
```

Interfaces and Chassis

- **Fast reboot option (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, you can enhance the reboot time on a QFX5100 by issuing the new **fast-boot** option with the **request system reboot** command (**request system reboot fast-boot**). The switch reboots in such a way as to minimize downtime of network ports by not bringing the network ports down immediately as in the normal reboot option. There is minimal traffic loss while the forwarding device is reprogrammed.

[See [request system reboot](#).]

- **Keep a link up on a multichassis link aggregation group (MC-LAG) when LACP is not configured on one of the MC-LAG peers (QFX5100 switch)**—Junos OS Release 14.1X53-D10 provides connectivity from provider edge devices to customer edge devices when LACP is not configured on a customer edge device. The customer edge device must have one link connected to the provider edge device, though, and multichassis link aggregation must be configured between the provider edge devices in the MC-LAG. You can configure the force-up feature in Link Aggregation Control Protocol (LACP) on the provider edge device for which you need connectivity. Additionally, only one member interface in the aggregated Ethernet interface can be active, otherwise the provider edge device will receive duplicate packets.

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

Layer 3 Features

- **Loop-free alternate (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, QFX5100 switches support loop-free alternates (LFA) to compute backup next hops for IS-IS routes, providing IP fast-reroute capability for IS-IS routes. These routes, with precomputed backup next hops, are preinstalled in the Packet Forwarding Engine, which performs a local repair and switches to the backup next hop when the link for the primary next hop for a particular route is no longer available. With local repair, the Packet Forwarding Engine can correct a path failure before it receives recomputed paths from the Routing Engine. Local repair reduces the amount of time needed to reroute traffic to less than 50 milliseconds. You can configure loop free alternates (LFA) for IS-IS at the **[edit protocols isis]** hierarchy level.

- **IS-IS support (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, on QFX5100 switches, the IS-IS protocol has extensions to differentiate between different sets of routing information sent between routers and switches for unicast and multicast. IS-IS routes can be added to the RPF table when special features such as traffic engineering and shortcuts are turned on. You configure the feature under the **[edit protocols isis]** hierarchy level.

MPLS

- **MPLS-based Layer 3 VPNs (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, MPLS-based Layer 3 VPNs are supported on QFX5100 switches.

Customer networks are private and can use either public addresses or private addresses. When customer networks that use private addresses connect to the public Internet infrastructure, the private addresses might overlap with private addresses being used by other network users. MPLS BGP VPNs solve this problem by adding the route distinguisher prefix to the route.

You can configure the switch as a CE or PE using Layer 3 MPLS/BGP VPN for interprovider and carrier-of-carrier VPNs. The key difference between interprovider and carrier-of-carriers VPNs is whether the customer sites belong to the same autonomous system (AS) or to a separate AS:

- **Interprovider VPNs**—The customer sites belong to different ASs. You need to configure EBGP to exchange the customer's external routes.
- **Carrier-of-carriers VPNs**—The customer sites belong to the same AS. You need to configure IBGP to exchange the customer's external routes.
- **Ethernet-over-MPLS (L2 circuit) (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, Ethernet-over-MPLS is supported on QFX5100 switches. Ethernet-over-MPLS enables you to send Layer 2 Ethernet frames transparently over an MPLS cloud. Ethernet-over-MPLS uses a tunneling mechanism for Ethernet traffic through an MPLS-enabled Layer 3 core. It encapsulates Ethernet protocol data units (PDUs) inside MPLS packets and forwards the packets, using label stacking, across the MPLS network. This technology has applications in service provider, enterprise, and data center environments. For disaster recovery purposes, data centers are hosted in multiple sites that are geographically distant and interconnected using a WAN network. These data centers require Layer 2 connectivity between them for the following reasons:
 - To replicate the storage over Fibre Channel over IP (FCIP). FCIP works only on the same broadcast domain.
 - To run a dynamic routing protocol between the sites.
 - To support high availability clusters that interconnect the nodes hosted in the various data centers.
- **MPLS LSP protection (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, the following types of MPLS LSP protection are supported on QFX5100 switches:
 - Fast reroute (FRR)

- Link protection
- Node link protection

[See [MPLS Overview](#).]

Network Management and Monitoring

- **Chef for Junos OS (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, Chef for Junos OS is supported on all QFX5100 switches, not just QFX5100 switches that are running Junos OS with automated enhancements for QFX5100 switches.
- **Puppet for Junos OS (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, Puppet for Junos OS is supported on QFX5100 switches that are not running Junos OS with automated enhancements for QFX5100 switches.
- **IEEE 802.3ah (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, QFX5100 switches support the IEEE 802.3ah standard for the Operation, Administration, and Maintenance (OAM) of Ethernet in networks. The standard defines OAM link fault management (LFM). You can configure IEEE 802.3ah OAM LFM on point-to-point Ethernet links that are connected either directly or through Ethernet repeaters. Ethernet OAM provides the tools that network management software and network managers can use to determine how a network of Ethernet links is functioning. You configure the feature under the **[edit protocols oam ethernet]** hierarchy level.

OpenFlow

- **Support for OpenFlow v1.0 and v1.3.1 (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, QFX5100 switches support OpenFlow v1.0 and v1.3.1. OpenFlow v1.0 enables you to control traffic in an existing network by adding, deleting, and modifying flows in the switch. You can configure one OpenFlow virtual switch and one active OpenFlow controller under the **[edit protocols openflow]** hierarchy on each QFX5100 switch in the network.

In addition to the OpenFlow v1.0 functionality, OpenFlow v1.3.1 allows the action specified in one or more flow entries to direct packets to a base action called a group. The purpose of the group action is to further process these packets and assign a more specific forwarding action to them. You can view groups that were added, modified, or deleted from the group table by way of the OpenFlow controller using the **show openflow groups** command. You can view group statistics using the **show openflow statistics groups** command.

OpenFlow v1.0 and v1.3.1 are not supported on MX Series routers or EX9200 switches in Junos OS Release 14.1X53-D10. OpenFlow v1.0 is supported in Junos OS Release 14.1 on these platforms.

[See [Understanding OpenFlow Operation and Forwarding Actions on Devices Running Junos OS.](#)]

Open vSwitch Database (OVSDB)

- **OVSDB support (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, the Junos OS implementation of the Open vSwitch Database (OVSDB) management protocol provides a means through which VMware NSX controllers and QFX5100 switches that support OVSDB can communicate. In an NSX multi-hypervisor environment, NSX version 4.0.3 controllers and QFX5100 switches can exchange control and statistical information via the OVSDB schema for physical devices, thereby enabling virtual machine (VM) traffic from entities in a virtual network to be forwarded to entities in a physical network and vice versa.

You can set up a connection between the QFX5100 management interface (**em0** or **em1**) and an NSX controller.

[See [Setting Up Open vSwitch Database Connections Between Junos OS Devices and Controllers.](#)]

Security

- **Port mirroring to IP address (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, you can send mirrored packets to an IP address over a Layer 3 network (for example, if there is no Layer 2 connectivity to the analyzer device). This feature also enables you to apply an IEEE-1588 timestamp to the mirrored packets.

Software Installation

- **Open Source Python modules supported in automation enhancement (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, these Open Source Python modules are pre-installed in the jinstall-qfx-5-flex-x.tgz software bundle:

- **ncclient**—Facilitates client scripting and application development through the NETCONF protocol.
- **lxml**—Combines the speed and XML feature completeness of the C libraries libxml2 and libxslt with the simplicity of a native Python API.
- **jinja2**—Serves as a fast, secure, designer-friendly templating language.

[See [Overview of Python with QFX5100 Switch Automation Enhancements.](#)]

Virtual Chassis and Virtual Chassis Fabric

- **Alias support for Virtual Chassis and Virtual Chassis Fabric (VCF) nodes**—Starting with Junos OS Release 14.1X53-D10, an alias can be used to label nodes in a Virtual Chassis and VCF. An alias allows you to more clearly identify a member switch in your Virtual Chassis or VCF by assigning a text label to it. The text label appears alongside the switch's serial number whenever operational commands, such as **show virtual-chassis**, are used to monitor Virtual Chassis status.

[See [aliases.](#)]

- **Local link bias support for Virtual Chassis with QFX Series member switches**—Starting with Junos OS Release 14.1X53-D10, Virtual Chassis Local Link Bias is available on Link Aggregation Group (LAG) bundles on QFX3500 Virtual Chassis, QFX3600 Virtual Chassis, and mixed QFX3500 and QFX3600 Virtual Chassis. Virtual Chassis local link bias conserves bandwidth on Virtual Chassis ports (VCPs) by using local links to forward unicast traffic exiting a Virtual Chassis that has a LAG bundle composed of member links on different member switches in the same Virtual Chassis. A local link is a member link in the LAG bundle that is on the member switch that received the traffic. Because traffic is received and forwarded on the same member switch when local link bias is enabled, no VCP bandwidth is consumed by traffic traversing the VCPs to exit the Virtual Chassis using a different member link in the LAG bundle.

[See [Understanding Local Link Bias.](#)]

- **Adaptive load balancing support (Virtual Chassis Fabric)**—Starting with Junos OS Release 14.1X53-D10, adaptive load balancing (ALB) is supported in Virtual Chassis Fabric (VCF). ALB improves traffic management within a VCF by using dynamic load information to make traffic forwarding decisions. ALB introduces a method to better manage extremely large traffic flows—*elephant flows*—by splicing them into smaller flows—*flowlets*—and individually forwarding the flowlets across the VCF to the same destination device over different paths.

[See [Understanding Traffic Flow Through a Virtual Chassis Fabric.](#)]

VXLAN

- **Layer 2 VXLAN gateway (QFX5100)**—Starting with Junos OS Release 14.1X53-D10, VXLAN is an overlay technology that enables you to stretch Layer 2 connections over an intervening Layer 3 network by encapsulating (tunneling) Ethernet frames in a VXLAN packet that includes IP addresses. You can use VXLAN tunnels to enable migration of virtual machines between servers that exist in separate Layer 2 domains by tunneling the traffic through Layer 3 networks. This functionality enables you to dynamically allocate resources within or between data centers without being constrained by Layer 2 boundaries or being forced to create large or geographically stretched Layer 2 domains. Using VXLANs to connect Layer 2 domains over a Layer 3 network means that you do not need to use STP to converge the topology (so no links are blocked) but can use more robust routing protocols in the Layer 3 network instead.

[See [Understanding VXLANs](#).]

Related Documentation

- [Changes in Behavior and Syntax on page 49](#)
- [Known Behavior on page 51](#)
- [Known Issues on page 60](#)
- [Resolved Issues on page 63](#)
- [Documentation Updates on page 68](#)
- [Migration, Upgrade, and Downgrade Instructions on page 69](#)
- [Product Compatibility on page 74](#)

Changes in Behavior and Syntax

The following are changes in known behavior in Junos OS Releases 14.1X53 for the QFX Series.

- [SNMP](#)
- [Open vSwitch Database \(OVSDB\)](#)
- [Software Upgrade](#)

SNMP

- **Change in value for a QFabric SNMP object**—The `jnxFabricDeviceEntryName` object now displays the alias of the device and the `jnxFabricDeviceEntryDescription` object contains the serial number only.

Open vSwitch Database (OVSDB)

- **Automatic configuration of trunk interfaces that handle untagged packets in OVSDB-managed VXLANs (QFX5100, QFX5100VC)**—In previous Junos OS releases, if you specified a VLAN ID of 0 for a logical switch port in VMware NSX Manager or in the NSX API, the QFX5100 switch automatically configured an access interface to handle untagged packets in the associated Open vSwitch Database (OVSDB) –managed Virtual Extensible LAN (VXLAN). Starting with 14.1X53-D26, specifying a VLAN ID of 0 in a logical switch port configuration causes the QFX5100 switch to automatically configure a trunk port. To enable the trunk port to handle untagged packets, the QFX5100 switch also configures a native VLAN with an ID of 4094. Upon receipt of an untagged packet, the trunk interface adds a VLAN tag of 4094 to the packet and removes the tag as the packet exits the interface, thereby rendering the packet as untagged again.

This change supports the division of an OVSDB-managed physical interface into multiple logical interfaces, some of which are associated with VXLANs that have untagged packets and some of which are associated with VXLANs that have tagged packets.

Software Upgrade

- A controlled version of Junos OS is introduced for the QFX Series in Junos OS Release 14.1X53-D15. The controlled version of Junos OS is required to enable Media Access Control security (MACsec) on a switch. The controlled version of a Junos OS release contains all features and functionality available in the standard version of the Junos OS release while also supporting MACsec. The controlled version of Junos OS is not, by default, shipped on any QFX Series switch. You can download the controlled version of Junos OS from the Software Download Center, provided that you are located in a geography where you are allowed to download the controlled version of Junos OS. If you are unsure of which version of Junos OS is running on your switch, enter the **show version** command. If the “JUNOS Crypto Software Suite” description appears in the output, you are running the controlled version of Junos OS.

The controlled version of Junos OS contains encryption and is, therefore, not available to customers in all geographies. The export and re-export of the controlled version of Junos OS is strictly controlled under United States export laws. The export, import, and use of the controlled version of Junos OS is also subject to controls imposed under the laws of other countries.

If you have questions about acquiring the controlled version of Junos OS in your country, contact the Juniper Networks Trade Compliance group at compliance_helpdesk@juniper.net.

Related Documentation

- [New and Changed Features on page 30](#)
- [Known Behavior on page 51](#)
- [Known Issues on page 60](#)
- [Resolved Issues on page 63](#)
- [Documentation Updates on page 68](#)
- [Migration, Upgrade, and Downgrade Instructions on page 69](#)
- [Product Compatibility on page 74](#)

Known Behavior

This section lists the limitations in Junos OS Release 14.1X53 for the QFX Series.

Interfaces and Chassis

- On a QFX5100 switch, if you configure MC-LAG, IRB mac sync, and LACP force up, the number of packets received (rx) might be twice the amount sent (tx) from the customer edge to the core. [PR1015655](#)
- When a transceiver on a QFX5100, QFX3600, QFX3500, or EX4300 switch is removed and reinserted into an interface within 30 seconds after you issued the **set virtual-chassis vc-port set** command to convert the interface into a Virtual Chassis port (VCP), the VCP is not created. [PR1029829](#)
- QFX5100-48T 10gbase-T copper ports support 100m speed in both autonegotiation and force speed mode. To configure 100m speed in autonegotiation mode, you must configure 100m speed on the peer. To configure 100m speed in force speed mode, you must delete the interface by using the **delete interface ether-options auto-negotiation configuration** command. Deleting the interface sets the port into force speed mode, in which 10gbase-T copper ports support only 100m speed. Therefore, the port speed mode is automatically set to 100m. That is, you do not need to explicitly configure the speed as 100m in force speed mode. [PR1044860](#)



NOTE: In Junos OS Release 14.1X53-D15, the **ether-options** statement is not available in the **[edit interfaces *interface-name*]** hierarchy.

Layer 3 Protocols

- On QFX5100 switches, if you use the **next-table** statement in the configuration of a static route that is part of a virtual routing instance, the switch does not forward ICMP packets destined to a route that is present in the inet.0 routing table. [PR970895](#)

MPLS

- If a link failure occurs when multiple LSPs are using a link-protected, fast-rerouted link, the convergence time is proportional to the number of LSPs sharing the protected link. [PR1015806](#)
- In a scaled configuration for MPLS FRR and L2 circuit, the convergence time for FRR might increase. For L2 circuit, there might be packet drops. [PR1016146](#)
- On a QFX5100 switch that is using the Ethernet tagged mode of operation on a pseudowire, L2 control protocols can fail to come up between customer edge devices (CEs) across the pseudowire. This issue is not seen when the pseudowire mode of operation is Ethernet raw mode. [PR1028537](#)
- For an L2 circuit on QFX5100 switches, when IS-IS is used as an IGP between CEs connected to an L2 circuit, the CEs fail to form an IS-IS adjacency over the pseudowire. As a workaround, consider using an alternative IGP protocol, such as OSPF. [PR1032007](#)

Multicast Protocols

- When an IGMP leave is sent from a host to a QFX5100 switch, one packet per multicast group is dropped during route programming. [PR995331](#)

OVSDB

- On QFX5100 switches, the amount of time that it takes for other Juniper Networks devices that function as hardware virtual tunnel endpoints (VTEPs) to learn a new MAC address after the first packet is sent from this MAC address is a maximum of 4.5 seconds. (The amount of time depends upon the server configuration on which VMware NSX is running.) During this time, traffic destined for this MAC address is flooded into the VXLAN. [PR962945](#)
- After the connections with NSX controllers are disabled on a Juniper Networks device, interfaces that were configured to be managed by OVSDB continue passing traffic. [PR980577](#)
- QFX5100 switches do not support multiple service nodes for the handling of Layer 2 broadcast, unknown unicast, and multicast (BUM) traffic within an OVSDB-managed VXLAN. [PR985872](#)
- If an entity with a particular MAC address is moved so that its traffic is handled by a different Juniper Networks device that functions as a hardware virtual tunnel endpoint (VTEP), this MAC address is not learned by entities served by the new hardware VTEP until the hardware VTEP that previously handled its traffic ages out the MAC address. During this transitional period, traffic destined for this MAC address is dropped. [PR988270](#)

- On QFX5100 switches, an NSX controller occasionally overrides an existing local MAC with a remote MAC of the same address. If the Junos OS hardware VTEP detects such a condition (that is, it receives a remote MAC from the NSX controller that conflicts (matches) with an existing local MAC), the hardware VTEP in a Junos OS network accepts the remote MAC and stops publishing the local MAC to the NSX controller. [PR991553](#)
- On QFX5100 switches, an active path in the OVSDB overlay, which you can view by using the **show ovssdb mac** operational command, does not always match the active path in the Layer 3 network underlay, which you can view by using the **show route** operational command. [PR1015998](#)
- On QFX5100 switches, in NSX Manager, when a logical switch is deleted, the corresponding VXLAN on a QFX5100 switch might not be automatically deleted and might still appear in the output of the **show vlans** command. [PR1024169](#)
- On a QFX5100 switch on which OVSDB-managed interfaces are automatically configured, if you delete the configuration of one or more of the interfaces from the switch using the **delete vlans interfaces** command, the interfaces will be automatically reconfigured per the logical switch, gateway service, and logical switch port configurations that still reside in NSX. Despite the automatic reconfiguration of the OVSDB-managed interfaces, an 8- to 12-second loss of traffic might occur. This loss is because local MAC addresses learned by the interfaces and port-to-logical switch bindings were cleared when the interfaces were deleted and must be re-learned after the interfaces are up and running again. [PR1069889](#)

QFabric Systems

- On a QFabric system, if the fabric control Routing Engines are not load balanced, when you request a "component all" style software upgrade, the upgrade fails. [PR892310](#)
- On a QFabric system, if the fabric control Routing Engines are not load balanced, when you request a **component all** style software upgrade, the upgrade fails. As a workaround, "service ccif restart from master DG will rebalance the VMs properly"; you can then request a **component all** style software upgrade. [PR932149](#)
- On a QFabric system, when you configure an alias for a Node device or an Interconnect device, use that alias when you configure a flow group. [PR1032693](#)

Routing Policy and Firewall Filters

- On QFX Series Virtual Chassis, packets that are generated in the CPU and exit from a non-master FPC port might be subjected to an egress port-based firewall filter (PACL) and be egress filtered, while packets that exit from a master FPC port might not be egress filtered. [PR923659](#)

Software Installation and Upgrade

- On a QFX5100 switch, system logs might not be retained after a unified in-service software upgrade (ISSU), due to the data disk being reformatted during the ISSU. [PR964950](#)

- On QFX5100 switches, if a port mirroring analyzer is configured with a VLAN input and you perform an ISSU, the analyzer state is restored after the upgrade. If you later delete the analyzer configuration, mirroring stops but there might be harmless stale entries in the hardware. [PR970011](#)

System Management

- On the QFX Series, using the **set license keys key** and **request system license add terminal** commands together does not work for installing and deleting licenses. For example, if you install the license using the **set license keys key**, use the **delete license keys** command to delete the license. This is true for the **request system license** commands. [PR1023672](#)

Storage and Fibre Channel

- Each Fibre Channel fabric on an FCoE-FC gateway supports a maximum of four Fibre Channel over Ethernet (FCoE) VLAN interfaces.
- The maximum number of logins for each FCoE node (ENode) is in the range of 32 through 2500. (Each ENode can log in to a particular fabric up to the maximum number of configured times. The maximum number of logins is per fabric, so an ENode can log in to more than one fabric and have its configured maximum number of logins on each fabric.)
- The maximum number of FCoE sessions for the switch, which equals the total number of fabric login (FLOGI) sessions plus the total number of fabric discovery (FDISC) sessions, is 2500.
- The maximum number of FIP snooping sessions per QFX3500 switch is 2500.
- When you configure FIP snooping filters, if the filters consume more space than is available in the ternary content-addressable memory (TCAM), the configuration commit operation succeeds even though the filters are not actually implemented in the configuration. Because the commit operation checks syntax but does not check available resources, it appears as if the FIP snooping filters are configured, but they are not. The only indication of this issue is that the switch generates a system log message that the TCAM is full. You must check the system log to find out if a TCAM full message has been logged if you suspect that the filters have not been implemented.
- You cannot use a fixed classifier to map FCoE traffic to an Ethernet interface. The FCoE application type, length, and value (TLV) carries the FCoE priority-based flow control (PFC) information when you use an explicit IEEE 802.1p classifier to map FCoE traffic to an Ethernet interface. You cannot use a fixed classifier to map FCoE traffic to an Ethernet interface because untagged traffic is classified in the FCoE forwarding class, but FCoE traffic must have a priority tag (FCoE traffic cannot be untagged).

For example, the following behavior aggregate classifier configuration is supported:

[edit class-of-service]

```
user@switch# set congestion notification profile fcoe-cnp input ieee-802.1 code-point 011 pfc
```

```
user@switch# set interfaces xe-0/0/24 unit 0 classifiers ieee-802.1 fcoe
```


For example, the following fixed classifier configuration is not supported:

[edit class-of-service]

user@switch# set interfaces xe-0/0/24 unit 0 forwarding-class fcoe

- On a QFX Series device, a DCBX interoperability issue between 10-Gigabit Ethernet interfaces on QFX Series devices and 10-Gigabit Ethernet interfaces on another vendor's devices can prevent the two interfaces from performing DCBX negotiation successfully in the following scenario:
 1. On a QFX Series 10-Gigabit Ethernet interface, LLDP is running, but DCBX is disabled.
 2. On another vendor's device 10-Gigabit Ethernet interface, both LLDP and DCBX are running, but the interface is administratively down.
 3. When you bring another vendor's 10-Gigabit Ethernet interface up by issuing the **no shutdown** command, the device sends DCBX 1.01 (CEE) TLVs, but receives no acknowledge (ACK) message from the QFX Series device, because DCBX is not enabled on the QFX Series device. After a few tries, another vendor's device sends DCBX 1.00 (CIN) TLVs, and again receive no ACK messages from the QFX Series device.
 4. Enable DCBX on the QFX Series 10-Gigabit Ethernet interface. The interface sends DCBX 1.01 (CEE) TLVs, but the other vendor's device ignores them and replies with DCBX 1.00 (CIN) TLVs. The other vendor's device does not attempt to send or acknowledge DCBX 1.01 TLVs, only DCBX 1.00 TLVs.

In this case, the QFX Series device ignores the DCBX 1.00 (CIN) TLVs because the QFX Series does not support DCBX 1.00 (the QFX Series supports DCBX 1.01 and IEEE DCBX). The result is that the DCBX capabilities negotiation between the two interfaces fails.

Traffic Management

- On a QFX5100 switch, running **tcpdump** on the console might cause system instability or cause protocols such as STP or LACP to fail. [PR932592](#)
- CoS on Virtual Chassis access interfaces is the same as CoS on QFX Series access interfaces with the exception of shared buffer settings. All of the documentation for QFX Series CoS on access interfaces applies to Virtual Chassis access interfaces.

Virtual Chassis access interfaces support the following CoS features:

- Forwarding classes—The default forwarding classes, queue mapping, and packet drop attributes are the same as on QFX Series access interfaces:

Default Forwarding Class	Default Queue Mapping	Default Packet Drop Attribute
best-effort (be)	0	drop
fcpe	3	no-loss
no-loss	4	no-loss
network-control (nc)	7	drop
mcast	8	drop

- Packet classification—Classifier default settings and configuration are the same as on QFX Series access interfaces. Support for behavior aggregate, multifield, multideestination, and fixed classifiers is the same as on QFX Series access interfaces.
- Enhanced transmission selection (ETS)—This data center bridging (DCB) feature that supports hierarchical scheduling has the same defaults and user configuration as on QFX Series access interfaces, including forwarding class set (priority group) and traffic control profile configuration.
- Priority-based flow control (PFC)—This DCB feature that supports lossless transport has the same defaults and user configuration as on QFX Series access interfaces, including support for six lossless priorities (forwarding classes).
- Ethernet PAUSE—Same defaults and configuration as on QFX Series access interfaces.
- Queue scheduling—Same defaults, configuration, and scheduler-to-forwarding-class mapping as on QFX Series access interfaces. Queue scheduling is a subset of hierarchical scheduling.
- Priority group (forwarding class set) scheduling—Same defaults and configuration as on QFX Series access interfaces. Priority group scheduling is a subset of hierarchical scheduling.
- Tail-drop profiles—Same defaults and configuration as on QFX Series access interfaces.
- Code-point aliases—Same defaults and configuration as on QFX Series access interfaces.
- Rewrite rules—As on the QFX Series access interfaces, there are no default rewrite rules applied to egress traffic.
- Host outbound traffic—Same defaults and configuration as on QFX Series access interfaces.

The default shared buffer settings and shared buffer configuration are also the same as on QFX Series access interfaces, except that the shared buffer configuration is global and applies to all access ports on all members of the Virtual Chassis. You cannot configure different shared buffer settings for different Virtual Chassis members.

- **Similarities in CoS support on VCP interfaces and QFabric system Node device fabric interfaces**—VCP interfaces support full hierarchical scheduling (ETS). ETS includes:
 - Creating forwarding class sets (priority groups) and mapping forwarding classes to forwarding class sets.
 - Scheduling for individual output queues. The scheduler defaults and configuration are the same as the scheduler on access interfaces.
 - Scheduling for priority groups (forwarding class sets) using a traffic control profile. The defaults and configuration are the same as on access interfaces.
 - No other CoS features are supported on VCP interfaces.



NOTE: You cannot attach classifiers, congestion notification profiles, or rewrite rules to VCP interfaces. Also, you cannot configure buffer settings on VCP interfaces. Similar to QFabric system Node device fabric interfaces, you can only attach forwarding class sets and traffic control profiles to VCP interfaces.

The behavior of lossless traffic across 40-Gigabit VCP interfaces is the same as the behavior of lossless traffic across QFabric system Node device fabric ports. Flow control for lossless forwarding classes (priorities) is enabled automatically. The system dynamically calculates buffer headroom that is allocated from the global lossless headroom buffer for the lossless forwarding classes on each 40-Gigabit VCP interface. If there is not enough global headroom buffer space to support the number of lossless flows on a 40-Gigabit VCP interface, the system generates a syslog message.



NOTE: After you configure lossless transport on a Virtual Chassis, check the syslog messages to ensure that there is sufficient buffer space to support the configuration.



NOTE: If you break out a 40-Gigabit VCP interface into 10-Gigabit VCP interfaces, lossless transport is not supported on the 10-Gigabit VCP interfaces. Lossless transport is supported only on 40-Gigabit VCP interfaces.

- **Differences in CoS support on VCP interfaces and QFabric system Node device fabric interfaces**—Although most of the CoS behavior on VCP interfaces is similar to CoS behavior on QFabric system Node device fabric ports, there are some important differences:

- Hierarchical scheduling (queue and priority group scheduling)—On QFabric system Node device fabric interfaces, you can apply a different hierarchical scheduler (traffic control profile) to different priority groups (forwarding class sets) on different interfaces. However, on VCP interfaces, the schedulers you apply to priority groups are global to all VCP interfaces. One hierarchical scheduler controls scheduling for a priority group on all VCP interfaces.

You attach a scheduler to VCP interfaces using the global identifier (*vcp-**) for VCP interfaces. For example, if you want to apply a traffic control profile (which contains both queue and priority group scheduling configuration) named *vcp-fcoe-tcp* to a forwarding class set named *vcp-fcoe-fcset*, you include the following statement in the configuration:

```
[edit]
user@switch# set class-of-service interfaces vcp-* forwarding-class-set vcp-fcoe-fcset
output-traffic-control-profile vcp-fcoe-tcp
```

The system applies the hierarchical scheduler *vcp-fcoe-tcp* to the traffic mapped to the priority group *vcp-fcoe-fcset* on all VCP interfaces.

- You cannot attach classifiers, congestion notification profiles, or rewrite rules to VCP interfaces. Also, you cannot configure buffer settings on VCP interfaces. Similar to QFabric system Node device fabric interfaces, you can only attach forwarding class sets and traffic control profiles to VCP interfaces.
- Lossless transport is supported only on 40-Gigabit VCP interfaces. If you break out a 40-Gigabit VCP interface into 10-Gigabit VCP interfaces, lossless transport is not supported on the 10-Gigabit VCP interfaces.
- On a QFX5100 switch, CPU-generated host outbound traffic is forwarded on the network-control forwarding class, which is mapped to queue 7. If you use the default scheduler, the network-control queue receives a guaranteed minimum bandwidth (transmit rate) of 5 percent of port bandwidth. The guaranteed minimum bandwidth is more than sufficient to ensure lossless transport of host outbound traffic.

However, if you configure a scheduler, you must ensure that the network-control forwarding class (or whatever forwarding class you configure for host outbound traffic) receives sufficient guaranteed bandwidth to prevent packet loss.

If you configure a scheduler, we recommend that you configure the network-control queue (or the queue you configure for host outbound traffic if it is not the network-control queue) as a strict-high priority queue. Strict-high priority queues receive the bandwidth required to transmit their entire queues before other queues are served.



NOTE: As with all strict-high priority traffic, if you configure the network-control queue (or any other queue) as a strict-high priority queue, you must also create a separate forwarding class set (priority group) that contains only strict-high priority traffic, and apply the strict-high priority forwarding class set and its traffic control profile (hierarchical scheduler) to the relevant interfaces.

- You cannot apply classifiers and rewrite rules to IRB interfaces because the members of an IRB interface are VLANs, not interfaces. You can apply classifiers and rewrite rules to Layer 2 logical interfaces and Layer 3 physical interfaces that are members of VLANs that belong to IRB interfaces.

Virtual Chassis and Virtual Chassis Fabric

- On a mixed Virtual Chassis Fabric (VCF), control plane packets, including control packets for OSPF or PIM, are not mirrored by the native analyzer when the output port belongs to another member switch. [PR969542](#)
- When a Virtual Chassis port (VCP) is added between two QFX5100 member switches that are already interconnected using a VCP, a VCP link aggregation group (LAG) is formed and some multicast packets between the two member switches might be duplicated. [PR1007204](#)
- On QFX5100 mixed-mode Virtual Chassis or Virtual Chassis Fabric (VCF) systems that include QFX3500 or QFX3600 switches, a MACsec configuration cannot be committed because MACsec is not supported on QFX3500 and QFX3600. [PR1024921](#)
- On a mixed Virtual Chassis Fabric (VCF), a VCP link between two members disappears after you perform a nonstop software upgrade. The **show virtual-chassis protocol adjacency member** command output shows the state of the VCP link as **initializing**. [PR1031296](#)

VXLAN

- On a QFX5100 switch with a VXLAN configured, (S,G) interface entries downstream from a VXLAN interface might be missing from the multicast routing table but be present in the kernel and packet forwarding engine. In this circumstance, traffic is forwarded as expected. [PR1027119](#)
- VXLANs with the VLAN IDs of 1 and 2 are configured on a QFX5100 switch. The replicated packets for these VXLANs should include the VLAN tags of 1 or 2, respectively. Instead, the replicated packets for these VXLANs are untagged, which might result in the packets being dropped by a Juniper Networks device that receives the packets. To avoid this situation, when configuring a VXLAN on a QFX5100 switch, we recommend using a VLAN ID of 3 or higher. [PR1072090](#)

Related Documentation

- [New and Changed Features on page 30](#)
- [Changes in Behavior and Syntax on page 49](#)

- [Known Issues on page 60](#)
- [Resolved Issues on page 63](#)
- [Documentation Updates on page 68](#)
- [Migration, Upgrade, and Downgrade Instructions on page 69](#)
- [Product Compatibility on page 74](#)

Known Issues

The following issues are outstanding in Junos OS Release 14.1X53 for the QFX Series. The identifier following the description is the tracking number in our bug database.

For the latest, most complete information about outstanding and resolved issues with the Junos OS software, see the Juniper Networks online software defect search application at <http://www.juniper.net/prsearch>.

- [Interfaces and Chassis](#)
- [MPLS](#)
- [Multicast Protocols](#)
- [Network Management and Monitoring](#)
- [OVSDB](#)
- [Platform and Infrastructure](#)
- [QFabric System](#)
- [System Management](#)
- [Virtual Chassis and Virtual Chassis Fabric](#)
- [VXLAN](#)

Interfaces and Chassis

- On a QFX5100 switch, if you configure MC-LAG with the **force-up option**, the FXP might create a core file and generate the following error message: **0x0806b7b8 in panic (format_string=0x9c72614 "Memory corruption in block %p\n" at ../../src/pfe/platform/fxpc/fxpc_panic.c:93.** [PR1024354](#)
- When a transceiver on a QFX5100, QFX3600, QFX3500, or EX4300 switch is removed and reinserted into an interface within 30 seconds after you issued the **set virtual-chassis vc-port set** command to convert the interface into a Virtual Chassis port (VCP), the VCP is not created. [PR1029829](#)
- When an EX4600-EM-8F expansion module is installed in a QFX5100-24Q switch or an EX4600 switch, it does not support the 100 Mbps speed on the 10-Gigabit Ethernet interfaces. [PR1032257](#)
- In a mixed QFX3500 and EX4300 Virtual Chassis configured for persistent MAC and MAC limiting, traffic is not received on aggregated Ethernet interfaces on EX4300 switches when the EX4300 switches are operating in the linecard role. [PR1033618](#)

- When an EX4600 or QFX5100 switch is downgraded from Junos OS Release 14.1X53-D15 or later to Junos OS Release 14.1X53-D10 or earlier, the 40-Gbps Ethernet interfaces on QSFP+ transceivers might not return to the up state. As a workaround, power cycle the switch after the Junos OS upgrade. [PR1061213](#)
- On a QFX5100 switch, the C0 SFP management port (em0) sometimes fails to come online. [PR1075001](#)

MPLS

- A pseudowire is a port-based Layer 2 circuit that emulates a service over a packet switched network (PSN). You can emulate any circuit end to end using a pseudowire. In the event of a link failure on a transit router that hosts a Layer 2 circuit over an RSVP tunnel, the traffic convergence time is approximately 350 milliseconds for a single pseudowire. [PR1016992](#)
- On a QFX5100 switch, if an MPLS link is in hot standby mode and a pseudowire switchover is triggered by the event **remote site local interface signaled down**, traffic flowing through the pseudowire is dropped. [PR1027755](#)

Multicast Protocols

- When an IGMP leave is sent from a host to a QFX5100 switch, one packet per multicast group is dropped during route programming. [PR995331](#)

Network Management and Monitoring

- This issue applies to the Cloud Analytics Engine feature. The Compute Agent Web API does not provide the option to configure the VxLAN destination port. [PR1036372](#)
- This issue applies to the Cloud Analytics Engine feature. Compute Agent CPU utilization goes up when 50 flows are sent. [PR1041190](#)
- This issue applies to the Cloud Analytics Engine feature. The Cloud Analytics Engine Compute Agent process (cagent) does not start after the server is rebooted. [PR1041931](#)
- On a QFX5100 switch, the DHCP relay bindings of clients bound via secondary addresses may get cleared when the primary address on the gateway interface configured as DHCP Smart Relay is modified or deactivated. [PR1084911](#)

OVSDB

- On QFX5100 switches, in general, Layer 3 routes use per-prefix load balancing without a routing policy that specifies that per-packet load balancing should be used. Note that the default behavior is different for Layer 3 routes for remote VTEP reachability. Layer 3 routes for remote VTEP reachability use per-packet load balancing, which means that load balancing is implemented if there are ECMP paths to the remote VTEP. [PR1018814](#)
- On a QFX5100 switch, deleting a VLAN and an interface configuration on an OVSDB-managed interface might cause the switch to reboot. A "Core was generated by `fxpc'" message appears on the console, and a core dump file is created. [PR1091446](#)

- In an IP fabric using EBGp and VTEP, convergence issues might cause traffic to be dropped for several minutes after BGP is deactivated on a spine device. [PR1091007](#)
- When QFX5100 switches are part of an OVSDb-managed VXLAN, traffic load balancing on a link aggregation group (LAG) doesn't work over ECMP for Layer 3 VXLAN interfaces. [PR1090791](#)

Platform and Infrastructure

- On a QFX5100 switch, Bidirectional Forwarding Detection (BFD) sessions might continuously switch from on to off for several minutes after an in-service software upgrade (ISSU). [PR980476](#)

QFabric System

- On a QFabric system, if the system sends and receives multicast traffic, you issue the **request fabric administration power-off node-device** command for the master Node device, and then replace the Node device, some multicast traffic might be dropped when the interfaces renegotiate their LACP settings. [PR1035254](#)

System Management

- On EX Series and QFX Series switches that are configured with the **include-option-82 nak** option so that DHCP servers include option 82 information in NAK messages, two copies of option-82 are sometimes appended to DHCP ACK packets. [PR1064969](#)

Virtual Chassis and Virtual Chassis Fabric

- On a mixed-mode Virtual Chassis Fabric, during a Routing Engine switchover, the system might experience a 200-300 millisecond loss of traffic. [PR964987](#)
- If a VCF is connected to a Juniper Networks router with a flexible PIC concentrator (FPC) and an xSTP bridge protocol data unit is distributed to the FPC, there might be traffic loss when the FPC is rebooted. [PR990247](#)
- When a Virtual Chassis port (VCP) is added between two QFX5100 member switches that are already interconnected using a VCP, a VCP link aggregation group (LAG) is formed and some multicast packets between the two member switches might be duplicated. [PR1007204](#)
- On a mixed-mode VCF, if you perform a nonstop software upgrade (NSSU) and a MAC address is present on the ingress or egress Packet Forwarding Engine, in some cases known Layer 2 unicast traffic might still be flooded over the VLAN. [PR1013416](#)
- If you change the VNIs of all the VXLANs in a QFX5100 Virtual Chassis Fabric, VXLAN traffic does not converge for some of the VXLANs. [PR1028588](#)
- On a non-mixed Virtual Chassis Fabric (VCF), LACP flaps when the switch in the master Routing Engine role is rebooted using the CLI or because of a power cycle. This issue is not experienced after a Routing Engine switchover. As a workaround, configure a slow LACP timeout. [PR1034377](#)

VXLAN

- On QFX5100 switches, the Layer 3 routes that form virtual extensible LAN (VXLAN) tunnels use per-packet load balancing by default, which means that load balancing is implemented if there are ECMP paths to the remote tunnel endpoint. This is different from normal routing behavior in which per-packet load balancing is not used by default. (Normal routing uses per-prefix load balancing by default.) [PR1018814](#)
- On a QFX5100 switch configured with a VXLAN and PIM, the (S,G) route for the VXLAN multicast group can get stuck pointing to the pime interface even though the RP has joined the multicast group. This does not affect traffic forwarding for multicast traffic as the forwarding state for the (S,G) route points correctly to the uplink interface to the RP. [PR1023447](#)
- If you perform a graceful Routing Engine switchover in a Virtual Chassis Fabric acting as a VXLAN virtual tunnel endpoint, known unicast traffic might be dropped from the VXLAN. [PR1026408](#)
- If you configure a QFX5100 switch to be a VXLAN virtual tunnel endpoint and also configure it to be a PIM RP, the multicast tree does not successfully converge and multicast traffic is dropped. [PR1027159](#)
- If you change the VNIs of all the VXLANs in a QFX5100 Virtual Chassis Fabric, VXLAN traffic does not converge for some of the VXLANs. [PR1028588](#)
- When a Layer 2 interface on a QFX5100 switch is deactivated and reactivated again, an encapsulated VXLAN packet received on a Layer 3 interface on another networking device is sent to the Routing Engine kernel instead of being de-encapsulated and forwarded to the Layer 2 interface. [PR1049752](#)

Related Documentation

- [New and Changed Features on page 30](#)
- [Changes in Behavior and Syntax on page 49](#)
- [Known Behavior on page 51](#)
- [Resolved Issues on page 63](#)
- [Documentation Updates on page 68](#)
- [Migration, Upgrade, and Downgrade Instructions on page 69](#)
- [Product Compatibility on page 74](#)

Resolved Issues

This section lists the issues fixed in the Junos OS Release 14.1X53 for the QFX Series.

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

- [Resolved Issues: Release 14.1X53-D27 on page 64](#)
- [Resolved Issues: Release 14.1X53-D26 on page 64](#)
- [Resolved Issues: Release 14.1X53-D25 on page 64](#)

- [Resolved Issues: Release 14.1X53-D16 on page 66](#)
- [Resolved Issues: Resolved Before Release 14.1X53-D16 on page 67](#)

[Resolved Issues: Release 14.1X53-D27](#)

No issues that were previously reported in any version of the Junos OS Release 14.1X53 release notes have been resolved in Junos OS Release 14.1X53-D27 for the QFX Series.

[Resolved Issues: Release 14.1X53-D26](#)

Interfaces and Chassis

- On EX4600 and QFX5100 switches, the 100Mbps LED functionality is not working. The LED does not glow when 100Mbps traffic is sent or received on the switch, and no output is displayed when the **show chassis led** command is entered to gather information on the 100Mbps interface. [PR1025359](#)

VXLAN

- On a QFX5100 Virtual Chassis, when approximately 3000 Virtual Extensible LANs (VXLANs) are configured and associated with logical interfaces for the same OVSDB-managed interface, a high level of memory usage might occur. As a workaround, disable the 802.1X and multicast snooping processes using the **set system processes dot1x-protocol disable** and **set system processes multicast-snooping disable** statements. [PR1073677](#)
- “On a QFX5100 Virtual Chassis, when approximately 3000 Virtual Extensible LANs (VXLANs) are configured and associated with logical interfaces for the same OVSDB-managed interface, a high level of memory usage might occur. As a workaround, disable the 802.1X and multicast snooping processes using the **set system processes dot1x-protocol disable** and **set system processes multicast-snooping disable** statements.” [PR1073677](#)

[Resolved Issues: Release 14.1X53-D25](#)

Class of Service

- On the QFX Series, applying a class-of-service (CoS) configuration globally (using the * wildcard) to all interfaces on a device can cause inconsistency in the packet forwarding state if the device has interfaces that are members of a link aggregation (LAG) interface bundle and also interfaces that are not members. [PR1001605](#)

Interfaces and Chassis

- On a QFX5100 switch, high ICMP delays are experienced when pinging directly connected integrated routing and bridging (IRB) interfaces. [PR966905](#)

MPLS

- Pseudowire emulates a service over packet-switched network (PSN) using only virtual wire. You can emulate any circuit end to end using pseudowire. In the event of a failure, the switchover from the active pseudowire to the standby/backup pseudowire takes longer than expected. [PR1025899](#)

- Pseudowire emulates a service over packet-switched network (PSN) using only virtual wire. You can emulate any circuit end to end using pseudowire. However, the switchover-delay timer for an Active/Standby pseudowire topology might not work as expected. [PR1026336](#)

Network Management and Monitoring

- This issue applies to the Cloud Analytics Engine feature. On QFX5100-48T-6Q switches, when error counters have been incremented in ERROR_CNTR TLV, a probe does not recognize those errors. ERROR_CNTR TLV is not populated in Cloud Analytics Engine probe responses. [PR1034928](#)
- This issue applies to the Cloud Analytics Engine feature. The default aging timer value is 60 seconds for a flow to get aged out. The flow will be marked for aging in the range of 60 to 120 seconds for the default aging timer value from the latest probe time stamp. It will be deleted in next 60 seconds (because the default aging time is 60 seconds). Total time to delete the flow will be a maximum of 3 minutes from the latest flow time stamp for default aging timer value. [PR1037738](#)
- This issue applies to the Cloud Analytics Engine feature. If an invalid Compute Agent IP address is specified in the CA-Discovery file uploaded to the Data Learning Engine, the Data Learning Engine will fail. [PR1041925](#)
- This issue applies to the Cloud Analytics Engine feature. Some application flows might not get registered in the signature database when high rate flow is on. [PR1048083](#)
- This issue applies to the Cloud Analytics Engine feature. Depending on how CentOS installation and configuration is performed, the loopback address might not be configured. This will cause Data Learning Engine components to be inaccessible. There must be at least one entry in the /etc/hosts file for a default loopback IP address mapping to local host. [PR1048890](#)

Software Installation and Upgrade

- On QFX5100 switches with a large number of firewall terms configured, firewall filters might stop working after you perform an in-service software upgrade (ISSU). [PR966445](#)

QFabric System

- On a QFabric system, if you include a QFX5100 switch as a Node device in a redundant server Node group, the Master LED light might not turn on or be displayed in the output of the **show chassis led** command. [PR1048853](#)

Resolved Issues: Release 14.1X53-D16

Interfaces and Chassis

- On QFX5100 switches with a VXLAN configured, if you add an interface to the VLAN that the VXLAN is associated with or delete an interface from that VLAN, the switch might drop traffic for devices connected to other interfaces in the same VLAN. [PR1019378](#)
- On a QFX Series switch, when you reboot the switch with an enabled 40-Gigabit Ethernet interface, the interface might be disabled after the reboot. As a workaround, remove and then reinsert the attached cable. [PR1014139](#)
- On QFX5100 switches, disabling a member link of an AE interface might cause packets to be sent to a port that is down, which results in traffic loss. As a workaround, to restore service, bring the port that is down back up again. [PR1050260](#)
- On a QFX5100 switch, issuing the **request system reboot** command might not shut down SFP-T interfaces. [PR1050650](#)
- On a QFX5100-48T switch that uses QSFP+ transceivers (QSFP-40G-SR4), if you upgrade the switch software to Junos OS Release 14.1X53-D15, the QSFP+ transceivers might not be detected after the upgrade. [PR1051903](#)
- On a QFX5100 switch, DHCP offer packets with double tags on trunk interfaces might be dropped. [PR1059557](#)
- On a QFX5100-48T-6Q switch, when you configure a Gigabit Ethernet interface on a fiber SFP transceiver with the speed set to 1g and the settings *full duplex* and *no autonegotiation*, the interface goes down. [PR1063118](#)

Network Management and Monitoring

- This issue applies to the Cloud Analytics Engine feature. The CPU utilization value is incorrect in the Cloud Analytics Engine probe response statistics. [PR1024840](#)
- This issue applies to the Cloud Analytics Engine feature. Packets are not mirrored when a mirror IP address is configured on a remote device. [PR1052028](#)

Port Security

- In a mixed-mode Virtual Chassis Fabric with storm control enabled, if autonegotiation is enabled on a 1-gigabit interface (the default setting), the storm-control value for allowed bandwidth might be set to 0, which would cause traffic to be dropped. As a workaround, manually configure the link speed instead of using autonegotiation. [PR1051756](#)

Routing Policy and Firewall Filters

- If you configure a QFX5100 switch with a firewall filter that redirects traffic to a different interface (by using the **interface** action modifier, rebooting the switch might cause the Packet Forwarding Engine daemon (fxpc) to crash and generate core files. [PR1037563](#)

Routing Protocols

- On a QFX5100 switch, the routing protocol daemon (rpd) might crash and create a core file if there is interior BGP (IBGP) route churn while IBGP multipath is configured and there are multiple levels of IBGP next-hop recursion. [PR1060133](#)

Software Installation and Upgrade

- On a QFX5100 switch, if a port mirroring analyzer is configured with a VLAN input and you perform an in-service software upgrade (ISSU), the analyzer state is restored after the upgrade. If you later delete the analyzer configuration, mirroring stops but there might be residual harmless stale entries in the hardware. [PR970011](#)
- On a QFX5100 switch, if you perform an ISSU, there might be approximately 2 seconds of IPv4 or IPv6 traffic loss during the em0 handoff. [PR985462](#)

Virtual Chassis and Virtual Chassis Fabric

- On a QFX5100 Virtual Chassis Fabric (VCF), routing protocols (for example, OSPF or ISIS) might flap after a master Routing Engine (RE) role switch powers off, causing traffic loss. This issue is not seen on leaf switches. [PR1029066](#)

VLAN Infrastructure

- On QFX Series platforms, naming a VLAN *vlan-rewrite* causes an error when you commit the configuration. [PR1054996](#)

Resolved Issues: Resolved Before Release 14.1X53-D16

Interfaces and Chassis

- On QFX5100 switches, traffic might be dropped on a 40G channelized port. [PR1015221](#)
- On a QFX5100 switch, after performing an in-service software upgrade (ISSU), Layer 3 traffic might be interrupted on a configured VLAN or IRB interface. [PR1014130](#)

Layer 3 Protocols

- On a QFX5100 switch, if you perform an in-service software upgrade on a QFX5100 switch with the virtual routing redundancy protocol (VRRP) configured and there are a large number of VRRP groups or there are many VRRP transitions, you might see duplicate VRRP my_station_tcam entries. [PR1028607](#)

OVSDB

- If you enter a **show configuration** command after installing the OVSDB software package (jsdn-i386-release) on a QFX5100 Virtual Chassis or VCF, you see the warning **ddl_sequence_number_match: sequence numbers don't match**. [PR1019087](#)

Software Installation and Upgrade

- ISSU does not work with VXLANs on QFX5100 switches. [PR1024457](#)

VXLAN

- On a QFX5100 switch with a VXLAN configured, (S,G) interface entries downstream from a VXLAN interface might be missing from the multicast routing table but be present in the kernel and Packet Forwarding Engine. In this circumstance, traffic is forwarded as expected. [PR1027119](#)
- If a 32-member VCF loads the MDconfig without any routes and traffic and receives the **nh_comp_msg_parse** message, the FXPC might create a core file. [PR1029884](#)
- The **interface-mac-limit** statement is not supported with VXLANs. If you configure this statement with a VXLAN, MAC learning might not occur and traffic might not be forwarded. In this circumstance, delete the **interface-mac-limit** statement and the VXLAN configuration, then reconfigure the VXLAN. [PR1032552](#)

Related Documentation

- [New and Changed Features on page 30](#)
- [Changes in Behavior and Syntax on page 49](#)
- [Known Behavior on page 51](#)
- [Known Issues on page 60](#)
- [Documentation Updates on page 68](#)
- [Migration, Upgrade, and Downgrade Instructions on page 69](#)
- [Product Compatibility on page 74](#)

Documentation Updates

This section lists the errata or changes in Junos OS Release 14.1X53 documentation for QFX Series.

Bridging and Learning

- Two new MIBs related to MAC notification are provided at Junos OS Release 14.1X53-D10:

- [jnxL2aldMacHistoryEntry](#)
- [jnxL2aldMacNotificationMIBGlobalObjects](#)

These MIBs are not yet described in the documentation.

Network Management and Monitoring

- The Network Management and Monitoring on the QFX Series feature guide at Junos OS Release 14.1X53-D10 erroneously contained topics that applied to QFabric systems but not to QFX Series standalone switches. Those topics have been removed from the guide.

Virtual Chassis and Virtual Chassis Fabric (VCF)

- The support plan for the maximum number of member devices in a Virtual Chassis Fabric (VCF) has been revised to support for a maximum of 20 devices for all platforms that support VCF. The announcement for 32-device support has been removed from New Features in Junos OS Release 14.1X53-D15 in these release notes.

Related Documentation

- [New and Changed Features on page 30](#)
- [Changes in Behavior and Syntax on page 49](#)
- [Known Behavior on page 51](#)
- [Known Issues on page 60](#)
- [Resolved Issues on page 63](#)
- [Migration, Upgrade, and Downgrade Instructions on page 69](#)
- [Product Compatibility on page 74](#)

Migration, Upgrade, and Downgrade Instructions

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

- [Upgrading to a Controlled Version of Junos OS on page 69](#)
- [Upgrading Software on QFX5100 Standalone Switches on page 70](#)
- [Performing an In-Service Software Upgrade \(ISSU\) on page 71](#)
- [Preparing the Switch for Software Installation on page 72](#)
- [Upgrading the Software Using ISSU on page 72](#)

Upgrading to a Controlled Version of Junos OS

Starting in Junos OS Release 14.1X53-D15, you can install a controlled version of Junos OS software on a QFX Series switch. The controlled version of Junos OS software is required to enable Media Access Control security (MACsec).

If you are upgrading your switch between a domestic version of Junos OS and a controlled version of Junos OS, keep the following issues in mind:

- You cannot use NSSU to upgrade or downgrade from a controlled version of Junos OS to a domestic version of Junos OS.
- In a Virtual Chassis, all member switches must be running the same release of Junos OS. A Virtual Chassis with member switches that are running domestic and export versions of the same Junos OS release does form.
- In a Virtual Chassis, all member switches must be running the same release of Junos OS.

To support MACsec, however, all member switches in the Virtual Chassis must be running the controlled version of Junos OS.

The upgrade or downgrade procedure from a domestic version of Junos OS to a controlled version of Junos OS is, otherwise, identical to any other Junos OS upgrade. See *Upgrading Software* for more information.

Upgrading Software on QFX5100 Standalone Switches

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

The download and installation process for Junos OS Release 14.1X53-D10 is the same as for previous Junos OS releases.

If you are not familiar with the download and installation process, follow these steps:

1. In a browser, go to <http://www.juniper.net/support/downloads/junos.html> .
The Junos Platforms Download Software page appears.
2. In the QFX Series section of the Junos Platforms Download Software page, select the QFX Series platform for which you want to download the software.
3. Select **14.1** in the Release pull-down list to the right of the Software tab on the Download Software page.
4. In the Install Package section of the Software tab, select the QFX Series Install Package for the 14.1 release.
An Alert box appears.
5. In the Alert box, click the link to the PSN document for details about the software, and click the link to download it.
A login screen appears.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Download the software to a local host.

8. Copy the software to the device or to your internal software distribution site.
9. Install the new jinstall package on the device.



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

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

```
user@host> request system software add
source/jinstall-qfx-5-14.1X53-D25-domestic-signed.tgz reboot
```

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

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

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

Rebooting occurs only if the upgrade is successful.



NOTE: After you install a Junos OS Release 14.1 jinstall package, you can issue the **request system software rollback** command to return to the previously installed software.

Performing an In-Service Software Upgrade (ISSU)

You can use an in-service software upgrade to upgrade the software running on the switch with minimal traffic disruption during the upgrade.



NOTE: ISSU is supported in Junos OS Release 13.2X51-D15 and later.

Perform the following tasks:

- [Preparing the Switch for Software Installation on page 72](#)
- [Upgrading the Software Using ISSU on page 72](#)

Preparing the Switch for Software Installation

Before you begin software installation using ISSU:

- Ensure that nonstop active routing (NSR), nonstop bridging (NSB), and graceful Routing Engine switchover (GRES) are enabled. NSB and GRES enable NSB-supported Layer 2 protocols to synchronize protocol information between the master and backup Routing Engines.

To verify that nonstop active routing is enabled:



NOTE: If nonstop active routing is enabled, then graceful Routing Engine switchover is enabled.

```
user@switch> show task replication
Stateful Replication: Enabled
RE mode: Master
```

If nonstop active routing is not enabled (**Stateful Replication is Disabled**), see *Configuring Nonstop Active Routing on Switches* for information about how to enable it.

- Enable nonstop bridging (NSB). See *Configuring Nonstop Bridging on Switches (CLI Procedure)* for information on how to enable it.
- (Optional) Back up the system software—Junos OS, the active configuration, and log files—on the switch to an external storage device with the **request system snapshot** command.

Upgrading the Software Using ISSU

This procedure describes how to upgrade the software running on a standalone switch:

To upgrade the switch using ISSU:

1. Download the software package by following the procedure in the Downloading Software Files with a Browser section in *Upgrading Software*.
2. Copy the software package or packages to the switch. We recommend that you copy the file to the **/var/tmp** directory.
3. Log in to the console connection. Using a console connection allows you to monitor the progress of the upgrade.
4. Start the ISSU:
 - On the switch, enter:

```
user@switch> request system software in-service-upgrade
/var/tmp/package-name.tgz
```

where **package-name.tgz** is, for example, **jinstall-132_x51_vjunos.domestic.tgz**.



NOTE: During the upgrade, you will not be able to access the Junos OS CLI.

The switch displays status messages similar to the following messages as the upgrade executes:

```
warning: Do NOT use /user during ISSU. Changes to /user during ISSU may get
lost!
ISSU: Validating Image
ISSU: Preparing Backup RE
Prepare for ISSU
ISSU: Backup RE Prepare Done
Extracting jinstall-qfx-5-13.2X51-D15.4-domestic ...
Install jinstall-qfx-5-13.2X51-D15.4-domestic completed
Spawning the backup RE
Spawn backup RE, index 0 successful
GRES in progress
GRES done in 0 seconds
Waiting for backup RE switchover ready
GRES operational
Copying home directories
Copying home directories successful
Initiating Chassis In-Service-Upgrade
Chassis ISSU Started
ISSU: Preparing Daemons
ISSU: Daemons Ready for ISSU
ISSU: Starting Upgrade for FRUs
ISSU: FPC Warm Booting
ISSU: FPC Warm Booted
ISSU: Preparing for Switchover
ISSU: Ready for Switchover
Checking In-Service-Upgrade status
  Item          Status          Reason
  FPC 0         Online (ISSU)
Send ISSU done to chassisd on backup RE
Chassis ISSU Completed
ISSU: IDLE
Initiate em0 device handoff
```



NOTE: An ISSU might stop instead of abort if the FPC is at the warm boot stage. Also, any links that go down and up will not be detected during a warm boot of the Packet Forwarding Engine (PFE).



NOTE: If the ISSU process stops, you can look at the log files to diagnose the problem. The log files are located at `/var/log/vjunos-log.tgz`.

5. Log in after the reboot of the switch completes. To verify that the software has been upgraded, enter the following command:

```
user@switch> show version
```


6. To ensure that the resilient dual-root partitions feature operates correctly, copy the new Junos OS image into the alternate root partitions of all of the switch:

```
user@switch> request system snapshot slice alternate
```

Resilient dual-root partitions allow the switch to boot transparently from the alternate root partition if the system fails to boot from the primary root partition.

**Related
Documentation**

- [New and Changed Features on page 30](#)
- [Changes in Behavior and Syntax on page 49](#)
- [Known Behavior on page 51](#)
- [Known Issues on page 60](#)
- [Resolved Issues on page 63](#)
- [Documentation Updates on page 68](#)
- [Product Compatibility on page 74](#)

Product Compatibility

- [Hardware Compatibility on page 74](#)
- [Software Compatibility on page 74](#)

Hardware Compatibility

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

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

<http://pathfinder.juniper.net/feature-explorer/>

Software Compatibility

The Juniper Networks implementation of the OVSDB management protocol on the QFX5100 switch supports the following OVSDB schema for physical devices versions:

- Starting with Junos OS Release 14.1X53-D10, OVSDB schema version 1.11.90. This schema version is compatible with NSX version 4.0.3
- Starting with Junos OS Release 14.1X53-D25, OVSDB schema version 1.3.0. This schema version is compatible with NSX version 4.0.3, and with NSX version 4.2 and later versions.

The Juniper Networks implementation of the Open vSwitch Database (OVSDB) management protocol on the QFX5100 switch is supported with the following VMware NSX versions:

- Starting with Junos OS Release 14.1X53-D10, NSX version 4.0.3.

Related Documentation

- Starting with Junos OS Release 14.1X53-D15, NSX version 4.2 and later versions.
- [New and Changed Features on page 30](#)
- [Changes in Behavior and Syntax on page 49](#)
- [Known Behavior on page 51](#)
- [Known Issues on page 60](#)
- [Resolved Issues on page 63](#)
- [Documentation Updates on page 68](#)
- [Migration, Upgrade, and Downgrade Instructions on page 69](#)

Third-Party Components

This product includes third-party components. To obtain a complete list of third-party components, see [Overview for Routing Devices](#).

For a list of open source attributes for this Junos OS release, see [Open Source: Source Files and Attributions](#).

Finding More Information

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

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

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

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- **Online feedback rating system**—On any page at the Juniper Networks Technical Documentation site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <https://www.juniper.net/cgi-bin/docbugreport/>.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

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

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

Self-Help Online Tools and Resources

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

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

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

Opening a Case with JTAC

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

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

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

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

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

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

Revision History

29 July 2016—Revision 2, Junos OS for the EX Series and the QFX Series, Release 14.1X53-D27—Removed item from QFX Series New Features, added item to Documentation Updates.

23 June 2015—Revision 1, Junos OS for the EX Series and the QFX Series, Release 14.1X53-D27—initial release

Copyright © 2016, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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