Junos® OS Software Release Notes for the Juniper Networks QFX Series

Release 12.1 X49-D20
24 August 2012
Revision 3

Contents

New Features in Junos OS Release 12.1 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.

Hardware

- **Support for SFP (small form-factor pluggable) interface modules on management board interfaces (QFX3500 switches)**—Provides two management interfaces that support Gigabit Ethernet SFP modules.

High Availability

- **Graceful protocol restart for BGP and OSPF protocols (QFX3500 switches)**—With standard implementations of routing protocols, any service interruption requires an affected routing device to recalculate adjacencies with neighboring routing devices, restore routing table entries, and update other protocol-specific information. An unprotected restart of a routing device can result in forwarding delays, route flapping, wait times stemming from protocol reconvergence, and even dropped packets. Graceful protocol restart allows a restarting routing device and its neighbors to continue forwarding packets without disrupting network performance.

  On QFX3500 switches, you can configure graceful protocol restart for the BGP and OSPF protocols.

Interfaces

- **Layer 3 logical interfaces (QFX3500 switches)**— A Layer 3 logical interface is a logical division of a physical interface or an aggregated Ethernet interface, which operates at the network level and can receive and forward IEEE 802.1Q VLAN tags. You can use these interfaces to route traffic between multiple VLANs along a single trunk line that connects a QFX3500 switch to a Layer 2 switch. Only one physical connection is required between the switches. This topology is often called a “router on a stick” or a “one-armed router” when the Layer 3 device is a router.

  To create Layer 3 logical interfaces on a QFX3500 switch, enable VLAN tagging, partition the physical interface into logical partitions, and bind the VLAN ID to the logical interface. You can partition one physical interface in up to 4089 different Layer 3 logical interfaces, one for each VLAN. We recommend that you use the VLAN ID as the logical interface number when you configure the logical interface. When you configure multiple VLANs on an interface, you must also enable tagging on that interface. VLAN tagging places the VLAN ID in the frame header, enabling each physical interface to handle multiple VLANs. Junos OS supports a subset of the 802.1Q standard for receiving and forwarding routed or bridged Ethernet frames with single VLAN tags and running Virtual Router Redundancy Protocol (VRRP) over 802.1Q-tagged interfaces. Double-tagging, which is assigning more than one VLAN ID in the frame header, is not supported.

Layer 2 Protocols

- **Q-in-Q tunneling and VLAN translation (QFX3500 switches)**—Enables service providers to create a Layer 2 Ethernet connection between two customer sites. Providers can segregate different customers’ VLAN traffic on a link (for example, if the customers use overlapping VLAN IDs) or bundle different customer VLANs into a single service VLAN. Data centers can use Q-in-Q tunneling and VLAN translation to isolate customer traffic within a single site or when customer traffic flows between cloud data centers in different geographic locations.
- **Layer 2 protocol tunneling (QFX3500 switches)**—Enables service providers to send Layer 2 protocol data units across the provider’s cloud and deliver them to switches that are not part of the local broadcast domain. This feature is useful when you want to run Layer 2 protocols (such as STP) between switches located at remote sites that are connected by a service provider network.
- **Private VLANs (QFX3500 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. 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 one another.
- **Virtual Ethernet Port Aggregator (VEPA) and reflective relay (QFX3500 Switches)**—Virtual Ethernet Port Aggregator (VEPA) technology takes all of the traffic generated by virtual machines located on a server and moves it to a physical switch. The physical switch then provides connectivity between the virtual machines located on the server, so the virtual machines do not talk directly to one another. A virtual switch can perform these tasks, but offloading switching activities from a virtual switch to a physical switch reduces the computing overhead on the virtual servers and takes advantage of the security, filtering, and management features of the physical switch.

  Reflective relay, also referred to as a “hairpin turn or “hairpin mode, returns aggregated packets to the VEPA by using the same downstream port that initially delivered the aggregated packets from the VEPA to the switch. Reflective relay must be configured on a physical interface located on the physical switch that receives aggregated packets, such as VEPA packets, because some of these packets might be sent back to the server and be destined for another virtual machine on the same server. Reflective relay only occurs in two situations:

  - When the destination address of the packet was learned on that downstream port.
  - When the destination has not yet been learned. Reflective relay does not otherwise change the operation of the switch. If the interface to which the virtual machine is connected and the MAC address of the virtual machine packet are not yet included in the Ethernet switching table for the virtual machine’s associated VLAN, an entry is added. If the source MAC address of an incoming packet under the respective VLAN is not yet present in the Ethernet switching table, the switch floods the packet on all the other ports that are members of the same VLAN, including the port on which the packet arrived.

Layer 3 Protocols

- **Bidirectional Forwarding Detection for static routes and the BGP, IS-IS, OSPF and RIP protocols (QFX3500 switches)**—The Bidirectional Forwarding Detection (BFD) protocol uses control packets and shorter detection time limits to rapidly detect failures in a network. Hello packets are sent at a specified, regular interval by routing devices. A neighbor failure is detected when a routing device stops receiving a reply after a specified interval.

  On QFX3500 switches, you can configure BFD for static routes and the BGP, IS-IS, OSPF, and RIP protocols.

- **IS-IS (QFX3500 switches)**—The Intermediate System–to–Intermediate System (IS-IS) protocol is an interior gateway protocol (IGP) for routing traffic within an autonomous system (AS). You can configure IS-IS at the **[edit protocols isis]** hierarchy level.

- **RIP (QFX3500 switches)**—The Routing Information Protocol (RIP) is an interior gateway protocol (IGP) for routing traffic within an autonomous system (AS). QFX3500 switches support RIPv1 and RIPv2. You can configure RIP at the **[edit protocols rip]** hierarchy level.

- **Virtual routing instances (QFX3500 switches)**—Enable you to divide a switch into multiple independent virtual routers, each with its own routing table. Splitting a device into many virtual routing instances isolates traffic traveling across the network without requiring multiple devices to segment the network. You can use virtual routing instances to isolate customer traffic on your network and to bind customer-specific instances to customer-owned interfaces. This release adds support for Protocol Independent Multicast (PIM) sparse mode.

Multicast Protocols

- **PIM-SSM (QFX3500 switches)**—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.

  To enable PIM-SSM, configure PIM sparse mode on all routing device interfaces and specify IGMPv3 on the host-facing interfaces. By default, a routing device enabled with PIM sparse mode and IGMPv3 accepts any SSM group multicast addresses in the IP address range from 232.0.0.0 through 232.255.255.255. However, you can extend SSM operations into another Class D multicast address range by including the **ssm-groups** statement at the **[edit routing-options multicast]** hierarchy level.

  You can also map IGMPv1 or v2 reports to IGMPv3 reports by creating a policy to match on these reports. To create the policy, include the **policy-statement *policy-name*** statement at the **[edit policy-options]** hierarchy level. To map the policy to PIM-SSM, include the **policy *policy-name*** statement at the **[edit routing-options multicast ssm-map map-name]** hierarchy level.

- **Bidirectional Forwarding Detection for PIM (QFX3500 switches)**—The Bidirectional Forwarding Detection (BFD) protocol uses control packets and shorter detection time limits to rapidly detect failures in a network. Hello packets are sent at a specified, regular interval by routing devices. A neighbor failure is detected when a routing device stops receiving a reply after a specified interval.

  On QFX3500 switches, you can configure BFD for Protocol Independent Multicast (PIM).

- **MSDP (QFX3500 switches)**—Enables you to connect multiple IP version 4 Protocol Independent Multicast sparse mode (PIM-SM) domains to one another. Multicast Source Discovery Protocol (MSDP) typically runs on the same routing device as a PIM-SM rendezvous point (RP). Each MSDP routing device establishes adjacencies with internal and external MSDP peers, similar to how BGP peering works. These peers inform each other about active sources within the domain. When they detect active sources, the peers send PIM sparse-mode explicit join messages to the active source. To configure MSDP, include the **msdp** statement at the **[edit protocols]** hierarchy level and specify groups of local addresses and MSDP peer addresses.

- **Anycast RP (QFX3500 switches)**—Supports multiple rendezvous points (RPs) using anycast addresses (RPs sharing a single routable IP address) in either a Protocol Independent Multicast (PIM) or Multicast Source Discovery Protocol (MSDP)-enabled network. To configure anycast RP, include the **anycast-pim** statement at the **[edit protocols pim rp local family inet]** hierarchy level.

- **IGMPv3 (QFX3500 switches)**—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. In Junos OS Release 12.1, the software supports include mode source filtering, in which hosts report interest in receiving packets that originate only from specific source addresses and are sent to a particular multicast group address. To configure IGMPv3, include the **version 3** statement at the **[edit protocols igmp interface interface-name]** hierarchy level.

- **IGMPv3 snooping (QFX3500 switches)**—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). Junos OS Release 12.1 adds support for IGMPv3 snooping.
- **IGMP filters (QFX3500 switches)**—Enable you to filter unwanted IGMP reports at the interface level. To filter IGMP group addresses (either IGMPv2 or IGMPv3), include the **route-filter** statement at the **[edit policy-statement policy-name from]** hierarchy level. To filter IGMP source addresses (IGMPv3 only), include the **source-address-filter** statement at the **[edit policy-statement policy-name from]** hierarchy level. Apply the filters by using the **group-policy *policy-name*** statement at the **[edit protocols igmp interface interface-name]** hierarchy level.

Network Management

- **Uplink failure detection (QFX3500 switches)**—Enables a switch to detect link failures on uplink interfaces and to propagate this information to downlink interfaces, so that servers connected to those downlink interfaces can switch over to secondary interfaces.

  Uplink failure detection supports network adapter teaming and provides network redundancy. In network adapter teaming, all of the network interface cards (NICs) on a server are configured in a primary or secondary relationship and share the same IP address. When the primary link goes down, the server transparently shifts the connection to the secondary link. With uplink failure detection, the switch monitors uplink interfaces for link failures. When it detects a failure, it disables the downlink interfaces. When the server detects a disabled downlink interface, it switches over to the secondary link to ensure traffic is not dropped but sent over the secondary path instead.

  When configuring uplink failure detection, you add an uplink interface and a corresponding downlink interface as a pair into a failure detection group. To add uplink interfaces to the group, include the **link-to-monitor *interface-name*** statement at the **[edit protocols uplink-failure-detection group *group-name*]** hierarchy level. To add downlink interfaces to the group, include the **link-to-disable *interface-name*** statement at the **[edit protocols uplink-failure-detection group *group-name*]** hierarchy level.
- **Port mirroring (QFX3500 switches)**—Copies packets entering or exiting a port or entering a VLAN and sends the copies to a local interface for local monitoring. You can use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on. Junos OS Release 12.1 adds support for remote analysis, which means that you can send the mirrored traffic to a VLAN that the analyzer is connected to.

Security

- **DHCP snooping (QFX3500 switches)**—Filters and blocks ingress DHCP server messages on untrusted ports and builds and maintains an IP address and MAC address binding database (called the DHCP snooping database).
- **Dynamic ARP inspection (DAI) (QFX3500 switches)**—Prevents ARP spoofing attacks. ARP requests and replies are compared against entries in the DHCP snooping database, and filtering decisions are made based on the results of those comparisons.
- **MAC move limiting (QFX3500 switches)**—Detects MAC movement and MAC spoofing on access ports.
- **Sticky MAC address (QFX3500 switches)**—Persistent (also called sticky) MAC addresses help restrict access to an access port by identifying the MAC addresses of workstations that are allowed access to a given access port. Secure access to these workstations is retained even if the switch is restarted.

Storage and Fibre Channel

- **DCBX application protocol TLV exchange (QFX3500 switches)**—Enables you to configure Layer 2 and Layer 4 application protocol TLV exchange on DCBX-enabled interfaces, by defining applications, mapping them to the IEEE 802.1p code points of incoming traffic, and applying the maps to interfaces. You define Layer 2 applications at the **[edit applications]** hierarchy level by including the **ether-type** statement, and you define Layer 4 applications by including the **protocol** and **destination-port** statements. You map applications to code points by including the **application** and **code-points** statements at the **[edit policy-options application-maps]** hierarchy level. You apply the application map to an interface by including the **application-map** statement at the **[edit dcbx interface]** hierarchy level.
- **Fibre Channel features (QFX3500 switches)**—Three new features have been added on systems configured as an FCoE-FC gateway: setting a load-balancing algorithm type, limiting the maximum number of FCoE login sessions per ENode, and ignoring the fabric worldwide name (WWN) in a fabric login accept message from the Fibre Channel switch. To configure the load-balancing algorithm, include the **load-balance-algorithm** statement at the **[edit fc-fabrics proxy]** hierarchy level. To configure the per ENode FCoE session limit, include the **max-sessions-per-enode** statement at the **[edit fc-fabrics protocols fip]** hierarchy level. To configure ignoring of the fabric WWN, include the **no-fabric-wwn-verify** statement at the **[edit fc-fabrics proxy]** hierarchy level.
- **Fibre Channel graceful restart (QFX3500 switches)**—Enables graceful restart of Fibre Channel processes running when the system is in FCoE-FC gateway mode. There is no user configuration for this feature: graceful restart is enabled automatically.

System Management

- **J-Web graphical interface (QFX3500 switches)**—The J-Web interface is an embedded Web-based device manager for the QFX Series. It provides an intuitive graphical user interface that allows users to configure, monitor, and maintain the various networking and security features available on the switch. It also provides troubleshooting and software management features. This version of the J-Web interface corresponds to the features available in the command line interface (CLI) of Junos OS Release 11.1 for the QFX Series. The J-Web interface is part of the **jinstall** package—no additional package is required.

Traffic Management

- **Ethernet PAUSE autonegotiation enhancements (QFX3500 switches)**—Enable you to configure asymmetric flow control. To configure PAUSE, include both the **rx-buffers** and **tx-buffers** statements at the **[edit interfaces interface-name ether-options configured-flow-control]** hierarchy level. The **rx-buffers** statement determines whether or not the interface generates and sends PAUSE messages. The **tx-buffers** statement determines whether or not the interfaces respond to received PAUSE messages.

Related Documentation

- Limitations in Junos OS Release 12.1 for the QFX Series on page 11
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for the QFX Series on page 10
- Outstanding Issues in Junos OS Release 12.1 for the QFX Series on page 13
- Resolved Issues in Junos OS Release 12.1 for the QFX Series on page 18
- Errata in Documentation for Junos OS Release 12.1 for the QFX Series on page 21
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for the QFX Series on page 22

Changes in Default Behavior and Syntax in Junos OS Release 12.1 for the QFX Series

This section lists the changes in default behavior and CLI syntax in Junos OS Release 12.1 for the QFX Series.

Security

- With Junos OS Release 12.1X49-D20, the following new firewall filter match conditions have been added:
  - **destination-port-range-optimize**
  - **source-port-range-optimize**

  If you use the new match conditions when you want a filter term to match a range of TCP or UDP port ranges, Junos OS uses the available memory much more efficiently than previously, which allows you to configure more firewall filters. For example, if you want to configure a filter to match a range using the original method, you might enter:


```
set firewall family inet filter f1 term t1 from protocol tcp
set firewall family inet filter f1 term t1 from source-port 1024-65535
```

With the new method, you would enter:

```
set firewall family inet filter f1 term t1 from protocol tcp
set firewall family inet filter f1 term t1 from source-port 1024-65535
set firewall family inet filter f1 term t1 from source-port-range-optimize
```

QFabric Deployment

- **Update to a QFabric device conversion command option (QFX3500 switches)**—The **fabric** option for the **request chassis device-mode** and **show chassis device-mode** commands has been renamed to **node-device**. This change enables you to identify which device mode your QFX3500 switch assumes in a QFabric system. The **fabric** statement will be supported for three releases and then deprecated, so we recommend you use the **node-device** option in Junos OS Release 12.1 and later.

Related Documentation

- New Features in Junos OS Release 12.1 for the QFX Series on page 3
- Limitations in Junos OS Release 12.1 for the QFX Series on page 11
- Outstanding Issues in Junos OS Release 12.1 for the QFX Series on page 13
- Errata in Documentation for Junos OS Release 12.1 for the QFX Series on page 21
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for the QFX Series on page 22

Limitations in Junos OS Release 12.1 for the QFX Series

This section lists the limitations in Junos OS Release 12.1 for the QFX Series.

Network Management

- If the QFX3500 switch drops traffic because of an ingress firewall filter, the switch does not generate an sFlow monitoring technology flow sample packet that contains this dropped traffic.

Storage

- A Fibre Channel fabric supports a maximum of four Fibre Channel over Ethernet (FCoE) VLAN interfaces.
- The maximum number of logins for each FCoE node (ENode) is a range of 32 to 2000 for trusted fabrics and 32 to 376 for untrusted fabrics. (Each ENode can log into 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, depends on how you configure the ports in a specified FC fabric. If you configure the ports as FCoE trusted, the maximum number of FCoE sessions (ENode

to FCF sessions) the system can support is 2500. If the ports are not FCoE trusted, the maximum number of FCoE sessions is 376.

- 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 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 interface. You cannot use a fixed classifier to map FCoE traffic to an interface because untagged traffic will be classified in the FCoE forwarding class, but FCoE traffic must have a priority tag (FCoE traffic cannot be untagged).

  For example, the following 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**

Traffic Management

- Classifiers are not supported on Layer 3 logical interfaces; therefore, classifiers cannot be applied to routed VLAN interfaces (RVIs). You can apply classifiers to Layer 2 logical interfaces.

Related Documentation

- New Features in Junos OS Release 12.1 for the QFX Series on page 3
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for the QFX Series on page 10
- Outstanding Issues in Junos OS Release 12.1 for the QFX Series on page 13
- Resolved Issues in Junos OS Release 12.1 for the QFX Series on page 18
- Errata in Documentation for Junos OS Release 12.1 for the QFX Series on page 21
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for the QFX Series on page 22

Outstanding Issues in Junos OS Release 12.1 for the QFX Series

The following issues are outstanding in Junos OS Release 12.1. 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 .

NOTE: Some issues that apply to EX Series switches may apply to the QFX Series as well. If you are looking for a resolved issue but cannot locate it in this section, see the "Resolved Issues in Junos OS Release 12.1 for the EX Series" section in the Junos OS 12.1 Release Notes.

- Configuration and File Management
- Ethernet Switching
- Hardware
- Interfaces
- Junos OS Basics
- Layer 3 Protocols
- Multicast
- Network Management
- Security
- Storage
- System Administration
- Traffic Management

Configuration and File Management

- On QFX3500 switches with STP configured, the **show ethernet-switching interfaces ae0** command incorrectly shows an LACP-enabled aggregated Ethernet interface as being "Blocked by STP" instead of being operationally down. [PR/676448]

Ethernet Switching

- On a QFX3500 switch, if you create 4090 VLANs (the maximum number of VLANs) and any of them are private secondary VLANs (community or isolated VLANs), a problem occurs if you later reduce the number of VLANs. In this case, traffic for the secondary VLANs is not forwarded between switches that participate in those VLANs. [PRs/611015, 671831]
- On a QFX3500 switch, Multiple Spanning Tree Protocol (MSTP) incorrectly displays internal ports as boundary ports when a peer port is disabled at the initial commit operation. Enabling the peer port fixes this problem and displays the internal ports correctly. [PR/688118]

- On a QFX3500 switch, when you configure Q-in-Q tunneling on an interface, persistent MAC learning does not happen. The MAC entries are learned as dynamic entries. [PR/720380]
- On a QFX3500 switch, if you capture packets with an egress port mirroring analyzer for traffic using VLAN translation or Q-in-Q rules, the access port and mirroring port might receive packets with different tag values as follows:
  - On access ports, packets captured by an egress analyzer might have a provider VLAN tag and an ethertype value of 0x8100, which differ from those of the original egress packet.
  - On trunk ports, packets captured by an egress analyzer might have an outer tag EtherType value of 0x8100, whereas the configured 802.1Q EtherType might be different.

  [PR/702568]
- On a QFX3500 switch with MSTP configured, a port whose peer port does not have MSTP enabled may be incorrectly displayed as a nonboundary port. [PR/720794]
- On a QFX3500 switch, a port mirroring analyzer configured to match on ingress packets in a VLAN does not match protocol data units (PDUs) for Layer 2 protocols (for example, STP or LACP). These Layer 2 control PDUs are not mirrored to the output interface or VLAN configured in the analyzer. [PR/725710]
- On a QFX3500 switch, if you use Q-in-Q tunneling for a configuration that includes private VLANs, you must explicitly enable tunneling for untagged traffic to be forwarded to the secondary VLANs. Use either of the following statements for this purpose:
  - **set vlans *vlan-name* dot1q-tunneling customer-vlan native**
  - **set vlans *vlan-name* interface *interface-name* mapping native push**

  [PR/728758]
- On a QFX3500 switch, you can use the statement **set vlans *vlan-name* interface *interface-name* mapping-range** to map a range of customer VLANs to a range of service VLANs instead of using multiple **set vlans *vlan-name* interface *interface-name* mapping (push | swap)** statements to configure Q-in-Q tunneling or VLAN translation on a per-VLAN basis. If you enter this statement and configure a range in which the first value is larger than the second value (which is unsupported), you see an error message that does not clearly describe the problem. [PR/728938]
- On a QFX3500 switch, if you configure multiple VLAN translations on an access interface, LLDP advertises only one of the C-VLAN IDs for which the mapping rules are configured. Neighboring devices do not learn the other C-VLAN IDs. [PR/736142]
- If you enable Layer 2 Protocol Tunneling on a QFX3500 switch and there are a large number of VLANs configured, the command **show ethernet-switching layer2-protocol-tunneling statistics** might not work. In this case, Layer 2 tunneling works properly, but the CLI command does not display any output. [PR/739027]

- On a QFX3500 switch, if traffic is flowing from tens of thousands of different MAC addresses and you issue the **clear ethernet-switching table** command, the switches can take more than 30 minutes to complete MAC learning. [PR/683515]
- On a QFX3500 switch, if you make several simultaneous changes to VLANs and an associated routed VLAN interface (RVI) and then issue a commit operation, ARP resolution might fail on the RVI interface. [PR/692103]

Hardware

- On QFX3500 switches, if the ambient temperature decreases to below 10 degrees C after a link is established, you may see transmission failure on ports 0 through 5, and 42 through 47 if those ports were configured with QFX-SFP-DAC-5M cables. The workaround is to use 1M or 3M DAC cable or SFP+ optical fiber cable on those ports if you expect ambient temperature to drop below 10 degrees C. [PR/570748]
- On QFX3500 switches, the **show chassis environment** and **show chassis hardware** commands show installed but unpowered PSUs as **absent** rather than **present**. [PR/580026]

Interfaces

- On QFX3500 switches, if you change the family of an interface by using the **load override** command, the interface might not be configured properly and might drop traffic as a result. To prevent this from occurring, use separate operations to delete the original family and configure the new family. For example, you might perform the following steps:

  1. Delete **family ethernet-switching** from an interface.
  2. Commit the change.
  3. Configure **family inet** for the same interface.
  4. Commit the change.

  [PR/668600]

Junos OS Basics

- On a QFX3500 switch, if you configure multiple routing instances, and each routing instance contains a link aggregation group (LAG) interface connected to another QFX3500 switch, one of the LAGs might be declared down even though all of its member interfaces are up. As a workaround, disable and enable each member link of the affected LAG to bring the LAG to the **up** state. [PR/612277]
- On a QFX3500 switch, targeted broadcast does not work. [PR/693801]
- On a QFX3500 switch, configure both the transmitting link and the receiving link mode as active when you configure LACP. [PR/744095]

- On a QFX3500 switch, the value of the ifInErrors field in the sFlow datagram for an interface does not match the value of the Input errors field in the output of the **show interfaces extensive** command for the same interface. [PR/603525]
- On a QFX3500 switch, momentary loss of Layer 3 unicast traffic might occur when traffic is switched from the default route to the longest prefix match (LPM) route. [PR/607695]

Layer 3 Protocols

- On a QFX3500 switch, IGMP group-specific queries without the router alert option are flooded to interested members only, and IGMP group-specific queries with the router alert option are flooded to all ports in the VLAN. [PR/684738]
- On a QFX3500 switch, although the **igmp-snooping** statement at the **[edit routing-instances instance-name protocols]** hierarchy level is visible, it is not supported. When you configure IGMP snooping in a routing instance, the configuration does not work. [PR/729629]
- On a QFX3500 switch, when ICMP redirect messages are sent out to the sending host by a receiving router to redirect the packet to a different IP address in the same LAN segment, forwarding of the data happens in both software and hardware in the receiving router. Software forwarding need not happen in this scenario. This could result in receipt of duplicate packets by the receiving host. However the sending host routes the data to the redirected or new IP address on receipt of the ICMP redirect messages, so this condition is only momentary. [PR/730549]
- On a QFX3500 switch, you might not be able to establish an internal BGP (IBGP) Bidirectional Forwarding Detection (BFD) session to an MX Series router. [PR/709400]
- On a QFX3500 switch, if you apply a single-rate two-color policer with more than 128 terms in a firewall filter, the output of the **show firewall** command displays incorrect data for the single-rate two-color policer associated with the firewall filter. [PR/667201]
- On a QFX3500 switch, if you enable IGMP snooping, some unregistered multicast MAC addresses in the **03-** and **09-** ranges might not be permitted and might cause some interoperability issues. [PR/691943]

Multicast

- On a QFX3500 switch, if a multicast route entry in the forwarding table is listed as **discard**, MSDP traffic might not be forwarded. [PR/728619]
- On a QFX3500 switch, the output of the **show msdp brief** command might display incorrect values for the **SA count** field. [PR/732115]
- On a QFX3500 switch, if you configure PIM and PIM trace options within a virtual router routing instance, PIM trace options might show the wrong source IP address for outgoing PIM register messages. [PR/735035]
- On a QFX3500 switch, if you enable the **register** flag for PIM trace options, the trace options log might display the wrong source IP address for outgoing register messages. [PR/735035]

- On a QFX3500 switch, if you issue the **show pim interface interface-name instance instance-name** command, the output might not display the PIM interface state correctly. [PR/748410]
- If a QFX3500 switch acting as a Protocol Independent Multicast (PIM) rendezvous point (RP) router is on the same LAN as the PIM designated router and last-hop router, and IGMP snooping is enabled on the PIM interfaces, there might be an error in the multicast forwarding cache entry on the RP. If this occurs, you see that the RP interface type is PIMD (PIM-Decapsulator) when you enter the **show interfaces** command for the PIM interface. In this situation, multicast traffic is still forwarded correctly. [PR/681734]
- On QFX3500 switches, if you enter the **clear igmp-snooping membership vlan *vlan*** command for a VLAN that does not exist, you see an error message that begins with a meaningless number that you should ignore. [PR/683996]

Network Management

- On QFX3500 switches, even if you configure an egress sampling rate for sFlow monitoring, the switch uses the ingress sampling rate instead. [PR/686002]

Security

- On a QFX3500 switch, if you configure a firewall filter with more than 128 policers and attempt to apply the filter to a Layer 3 interface in the output direction, the commit operation fails and the filter is not created. [PR/745327]

Storage

- On a QFX3500 switch that has a large number of FCoE sessions (approximately 2000 sessions), when you issue the **show fibre-channel fip statistics** command, FLOGI_RJT messages may be counted as FDISC_RJT messages. (Messages that should appear in the FLOGI_RJT output may appear in the FDISC_RJT output.) [PR/740417]

System Administration

- On a QFX3500 switch, ingress and egress sFlow sampling can be enabled only on interfaces that are configured with the logical unit 0. Sampling using sFlow monitoring does not work on IEEE 802.1q subinterfaces with a nonzero logical unit number. [PR/693879]
- After you install the Junos SDK on a QFX3500 switch, you must reboot the switch to complete the installation. [PR/700167]
- On a QFX3500 switch, log messages with IP addresses assigned by a DHCP server are not displayed unless the **level** flag in the **traceoptions** statement is set. [PR/729571]

Traffic Management

- On a QFX3500 switch, the actual output rate is different than the expected output rate for no-loss and FCoE forwarding classes. When you configure a minimum guaranteed queue bandwidth (transmit rate) and enable priority-based flow control (PFC) on no-loss and FCoE queues, if the traffic consists of jumbo frames (frame size of 9216 bytes), the no-loss and FCoE queues might receive more or less bandwidth than expected. This is because the queue buffer stores fewer jumbo frames, and the transmit queue can be underrun when PFC temporarily stops the flow of frames. [PR/659621]

Related Documentation

- New Features in Junos OS Release 12.1 for the QFX Series on page 3
- Limitations in Junos OS Release 12.1 for the QFX Series on page 11
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for the QFX Series on page 10
- Errata in Documentation for Junos OS Release 12.1 for the QFX Series on page 21
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for the QFX Series on page 22

Resolved Issues in Junos OS Release 12.1 for the QFX Series

The following issues have been resolved in Junos OS Release 12.1.

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 .

NOTE: Some issues that apply to EX Series switches may apply to the QFX Series as well. If you are looking for a resolved issue but cannot locate it in this section, see the "Resolved Issues in Junos OS Release 12.1 for the EX Series" section in the Junos OS 12.1 Release Notes.

- Issues Resolved in Release Junos OS 12.1 X49-D20 on page 18
- Issues Resolved in Release Junos OS 12.1 X49-D1.2 on page 20

Issues Resolved in Release Junos OS 12.1 X49-D20

The following issues have been resolved in Junos OS Release 12.1 X49-D20. The identifier following each description is the tracking number in our bug database.

Ethernet Switching

- On a QFX3500 switch, Q-in-Q traffic forwarding may stop after a customer range change is applied with a deleted overlapping range in the same commit operation.. [PR/733942: This issue has been resolved.]

Junos OS Basics

- On a QFX3500 switch, pinging between directly connected interfaces does not work when one of the interfaces is the first 10-Gigabit Ethernet interface (xe-0/0/0) on the switch. [PR/730038: This issue has been resolved.]

Layer 3 Protocols

- QFX3500 switches running previous builds of Junos OS Release 12.1 might have stale ECMP entries even though there are no actual routes for those entries. [PR/797328: This issue has been resolved.]
- When the ECMP table temporarily overflows on QFX3500 switches running previous builds of Junos OS 12.1, the system does not queue the ECMP entries to be programmed into the packet forwarding engine. With Junos OS Release 12.1X49-D20, ECMP groups that cannot be installed when they are created because of insufficient memory space are saved until there is enough memory space to install them. [PR/801549: This issue has been resolved.]

Multicast Protocols

- On QFX3500 switches running previous builds of Junos OS Release 12.1, the multicast replication table is deleted if you configure more than the supported number of Layer 3 interfaces for multicast replication. [PR/787040: This issue has been resolved.]

Network Management

- On a QFX3500 switch running previous builds of Junos OS Release 12.1, the sflowd daemon might experience schedule delays during periods of high CPU utilization. If this occurs, the system displays messages similar to the following:

  Jul 2 07:39:07 iad7-br-fab-f1t1-r1 sflo[16261]: %DAEMON-3-JTASK_SCHED_SLIP: 4 sec scheduler slip, user: 0 sec 15601 usec, system: 0 sec, 31577 usec

  Jul 2 07:39:31 iad7-br-fab-f1t1-r1 sflo[16261]: %DAEMON-3-JTASK_SCHED_SLIP: 5 sec scheduler slip, user: 0 sec 16440 usec, system: 0 sec, 26689 usec

  Jul 2 07:39:53 iad7-br-fab-f1t1-r1 sflo[16261]: %DAEMON-3-JTASK_SCHED_SLIP: 4 sec scheduler slip, user: 0 sec 11029 usec, system: 0 sec, 34085 usec

  Core dumps might also occur during periods of high CPU utilization. This issue has been resolved in Junos OS Release 12.1X49-D20. [PR/793135: This issue has been resolved.]

Security

- if you upgrade to a previous build of Junos OS Release 12.1 on a QFX3500 switch, a firewall filter applied to the loopback interface might block DHCP discover packets. [PR/756151: This issue has been resolved.]

System Administration

- When installing a Junos OS image on a QFX3500 switch, you might see the error message **LA : fips-mode:: not found**. This does not indicate a problem with the installation and may be safely ignored. [PR/739453: This issue has been resolved.]

Issues Resolved in Release Junos OS 12.1 X49-D1.2

The following issues have been resolved in Junos OS Release 12.1 X49-D1.2. The identifier following each description is the tracking number in our bug database.

Configuration and File Management

- With the previous release of Junos OS Release 12.1 X49-D1, the following message appears when you install the software image on a QFX3500 switch:

  At least one package installed on this device has limited support. Run 'file show /etc/notices/unsupported.txt' for details.

  The message can be ignored, and it does not appear in Junos OS Release X49-D1.2. [PR/754332 and PR/755048: This issue has been resolved.]

- With the previous release of Junos OS Release 12.1X49-D1, the period packet management daemon (ppmd) might crash and produce core files repeatedly if

Bidirectional Forwarding Detection (BFD) is enabled. This daemon is responsible for periodic transmission of packets on behalf of its various client processes, such as BFD, and it also receives packets on behalf of client processes. [PR/745180: This issue has been resolved.]

Related Documentation

- New Features in Junos OS Release 12.1 for the QFX Series on page 3
- Limitations in Junos OS Release 12.1 for the QFX Series on page 11
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for the QFX Series on page 10
- Outstanding Issues in Junos OS Release 12.1 for the QFX Series on page 13
- Errata in Documentation for Junos OS Release 12.1 for the QFX Series on page 21
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for the QFX Series on page 22

Errata in Documentation for Junos OS Release 12.1 for the QFX Series

This section lists outstanding issues with the documentation.

Standards Support

- In addition to the standards listed in the Standards Supported by the Junos OS document, the QFX Series supports the following RFC standards:
  - *IEEE 802.1ad (QinQ)*
  - *IEEE 802.3x (Ethernet PAUSE)*
  - *RFC 1142, OSI IS-IS Intra-domain Routing Protocol*
  - *RFC 1591 Domain Name System Structure and Delegation*

Related Documentation

- New Features in Junos OS Release 12.1 for the QFX Series on page 3
- Limitations in Junos OS Release 12.1 for the QFX Series on page 11
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for the QFX Series on page 10
- Outstanding Issues in Junos OS Release 12.1 for the QFX Series on page 13
- Resolved Issues in Junos OS Release 12.1 for the QFX Series on page 18
- Upgrade and Downgrade Instructions for Junos OS Release 12.1 for the QFX Series on page 22

Upgrade and Downgrade Instructions for Junos OS Release 12.1 for the QFX Series

This section discusses the following topics:

Procedure for Upgrading CoS from Junos OS Release 11.1 or Release 11.2 to Release 11.3 or Later

Before you upgrade to Junos OS Release 11.3 or later, you must deactivate the CoS configuration on the QFX3500 switch if the CoS configuration uses the **excess-rate** option, **strict-high** or **high** priority queues, or any of the default multidestination forwarding classes. For full information about this topic, see Overview of CoS Upgrade Requirements (Junos OS Release 11.1 or 11.2 to a Later Release). A summary of the upgrade steps is included here.

After you upgrade to Junos OS Release 11.3 or later, modify the CoS configuration on the QFX3500 switch to conform to the Junos OS Release 11.3 or later CoS requirements. Then activate the CoS configuration and commit the changes:

1. Deactivate the CoS configuration.

   user@switch# **deactivate class-of-service**

2. Upgrade to Junos OS Release 11.3 or later.
3. Make the following changes to the CoS configuration:
   - Remove the **excess-rate** option from the CoS configuration if you have used it at the **[edit class-of-service schedulers]** or **[edit class-of-service traffic-control-profiles]** hierarchy level.
   - Remove the default multidestination forwarding classes (**mcast-be**, **mcast-af**, **mcast-ef**, and **mcast-nc**) if you have used them at the **[edit class-of-service schedulers]**, **[edit class-of-service rewrite-rules]**, or **[edit class-of-service classifiers]** hierarchy level. Alternatively, you can change the mapping of the multidestination traffic to use the new default multidestination forwarding class (**mcast**).
4. If desired, configure **strict-high** priority queues in accordance with the Junos OS Release 11.3 or later **strict-high** priority queue rules, and map multidestination traffic to the default multidestination forwarding class (**mcast**).
5. Activate the CoS configuration.

   user@switch# **activate class-of-service**

6. Commit the CoS configuration.

NOTE: If you have configured the **transmit-rate** option for any queues at the **[edit class-of-service schedulers]** hierarchy level, if the rate is configured as an exact rate in Mbps, we recommend that you reconfigure the **transmit-rate** option as a percentage. This is because the scheduler converts exact rates to percentages, and when the exact rate is below 1 Gbps, some granularity may be lost in the conversion. You can avoid this potential issue by specifying the **transmit-rate** option as a percentage.

Basic Procedure for Upgrading to Junos OS Release 12.1

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

NOTE: You cannot upgrade by more than three releases at a time. For example, if your routing device is running Junos OS Release 11.1, you can upgrade to Junos OS Release 11.3 but not to Junos OS Release 12.1. As a workaround, first upgrade to Junos OS Release 11.3 and then upgrade to Junos OS Release 12.1.

NOTE: In some cases, when you downgrade the QFX3500 switch to an earlier software version, the switch might not operate properly. As a workaround, choose one of the following options when downgrading:

1. Issue the **request system software add** command to downgrade to the following software versions or later:
   - Junos OS Release 11.1R5
   - Junos OS Release 11.2R2
   - Junos OS Release 11.3R1
2. Include the **no-validate** option when you issue the **request system software add** command during a downgrade to a software version earlier than the ones listed in option #1.

The download and installation process for Junos OS Release 12.1 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 **12.1** 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 Switch Install Package** for the 12.1 X49-D20 release.
5. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
6. Download the software to a local host.
7. Copy the software to the device or to your internal software distribution site.
8. 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 validate *source*/jinstall-qfx-12.1 X49D20-D1-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)

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

   Adding the **reboot** command reboots the switch after the upgrade is validated and 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 12.1 **jinstall** package, you cannot issue the **request system software rollback** command to return to the previously installed software. Instead you must issue the **request system software add validate** command and specify the **jinstall** package that corresponds to the previously installed software.

Upgrade and Downgrade Support Policy for Junos OS Extended End-of-Life Software 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. However, you cannot upgrade directly from a non-EEOL release that is more than three releases before or after.

To upgrade or downgrade from a non-EEOL release to a release more than three releases before or after, first upgrade to the next EEOL release and then upgrade or downgrade from that EEOL release to your target release. For more information on EEOL releases and to review a list of EEOL releases, see Junos Software Release Dates and Milestones.

Related Documentation

- New Features in Junos OS Release 12.1 for the QFX Series on page 3
- Limitations in Junos OS Release 12.1 for the QFX Series on page 11
- Changes in Default Behavior and Syntax in Junos OS Release 12.1 for the QFX Series on page 10
- Outstanding Issues in Junos OS Release 12.1 for the QFX Series on page 13
- Errata in Documentation for Junos OS Release 12.1 for the QFX Series on page 21

QFX Series Documentation for Junos OS Release 12.1

Title	Description
QFX3500 Hardware Documentation	Component descriptions, site preparation, installation, replacement, and safety and compliance information for QFX3500 switches
Complete Software Guide for Junos OS for the QFX Series, Release 12.1	Software feature descriptions, configuration examples, and tasks for Junos OS for the QFX Series
Junos OS Software Release Notes for the Juniper Networks QFX Series, Release 12.1	Summary of hardware and software features, and known problems with the software and hardware

Requesting Support

For technical support, open a support case with the Case Manager link at http://www.juniper.net/customers/support/, email the technical assistance center (TAC) at support@juniper.net, or call 1-888-314-JTAC (from the United States, Canada, or Mexico) or 1-408-745-9500 (from elsewhere).

Revision History

24 August 2012—Revision 3, Junos OS for the QFX Series, Release 12.1