Release Notes: Junos® OS Release 15.1X53-D34 for QFX10000 Switches

Release 15.1X53-D34
October 4, 2016
Revision 2

Contents

Junos OS Release Notes for QFX10000 Switches

These release notes accompany Junos OS Release 15.1X53-D34 for QFX10000 switches.

New and Changed Features for QFX10000 Switches

This section describes the new features in Junos OS Release 15.1X53-D30 for QFX10000 switches.

NOTE: For further information about the features, see the Complete Software Guide for Junos OS for QFX10000 Switches, Release 15.1X53-D30.

New Features in Release 15.1X53-D30

Hardware

- **QFX10008 switch**—The Juniper Networks QFX10000 line of Ethernet switches provides cloud builders and data center operators scalable solutions for both core and spine data center deployments. The QFX10008 switch is an 8-slot, 13 U chassis that supports up to eight line cards.
- **Support for 100-Gigabit optical transceivers (QFX10008 switch)**—Provides support for:
  - JNP-QSFP 100G-SR4—QSFP28 module 100GBASE-SR4, 100-Gigabit Ethernet pluggable; 850 nm for up to 150 m transmission on multi-mode fiber (MMF) cable.
  - JNP-QSFP-100G-LR4—QSFP28 module 100GBASE-LR4, 100-Gigabit Ethernet pluggable; 1310 nm for up to 10 km single-mode fiber-optic (SMF) cable.
- **Support for 40-Gigabit optical transceivers (QFX10008 switch)**—Provides support for:
  - QFX-QSFP-40G-SR4—QSFP+ module 40GBASE-SR4, 40-Gigabit Ethernet optics; 100 m transmission on OM3, MMF cable and 150 m transmission on OM4, MMF cable.
  - QFX-QSFP-40G-ESR4—Juniper Networks proprietary 4X10G-IR parallel single mode QSFP+ module, 40-Gigabit Ethernet- optics; 300m transmission on OM3, MMF cable or 400 M transmission on OM4 cable.
  - JNP-QSFP-4X10GE-IR—QSFP+ parallel single mode module 40-Gigabit Ethernet pluggable; 1.4 km transmission on SMF cable.
  - JNP-QSFP-40GE-IR4—Juniper Networks proprietary 40GBASE-IR4, 40Gigabit Ethernet pluggable; 2 km transmission on SMF cable.
  - JNP-QSFP-40G-LR4—QSFP+ module 40GBASE-LR4, 40-Gigabit Ethernet pluggable; 10 km transmission on SMF cable.

  - JNP-QSFP-4X10GE-LR—Juniper Networks proprietary 4X10G-LR, 40-Gigabit Ethernet; 10 km transmission on SMF cable.
  - JNP-QSFP-40G-LX4—QSFP+ module 40GBASE-LX4, 40-Gigabit Ethernet pluggable;2 km transmission on SMF cable, 100 m transmission on OM3, MMF cable, or 150 m transmission on OM4, MMF cable

- **Support for 1-Gigabit optical transceivers on the SFP management port (QFX10008 switch)**—Provides support for:
  - QFX-SFP-1GE-SX—SFP module 1000BASE-SX Gigabit Ethernet; 220 m transmission on FDDI, MMF cable, 275 m transmission on OM1, MMF cable, or 550 m transmission on OM2 cable.
  - QFX-SFP-1GE-T—SFP module 1000BASE-T Gigabit Ethernet; 100m transmission on Category 5 cable.
  - QFX-SFP-1GE-LX—SFP module 1000BASE-LX Gigabit Ethernet; 10 km transmission on SSF cable, 550 m transmission on OM1, MMF cable, or 550 m transmission on OM2, MMF cable.
- **QFX10000-36Q line card (QFX10008 switches)**—Provides 36 ports of 40-gigabit QSFP+. Twelve ports are designed to be 100-gigabit capable using QSFP28. Each 40-gigabit QSFP+ can be configured as either a native 40-gigabit port or four 10-gigabit ports using a breakout cable. With breakout cables, the line card supports a maximum of 144 logical 10-Gigabit Ethernet ports.
- **QFX10000-30C line card (QFX10008 switches)**—Provides 30 ports of either 100-gigabit or 40-gigabit QSFP28. The ports autodetect the type of transceiver installed and set the configuration to the appropriate speed.

High Availability and Resiliency

- **High availability feature support (QFX10008 switch)**—The QFX10008 switch supports the following high availability features:
  - **Graceful Routing Engine switchover (GRES)**—Enables a switch with redundant Routing Engines to continue forwarding packets, even if one Routing Engine fails. To configure GRES, include the **graceful-switchover** statement at the **[edit chassis redundancy]** hierarchy level and the **synchronize** statement at the **[edit system commit]** hierarchy level.
  - **Nonstop active routing (NSR)**—Uses the same infrastructure as GRES to preserve interface and kernel information. NSR also saves routing protocol information by running the routing protocol process (rpd) on the backup Routing Engine. To configure NSR, include the **nonstop-routing** statement at the **[edit routing-options]** hierarchy level.
  - **Nonstop bridging (NSB)**—Uses the same infrastructure as GRES to preserve interface and kernel information. NSB also saves Layer 2 Control Protocol (L2CP) information by running the Layer 2 Control Protocol process (l2cpd) on the backup Routing

Engine. To configure NSB, include the **nonstop-bridging** statement at the **[edit protocols layer2-control]** hierarchy level.

Infrastructure

- **Secure Boot (QFX10008 switch)**—Junos OS Release 15.1X53-D30 introduces a significant system security enhancement: Secure Boot. The Secure Boot implementation is based on the UEFI 2.4 standard. The BIOS has been hardened and serves as a core root of trust. The BIOS updates, the bootloader, and the kernel are cryptographically protected. No action is required to implement Secure Boot.

Interfaces and Chassis

- **Adaptive load balancing (ALB) for aggregated Ethernet bundles (QFX10008 switch)**—ALB evenly distributes data flows across aggregated Ethernet member links. You use ALB to manage uneven or overloaded data flows on member links. ALB supports up to 64 member links and up to 50 aggregated Ethernet bundles. The algorithm determines which link to use by taking into account the scanned packet or bit rate associated with each hash value in conjunction with the mapping of hash values to a given link. ALB can be applied to IPv4, IPv6, and MPLS packet headers. ALB is disabled by default.

  Configure ALB by setting the adaptive statement at the **[edit interfaces ae-interface aggregated-ether-options load-balance]** hierarchy level. Under the **load-balance** statement, you can set the following ALB options:

  - **scan-interval interval**—Scan interval in multiples of 30 seconds to check the tolerance deviation. The range is 1 to 5. The default is 1.
  - **bps**—Scan traffic in bits per second (pps). The default is bits per second.
  - **pps**—Scan traffic in packets per second (pps).

- **Channelizing 40-Gigabit Ethernet QSFP+ ports (QFX10008 switch)**—This feature enables you to channelize four 10-Gigabit Ethernet interfaces from the 40-Gigabit Ethernet QSFP+ interfaces. Channelization is supported on fiber break-out cable using standard structured cabling techniques.

  NOTE: **This feature is not supported on the QFX10000-30C line card.**

  By default, the 40-Gigabit Ethernet QSFP+ interfaces are named **et-fpc/pic/port**. The resulting 10-Gigabit Ethernet interfaces appear in the following format: **xe-fpc/pic/port:channel**, where channel can be a value of 0 through 3. To channelize a 40-Gigabit Ethernet QSFP+ interface into four 10-Gigabit Ethernet interfaces, include the **10g** statement at the **[edit chassis fpc fpc-slot pic pic-slot (port port-number | port-range port-range-low port-range-high) channel-speed]** hierarchy level. To revert the 10-Gigabit Ethernet channels to a full 40-Gigabit Ethernet interface, remove the **10g** statement from the same hierarchy level.

  There are 100-Gigabit Ethernet ports that work either as 100-Gigabit Ethernet or as 40-Gigabit Ethernet but are recognized as 40-Gigabit Ethernet by default. You cannot

channelize the 100-Gigabit Ethernet ports when they are operating as 100-Gigabit Ethernet interfaces. The 40-Gigabit Ethernet ports can operate independently or be channelized into four 10-Gigabit Ethernet ports as part of a port range. Ports cannot be channelized individually. Only the first and fourth port in each 6XQSFP cage is available to channelize as part of a port range. In a port range, the ports are bundled with the next two consecutive ports. For example, if you want to channelize ports 0 through 2, you channelize port 0 only. If you try to channelize a port that is not supported, you receive an error message when you commit the configuration. Auto-channelization is not supported on any ports.

When a 40-Gigabit Ethernet transceiver is inserted into a 100-Gigabit Ethernet port, the port recognizes the 40-Gigabit Ethernet port speed. When a 100-Gigabit Ethernet transceiver is inserted into the port and enabled in the CLI, the port recognizes the 100-Gigabit Ethernet speed and disables two adjacent 40-Gigabit Ethernet ports.

- **Link aggregation (QFX10008 switch)**—Link aggregation enables you to use multiple network cables and ports in parallel to increase link speed and redundancy.
- **Multichassis link aggregation group (MC-LAG) (QFX10008 switch)—**MC-LAG enables a client device to form a logical LAG interface using two QFX10008 switches. MC-LAG provides redundancy and load balancing between the two QFX10008 switches, multihoming support, and a loop-free Layer 2 network without running STP.

  On one end of an MC-LAG is an MC-LAG client that has one or more physical links in a LAG. This client does not need to detect the MC-LAG. On the other side of the MC-LAG are two MC-LAG QFX10008 switches. Each of these QFX10008 switches has one or more physical links connected to a single client. The QFX10008 switches coordinate with each other to ensure that data traffic is forwarded properly.

  To configure an MC-LAG, include the following statements:

  - **mc-ae** statement at the **[edit interfaces *interface-name* aggregated-ether-options]** hierarchy level
  - **iccp** statement at the [**edit protocols]** hierarchy level
  - **multi-chassis** statement at the **[edit]** hierarchy level

- **Ability to create link aggregation groups with interfaces operating at different speeds (QFX10008 switch)**—You can add 10-Gigabit Ethernet, 40-Gigabit Ethernet, and 100-Gigabit Ethernet interfaces into the same link aggregation group (LAG). Configuring LAGs with interfaces configured at speeds other than 10g, 40g, and 100g is not supported.
- **Support for Layer 3 logical interfaces (QFX10008 switch)**—A Layer 3 logical interface is a logical division of a physical interface or an aggregated Ethernet interface that operates at the network level and that 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 QFX10008 switch to a Layer 2 switch. Only one physical connection is required between the switches.
- **Generic routing encapsulation (GRE) support (QFX10008 switch)**—You can use GRE tunneling services to encapsulate any network layer protocol over an IP network. Acting as a tunnel source router, the switch encapsulates a payload packet that is to

be transported through a tunnel to a destination network. The switch first adds a GRE header and then adds an outer IP header that is used to route the packet. When it receives the packet, a switch performing the role of a tunnel remote router extracts the tunneled packet and forwards the packet to the destination network. GRE tunnels can be used to connect noncontiguous networks and to provide options for networks that contain protocols with limited hop counts.

- **Enhanced hash key (QFX10002 switches)**—Starting with Junos OS Release 15.1X53-D30, you can configure the **inet**, **inet6**, GRE, **no-mpls**, **vxlan-vnid**, and **hash-seed** values for load-balancing functions. By default, the QFX10002 switches use the system MAC address to generate a **hash-seed** value. You can configure the value for the **hash-seed** statement at the **[edit forwarding-options enhanced-hash-key]** hierarchy level. The **fabric-load-balance** and **user-defined-fields** statements are not supported at the **[edit forwarding-options enhanced-hash-key]** hierarchy level.
- **Support for Micro BFD over child links of AE or LAG bundle (cross-functional Packet Forwarding Engine/kernel/rpd) (QFX10002 switches)**—Provides a Layer 3 BFD liveness detection mechanism for child links of the Ethernet LAG interface. In scenarios in which you do not have a point-to-point link, and a Layer 1 device fails at one end of the link, Micro BFD detects failures faster than traditional LACP. Micro BFD sessions are independent of each other despite having a single client that manages the LAG interface. Micro BFD is not supported on pure Layer 2 interfaces. To enable failure detection for aggregated Ethernet interfaces, include the **bfd-liveness-detection** statement at the **[edit interfaces aex aggregated-ether-options bfd-liveness-detection]** hierarchy level.

Layer 2 Features

- **VLAN support (QFX10008 switch)**—VLANs enable you to divide one physical broadcast domain into multiple virtual domains.
- **Link Layer Discovery Protocol (LLDP) support (QFX10008 switch)**—LLDP enables a switch to advertise its identity and capabilities on a LAN, as well as receive information about other network devices.
- **Q-in-Q tunneling support (QFX10008 switch)**—This feature allows service providers on Ethernet access networks to extend a Layer 2 Ethernet connection between two customer sites. Using Q-in-Q tunneling, providers can also segregate or bundle customer traffic into fewer VLANs or different VLANs by adding another layer of 802.1Q tags. Q-in-Q tunneling is useful when customers have overlapping VLAN IDs, because the customer's 802.1Q (dot1Q) VLAN tags are prepended by the service VLAN (S-VLAN) tag.
- **Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and VLAN Spanning Tree Protocol (VSTP) support (QFX10008 switch)**—These protocols enable a switch to advertise its identity and capabilities on a LAN and receive information about other network devices.

Layer 3 Features

- **BGP support (QFX10008 switch)**—BGP is an exterior gateway protocol (EGP) for routing traffic between autonomous systems (ASs). You can configure BGP at the **[edit protocols bgp]** hierarchy level.
- **OSPF support (QFX10008 switch)**—The IPv4 OSPF protocol is an interior gateway protocol (IGP) for routing traffic within an autonomous system (AS). QFX10008 switches support OSPFv1 and OSPFv2. You can configure OSPF at the **[edit protocols ospf]** hierarchy level.
- **Bidirectional Forwarding Detection (BFD) support for static routes and the BGP, IS-IS, OSPF, PIM, and RIP protocols (QFX10008 switch)**—BFD uses control packets and shorter detection time limits to rapidly detect failures in a network. Hello packets are sent at a specified, regular interval by routing devices. A neighbor failure is detected when a routing device stops receiving a reply after a specified interval.

  On a QFX10008 switch, you can configure BFD for static routes and for the BGP, IS-IS, OSPF, PIM, and RIP protocols.
- **IS-IS support (QFX10008 switch)**—The IS-IS protocol is an IGP for routing traffic within an AS.
- **Virtual Router Redundancy Protocol (VRRP) support (QFX10008 switch)**—VRRP enables you to provide alternative gateways for end hosts that are configured with static default routes. You can implement VRRP to provide a highly available default path to a gateway without needing to configure dynamic routing or router discovery protocols on end hosts.
- **IPv4 address conservation method for hosting providers (QFX10008 switch)**—If your company hosts servers for customers, you might be using many routable IP addresses when you assign addresses for servers. For example, you need to assign network and broadcast IP addresses, the address for the gateway that the server is connected to, and the address of the individual server, all of which are publicly routable addresses. When this approach is multiplied across thousands of customers, you end up using a large number of publicly routable addresses.

  Starting with Junos OS Release 15.1X53-D30, this issue can be resolved by configuring an interface on the gateway switch with an address from the reserved IPv4 prefix for shared address space (RFC 6598) and by creating static routes that use that interface as the next hop. (The shared address space address range is 100.64.0.0/10.) You also configure the network and broadcast addresses from this range. You then configure the server with a static route that points to the RFC 6598 address used on the switch interface. With this approach, you can significantly reduce the number of routable IPv4 addresses that you use for your hosting customers.

Multicast Protocols

- **Internet Group Management Protocol (IGMP) support (QFX10008 switch)**—IGMP manages the membership of hosts and routers in multicast groups. IP hosts use IGMP to report their multicast group memberships to any immediately neighboring multicast routers. Multicast routers use IGMP to learn, for each of their attached physical networks, which groups have members.
- **IGMP snooping support (QFX10008 switch)**—IGMP snooping regulates multicast traffic in a switched network. With IGMP snooping enabled, a LAN switch monitors the IGMP transmissions between a host (a network device) and a multicast router, keeping track of the multicast groups and associated member interfaces. The switch uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces.
- **Protocol Independent Multicast (PIM) sparse mode support (QFX10008 switch)**—PIM sparse mode enables efficient routing to multicast groups with receivers that are sparsely spread over multiple networks. To configure PIM sparse mode, include the **pim** statement at the **[edit protocols]** hierarchy level.
- **PIM source-specific multicast (PIM SSM) support (QFX10008 switch)**—PIM SSM uses a subset of PIM sparse mode and 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.
- **Multicast Source Discovery Protocol (MSDP) support (QFX10008 switch)**—MSDP enables you to connect multiple domains to one another. MSDP typically runs on the same routing device as a PIM sparse mode rendezvous point. 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.
- **Rendezvous point (RP) support (QFX10008 switch)**—This feature supports multiple rendezvous points using anycast addresses (RPs sharing a single routable IP address) in either a PIM or MSDP-enabled network. To configure anycast RP, include the **anycast-pim** statement at the **[edit protocols pim rp local family inet]** hierarchy level.
- **IGMP querier support (QFX10008 switch)**—This feature 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.

Multiprotocol Label Switching (MPLS)

- **MPLS support (QFX10008 switch)**—MPLS provides both label edge router (LER) and label switch router (LSR) and provides the following capabilities:
  - Support for both MPLS major protocols, LDP and RSVP
  - IS-IS interior gateway protocol (IGP) traffic engineering
  - Class of service (CoS)
  - Object access method, including ping, traceroute, and Bidirectional Forwarding Detection (BFD)
  - Fast reroute (FRR), a component of MPLS local protection

    Both one-to-one local protection and many-to-one local protection are supported.
  - Loop free alternate (LFA) FRR
  - 6PE devices
  - Layer 3 VPNs for both IPv4 and IPv6
  - LDP tunneling over RSVP
- **Auto-bandwidth and dynamic LSP count sizing (QFX10000 switches)**—Starting with Junos OS Release 15.1X53-D30, auto-bandwidth and dynamic label-switched path (LSP) count sizing are supported on QFX10000 switches. Auto-bandwidth allows an MPLS tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel. Dynamic LSP count sizing provides an ingress router with the capability of acquiring as much network bandwidth as possible by creating parallel LSPs dynamically.

Network Management and Monitoring

- **SNMP support (QFX10008 switch)**—SNMP includes versions 1, 2, and 3 for monitoring system activity.
- **System logging (syslog) support (QFX10008 switch)**—Syslog enables you to log system messages into a local directory on the switch or to a syslog server.
- **sFlow technology support (QFX10008 switch)**—This feature provides monitoring technology for high-speed switched or routed networks. You can configure sFlow technology to monitor traffic continuously at wire speed on all interfaces simultaneously. sFlow technology also collects samples of network packets, providing you with visibility into network traffic information. You configure sFlow monitoring at the **[edit protocols sflow]** hierarchy level. sFlow operational commands include **show sflow** and **clear sflow collector statistics**.
- **Port mirroring support (QFX10008 switch)**—Port mirroring copies packets entering or exiting a port or entering a VLAN and sends the copies to a local interface for local monitoring. You can use port mirroring to send traffic to applications that analyze

traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, correlating events, and so on.

- **Virtual-router aware DHCP server/DHCP relay agent (QFX10008 switch)**—The QFX10008 switch can be configured to act as a DHCP server or DHCP relay agent for IPv4 and IPv6. If you have virtual router instances on the switch, the DHCP implementation can works with them.

Security

- **Firewall filter support (QFX10008 switch)**—You can provide rules that define whether to accept or discard packets. You can use firewall filters on interfaces, VLANs, routed VLAN interfaces (RVIs), link aggregation groups (LAGs), and loopback interfaces.
- **Policing support (QFX10008 switch)**—You can use policing to apply limits to traffic flow and to set consequences for packets that exceed those limits.
- **MAC limiting support (QFX10008 switch)**—You can protect a LAN against flooding by setting a limit on the number of MAC addresses that can be learned from the Layer 2 access interfaces on a switch.
- **MAC move limiting support (QFX10008 switch)**—You can detect MAC movement and MAC spoofing on access ports.
- **Storm control support (QFX10008 switch)**—You can enable the switch to monitor traffic levels and take a specified action when a specified traffic level—called the storm control level—is exceeded, preventing packets from proliferating and degrading service. You can configure a switch to drop broadcast and unknown unicast packets, shut down interfaces, or temporarily disable interfaces when a traffic storm occurs.

Software-Defined Networking (SDN)

- **Layer 2 VXLAN gateway and OVSDB support (QFX10008 switch)**—In a physical network, a Juniper Networks device that supports a Virtual Extensible LAN (VXLAN) can function as a hardware virtual tunnel endpoint (VTEP). In this role, the Juniper Networks device encapsulates in VXLAN packets Layer 2 Ethernet frames received from software applications that run directly on a physical server. The VXLAN packets are tunneled over a Layer 3 fabric. Upon receipt of the VXLAN packets, software VTEPs in the virtual network de-encapsulate the packets and forward the packets to virtual machines (VMs).

  In this VXLAN environment, you can also include SDN (VMware NSX or Contrail) controllers and implement the Open vSwitch Database (OVSDB) management protocol on the Juniper Networks device that functions as a hardware VTEP. The Junos OS implementation of OVSDB provides a means through which SDN controllers and Juniper Networks devices can exchange MAC addresses of entities in both physical and virtual networks. This exchange of MAC addresses enables the Juniper Networks device that functions as a hardware VTEP to forward traffic to software VTEPs in the virtual network and software VTEPs in the virtual network to forward traffic to the Juniper Networks device in the physical network.

- **Integrated routing and bridging support for EVPN-VXLAN (QFX10000 switches)**—Starting with Junos OS Release 15.1X53-D30, QFX10000 switches support

integrated routing and bridging (IRB) interfaces that route packets between Virtual Extensible LANs (VXLAN)s in an Ethernet VPN (EVPN)-VXLAN topology. This functionality is typically needed to provide Layer 3 connectivity between physical servers and virtual machines (VMs) on servers in the virtual network. Use the **set interfaces irb** command to configure an IRB interface for each VXLAN that needs to exchange packets with a host in another VXLAN, and specify a default gateway address for the hosts in the VXLAN to use by including the **virtual-gateway-address** configuration statement. Configuring this default gateway sets up a redundant default gateway for the hosts in the VXLAN.

- **EVPN control plane for VXLAN supported interfaces (QFX10000 switches)**—Traditionally, data centers have used Layer 2 technologies such as Spanning Tree Protocol (STP), multichassis link aggregation groups (MC-LAGs), or TRILL for compute and storage connectivity. As the design of data centers shifts from more traditional to scale-out, service-oriented multitenant networks, a new data center architecture allows decoupling of an underlay network from the tenant overlay network with VXLAN. By using a Layer 3 IP-based underlay coupled with a VXLAN-EVPN overlay, you can deploy larger networks than those possible with traditional Layer 2 Ethernet-based architectures. With overlays, end points (servers or virtual machines) can be placed anywhere in the network and remain connected to the same logical Layer 2 network. The benefit is that virtual topology, using both MX Series routers and QFX10000 switches, can be decoupled from the physical topology.

- **Layer 3 connectivity between data centers (QFX10002 switch)**—Starting with Junos OS Release 15.1X53-D30, you can create pure Layer 3 connections between data centers with VXLAN encapsulation by using the EVPN type-5 IP prefix routes. If you do not have VLANs that stretch between data centers, you do not need to advertise MAC and IP routes between your data centers, so a pure Layer 3 approach is feasible. EVPN pure type-5 routes decouple MAC addresses from IP addresses and advertise only IP prefixes. Include the **ip-prefix-support forwarding-mode symmetric** statement at the **[edit routing-instances *routing-instance-name* protocols evpn]** hierarchy level to configure EVPN pure type-5 routes between QFX10002 switches.

Storage

- **FCoE transit switch support (QFX10008 switch)**—You can configure a QFX10008 switch as a Fibre Channel over Ethernet (FCoE) transit switch that transports FCoE frames across the Ethernet network and supports the following data center bridging (DCB) standards: priority-based flow control (PFC) and Data Center Bridging Exchange Capability (DCBX) protocol.

System Management

- **Fabric management support (QFX10008 switch)**—You can set up and manage the fabric connections between the Packet Forwarding Engines in the switch. Fabric management collects fabric statistics, monitors hardware health, and responds to CLI queries. It also tracks when you add or remove FRUs from the switch and monitors faults in the data plane. It is enabled by default and can be monitored by using the following operational mode commands:

  - **show chassis fabric summary**—Display summary status information for the fabric.
  - **show chassis fabric fpcs fpc *fpc-slot***—Display information for Flexible PIC Concentrators (FPCs) in the fabric.
  - **show chassis fabric plane-location**—Display the fabric plane location of each Switch Interface Board (SIB).
  - **show chassis fabric sibs**—Display the state of the switch fabric link between the SIBs and the FPCs.
  - **show chassis fabric topology**—Display the input-output link topology.

- **Login authentication using RADIUS and TACACS+ (QFX10008 switch)**—You can use RADIUS and TACACS+ authentication to validate users who attempt to access the switch.
- **System utilization alarms support (QFX10008 switch)**—This feature provides system alarms to alert you of high disk usage in the /var partition on the switch. You can display these alarm messages by issuing the **show system alarms** operational mode command if the /var partition usage is higher than 75 percent. A usage level between 76 and 90 percent indicates high usage and raises a minor alarm condition, whereas a usage level over 90 percent indicates that the partition is full and raises a major alarm condition.
- **FATAL and MAJOR FAULT information support (QFX10000 switches)**—Starting with Junos OS Release 15.1X53-D30, QFX10000 switches support the ability to report FATAL and MAJOR errors in the output of the **show chassis fpc errors** command.

Traffic Management

- **Class-of-service (CoS) rewrite rules support (QFX10008 switch)**—You can use rewrite rules to set the value of the CoS bits within a packet header, so you can alter the CoS settings of incoming packets.
- **Queue shaping support (QFX10008 switch)**—You can manage excess traffic and avoid congestion on a network interface where traffic might exceed the maximum port bandwidth.
- **Ethernet PAUSE autonegotiation support (QFX10008 switch)**—You can configure symmetric flow control. To configure PAUSE, include the **flow-control** statement at the **[edit interfaces *interface-name* ether-options]** hierarchy level
- **CoS command to detect the source of RED-dropped packets (QFX10008 switch)**—If traffic on the switch is congested, you can use the **show interfaces voq *interface-name*** CLI command to identify which ingress Packet Forwarding Engine is the source of random early detection (RED)-dropped packets that are contributing to congestion. The command output displays RED drop statistics from all ingress Packet Forwarding Engines associated with the specified physical egress interface. In the VOQ architecture on the switch, egress output queues (shallow buffers) buffer data in virtual queues on ingress Packet Forwarding Engines.
- **DCB standards support (QFX10008 switch)**—The switch supports these data center bridging standards:

- Priority-based flow control (PFC) allows you to select traffic flows within a link and pause them, so that the output queues associated with the flows do not overflow and drop packets.
- Explicit congestion notification (ECN) enables end-to-end congestion notification between two endpoints on TCP/IP-based networks.

Virtual Private Networks (VPNs)

- **Layer 2 Ethernet virtual private network control plane support (QFX10000 switches)**—Ethernet VPNs (EVPNs) enable you to connect groups of dispersed customer sites to one another using Layer 2 virtual bridges. Layer 2 EVPN control planes support is supported on QFX10000 switches starting in Junos OS Release 15.1X53-D30. You configure the feature on QFX10000 switches under the global **[edit switching-options]** and **[edit protocols evpn]** hierarchy levels.

Related Documentation

- Changes in Behavior and Syntax for QFX10000 Switches on page 14
- Known Behavior for QFX10000 Switches on page 14
- Known Issues for QFX10000 Switches on page 16
- Resolved Issues for QFX10000 Switches on page 20
- Migration, Upgrade, and Downgrade Instructions for QFX10002 Switches on page 22
- Migration, Upgrade, and Downgrade Instructions for QFX10008 Switches on page 24

Changes in Behavior and Syntax for QFX10000 Switches

There are no changes in behavior of Junos OS features or changes in the syntax of Junos OS statements and commands for Junos OS Release 15.1X53 for QFX10000 switches.

Related Documentation

- New and Changed Features for QFX10000 Switches on page 3
- Known Behavior for QFX10000 Switches on page 14
- Known Issues for QFX10000 Switches on page 16
- Resolved Issues for QFX10000 Switches on page 20
- Migration, Upgrade, and Downgrade Instructions for QFX10002 Switches on page 22
- Migration, Upgrade, and Downgrade Instructions for QFX10008 Switches on page 24

Known Behavior for QFX10000 Switches

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 15.1X53-D30 for QFX10000 switches.

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

Platform and Chassis

- On QFX10002 switches, during upgrades or downgrades between Junos OS Release 15.1X53-D30 and any releases later than 15.1X53-D30 up through 15.1X53-D34, during the transient state between the issuing of the **request system software add force-host /var/tmp/** command and the issuing of the **request system reboot** command, the fan trays and power supplies (PSUs) are incorrectly reported in command output as **Absent**. This is a transient state, and the reporting of the PSUs or fan trays as **Absent** is cosmetic. After you issue the **request system reboot** command, the upgrade or downgrade finishes successfully.

VXLAN

- On QFX10000 switches with a VXLAN configuration, functions and features such as link up or link down, failover, reboot, and load balancing over VXLAN might not work properly, and traffic might drop. In some cases, traffic might not recover. As a workaround, if you are going to upgrade the switch to Junos OS Release 15.1X53-D33, configure the following commands before you run the upgrade:

  ```
  [edit]
  set routing-options forwarding-table no-indirect-next-hop
  set routing-options forwarding-table no-indirect-next-hop-change-acknowledgements
  ```

  If you have already upgraded the switch to Release 15.1X53-D33, configure the preceding two CLI commands and then reboot the switch.

  If you upgrade the switch from Release 15.1X53-D33 to any another release, remove the workaround CLI commands before you run the upgrade. PR1202595

Related Documentation

- New and Changed Features for QFX10000 Switches on page 3
- Changes in Behavior and Syntax for QFX10000 Switches on page 14
- Known Issues for QFX10000 Switches on page 16
- Resolved Issues for QFX10000 Switches on page 20
- Migration, Upgrade, and Downgrade Instructions for QFX10002 Switches on page 22
- Migration, Upgrade, and Downgrade Instructions for QFX10008 Switches on page 24

Known Issues for QFX10000 Switches

This section lists the known issues in hardware and software in Junos OS Release 15.1X53-D30 for QFX10000 switches.

High Availability (HA) and Resiliency

- On a QFX10008 switch, during a master switchover caused by a master reboot with GRES, NSR, or NSB enabled, there might be up to 8 seconds of packet loss for PING packets. PR1145296
- On a QFX10008 switch, you might see a traffic loss for a few seconds for some IPv4 and IPv6 flows during a master reboot. PR1145342
- On QFX10008 switches, if VRRP is configured to a scale of 300 sessions or more, the VRRP sessions might flap when GRES is performed, causing traffic to be dropped. PR1153784

Infrastructure and Chassis

- On QFX10002 and QFX10008 switches, STP, RSTP, MSTP, and VSTP are not supported along with QinQ on the same physical interface. PR1075230
- On QFX10002 and QFX10008 switches, modifying or rolling back a scaled configuration multiple times might cause disk space issues in the configuration partition (**/var/rundb**). The scale of the configuration depends on the configuration hierarchy. For example, configuring more than 32K firewall filters or terms and doing a modification more than four times can result in this issue. As a workaround:

  1. Navigate to the Junos OS shell by issuing **start shell** at the CLI prompt.
  2. Run mgd -i.
  3. Make a small change in the configuration and commit the configuration.

  PR1076356
- On a fully loaded QFX10008 chassis, line cards might take as many as 15 minutes to become operational after startup. PR1124967

- On QFX10002 switches, DDOS violations are not reported in the system log. As a workaround, issue the **show ddos-protection protocols** command. PR1127874
- On QFX10002 switches, DDOS rate limiting might not work correctly for RSVP packets with router-alert options. PR1130577
- On QFX10008 switches, if there are unexpected fabric link errors, traffic might be impacted. In such cases, gracefully offline the SIB. PR1134085
- On QFX10008 switches, BFD sessions might flap on a CLI GRES or master reboot if the BFD timer is configured for 300 ms.PR1138768
- On a QFX10008 switch with scaled configurations, interface statistics might not be updated in a timely fashion and might include inaccurate values when the CPU is updating forwarding tables during an FPC transition. Statistics are accurate when CPU utilization returns to normal. PR1141142
- On a QFX10008 switch, you might see a traffic loss of 2 to 6 seconds if node-link protection is configured. As a workaround, issue **set protocols mpls optimize-switchover-delay 60** in the configuration to minimize traffic loss. PR1148293
- On QFX10008 switches, if DHCP relay is configured after trace options are enabled for DHCP, then the relay agent might not process DHCP packets. As a workaround, remove the trace option configuration for DHCP prior to configuring DHCP relay. PR1154990
- On QFX10008 switches, BFD sessions might go down and then come back up after a nonanchor line card is restarted and if the sessions are configured on a LAG with members spread across line cards. PR1155018

Interfaces

- On a QFX10002 switch, an ICL interface might be enabled and then disabled with running traffic. PR1080327
- On a QFX10002 or a QFX10008 switch, when an MC-AE interface is disabled and then enabled, there might be Layer 3 over IRB traffic loss for approximately 20 seconds. PR1130010, PR1092742
- On QFX10008 switches, when a line card comes online after being rebooted, BFD sessions running on aggregated Ethernet bundles might revert to the initializing state. PR1148221

Layer 3 Protocols

- The IS-IS protocol is an interior gateway protocol (IGP) that uses link-state information to make routing decisions. On QFX10008 switches, IS-IS v4 and v6 VRF sessions can flap and cause a traffic drop during either a Routing Engine switchover or a master reboot. As a workaround, increase the hello timer to 30 seconds and the hold timer to 90 seconds or configure IS-IS VRF sessions as a P2P network. PR1143260
- On QFX10008 switches, when you disable one Layer 3 ECMP member link, IPv6 traffic loss might occur for more than 10 seconds. PR1144847

- When a QFX10002 switch is used as an EVPN VXLAN Layer 3 gateway, ARP requests for VRF leaked routes in a static route over IRB might not be resolved. PR1147176

MPLS

- On a QFX10008 switch, if maximum ECMP (16) and BGP multipath are configured, the switch might install 32 paths instead of 16 paths. PR1141454
- On QFX10008 switches, when MPLS automatic bandwidth allocation is configured for an LSP, disabling the configuration might generate an RPD core file. PR1152449

Multicast Protocols

- On a QFX10008 switch, a line card might drop multicast traffic if another line card is restarted while the traffic is in transit. PR1134447
- If there is a failover from one Routing Engine to another on a QFX10008 switch, IPv6 traffic might be dropped. This loss can occur regardless of whether the traffic is for the default routing instance or a virtual routing instance. PR1134476
- On a QFX10008 switch with MC-LAG configured, when a PIM DR node is rebooted and comes back up as a DR, a multicast route add or delete takes a long time, causing traffic loss for about 10 seconds. PR1138561
- On QFX10008 switches, multicast traffic drops might occur on multiple ports when one of the ports flaps or comes online. This behavior is seen with IGMP snooping and multicast port replication. PR1151829

Network Management and Monitoring

- If a QFX10008 switch is fully populated with line cards and all the interfaces are configured, SNMP timeouts can occur if the switch is simultaneously polled by multiple network management stations. PR1147934

Routing Policy and Firewall Filters

- On QFX10002 switches, when a firewall term is configured with destination-port without any Layer 3 fields such as src and dest IP, then the term processes pure Layer 3 packets such as RSVP and OSPF. As a workaround, when you configure a firewall term with destination-port, use the term with appropriate IP protocols. PR1147694

Software Installation and Upgrade

- On QFX10002 switches, rolling back the software by issuing the **request system software rollback** command is not supported. PR1070892

Software-Defined Networking

- On QFX10002 switches, the collection of statistics for OVSDB-managed interfaces is not supported. As a result, even if an OVSDB-managed interface is up and running, the **show ovsdb statistics interface** command output for this interface displays 0. PR1090363
- In a VXLAN-OVSDB topology with Contrail controllers, broadcast, unknown unicast, and multicast (BUM) traffic might not be forwarded to a ToR services node (TSN) if the traffic is handled by an integrated routing and bridging (IRB) interface configured on a QFX10002 switch. Note that the physical interface on which the IRB interface is configured is part of an aggregated Ethernet bundle. PR1133126
- In a VXLAN-OVSDB topology in which a QFX10002 switch is deployed as a Layer 2 gateway, adding or deleting a VXLAN might cause the switch's CPU to be excessively consumed. As a workaround, either issue the **traceoptions** configuration statement at the **[edit protocols ovsdb]** hierarchy level or restart the OVSDB server. PR1151150
- On QFX10002 switches, EVPN Type 5 data packets that are larger than the outgoing physical interface's MTU are sent without fragmentation. PR1156266

Related Documentation

- New and Changed Features for QFX10000 Switches on page 3
- Changes in Behavior and Syntax for QFX10000 Switches on page 14
- Known Behavior for QFX10000 Switches on page 14
- Resolved Issues for QFX10000 Switches on page 20
- Migration, Upgrade, and Downgrade Instructions for QFX10002 Switches on page 22
- Migration, Upgrade, and Downgrade Instructions for QFX10008 Switches on page 24

Resolved Issues for QFX10000 Switches

This section lists the issues fixed in the Junos OS 15.1X53 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 15.1X53-D34

Firewall Filters

- On QFX10000 switches, when a filter is applied to an integrated routing and bridging (IRB) interface, if you change the filter (for example, you add, delete, or modify a term), then Layer 2 packets switched within the VLAN associated with the IRB might be impacted by the IRB filter. As a workaround, unbind the IRB filter and then rebind it. PR1201825

Infrastructure and Chassis

- On QFX10008 switches, FPCs might randomly reboot and traffic might be impacted during the reboot. The TCP connection between the Routing Engine and the FPC has timed out, and the FPC does not reconnect until the Routing Engine restores the TCP connection after 15 minutes of timeout. PR1195188

Interfaces

- On QFX10002 switches, the JNP-QSFP-100G-LR4 optical transceiver might continue to send laser output after the port has been disabled. PR1192489

Resolved Issues: Release 15.1X53-D33

- High Availability (HA) and Resiliency
- Interfaces and Chassis
- Layer 3 Unicast Forwarding
- MPLS
- Network Management and Monitoring

High Availability (HA) and Resiliency

- On QFX10000 switches, if you configure adaptive load balancing (ALB) on a VLAN-based Layer 3 LAG interface, the commit fails. A commit error is displayed. PR1176139

Interfaces and Chassis

- On a QFX10002 switch, if an aggregated Ethernet interface has only one member, and you perform an online insertion and removal on the transceiver of the physical interface, traffic might be dropped. As a workaround, reconfigure the aggregated Ethernet interface. PR1168984
- On a QFX10008 switch, a commit might fail because the MGD process requires high CPU utilization on the backup Routing Engine. PR1176407
- On QFX10000 switches, an ARP reply with the switch as its destination is instead flooded to the entire VLAN. PR1179024
- QFX10000 switches perform subnet flooding when routed transit unicast traffic received on IRB interfaces does not have an external route present to a destination address. PR1179605

Layer 3 Unicast Forwarding

- On QFX10000 switches, strict mode for unicast reverse path forwarding (URPF) does not work with the default route. PR1157702

MPLS

- On QFX10000 switches, the incoming MPLS-labeled packet on the provider edge (PE) switch is dropped when the destination host ARP entry is not in the customer edge (CE) VPN routing and forwarding (VRF) table. PR1180469

Network Management and Monitoring

- On QFX10000 switches, the output for **run show sflow collector** shows the wrong “No of Samples” count. PR1174894

Resolved Issues: Release 15.1X53-D32

- Interfaces and Chassis
- Network Management and Monitoring

Interfaces and Chassis

- If you commit a huge configuration on a QFX10000 switch, in rare cases some ports are not activated. PR1160220
- On a QFX10008 switch, a 100-Gigabit optical interface might not activate if the interface is disabled and enabled several times. PR1160236

- On a QFX10002 switch, the major alarm LED may light even though there are no alarms. PR1160248

Network Management and Monitoring

- On QFX10000 switches, when sFlow is configured and traffic is routed out of a link aggregation interface, the SNMP index of the output port might not be displayed, which means that the traffic flows cannot be monitored. PR1161197

Related Documentation

- New and Changed Features for QFX10000 Switches on page 3
- Changes in Behavior and Syntax for QFX10000 Switches on page 14
- Known Behavior for QFX10000 Switches on page 14
- Known Issues for QFX10000 Switches on page 16
- Migration, Upgrade, and Downgrade Instructions for QFX10002 Switches on page 22
- Migration, Upgrade, and Downgrade Instructions for QFX10008 Switches on page 24

Migration, Upgrade, and Downgrade Instructions for QFX10002 Switches

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS.

- Downloading Software Files with a Browser on page 22
- Backing Up the Current Configuration Files on page 23
- Installing the Software on page 23

Downloading Software Files with a Browser

To download the software package from the Juniper Networks Support website, go to http://www.juniper.net/support/ .

NOTE: To access the download site, you must have a service contract with Juniper Networks and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks website https://www.juniper.net/registration/Register.jsp .

This procedure shows you how to upgrade software on a QFX10002 switch.

1. Using a Web browser, navigate to http://www.juniper.net/support .
2. Click **Download Software**.
3. In the By Technology box, click **Switching | QFX Series | QFX10002**.
4. In the QFX Series section, click the name of the platform for which you want to download software.
5. Click the **Software** tab and select the install package from the Install Package box.

A login screen appears.

6. Enter your name and password and press **Enter**.
7. Read the End User License Agreement, click the **I agree** radio button, and then click **Proceed**.
8. Save the **jinstall-qfx-10-f-flex-<*version*>-domestic-signed.tgz** file on your computer.
9. Open or save the installation package either to the local system in the **var/tmp** directory or to a remote location. If you are saving the installation package to a remote system, make sure that you can access it using HTTP, TFTP, FTP, or scp.

Backing Up the Current Configuration Files

Before you install the new installation package, we strongly recommend that you back up your current configuration files, because the upgrade process removes all of the stored files on the switch.

To back up your current configuration files:

```
user@switch# save filename
```

Executing this command saves a copy of your configuration files to a remote location such as an external USB device.

Installing the Software

NOTE: On the switch, use the force-host option to force-install the latest version of the Host OS. However, by default, if the Host OS version is different from the one that is already installed on the switch, the latest version is installed without using the force-host option.

If the installation package resides locally on the switch, execute the **request system software add <*pathname*><*source*> reboot** command.

For example:

```
user@switch> request system software add
/var/tmp/jinstall-qfx-10-f-flex-15.1X53-D30-domestic.tgz reboot
```

If the Install Package resides remotely from the switch, execute the **request system software add <*pathname*><*source*> reboot** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-qfx-10-f-flex-15.1X53-D30-domestic.tgz reboot
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

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

Related Documentation

- New and Changed Features for QFX10000 Switches on page 3
- Changes in Behavior and Syntax for QFX10000 Switches on page 14

Migration, Upgrade, and Downgrade Instructions for QFX10008 Switches

This section contains the procedure to upgrade Junos OS, and the upgrade and downgrade policies for Junos OS.

Downloading Software Files with a Browser

To download the software package from the Juniper Networks Support website, go to http://www.juniper.net/support/ .

NOTE: To access the download site, you must have a service contract with Juniper Networks and an access account. If you need help obtaining an account, complete the registration form at the Juniper Networks website https://www.juniper.net/registration/Register.jsp .

This procedure shows you how to upgrade software on a QFX10008 switch.

1. Using a Web browser, navigate to http://www.juniper.net/support .
2. Click **Download Software**.
3. In the By Technology box, click **Switching** | **QFX Series** | **QFX10008**.
4. In the QFX Series section, click the name of the platform for which you want to download software.
5. Click the **Software** tab and select the install package from the Install Package box.

   A login screen appears.
6. Enter your name and password and press **Enter**.
7. Read the End User License Agreement, click the **I agree** radio button, and then click **Proceed**.
8. Save the **jinstall-qfx-10-m-flex-<*version*>-secure-domestic-signed.tgz** file on your computer.
9. Open or save the installation package either to the local system in the **var/tmp** directory or to a remote location. If you are saving the installation package to a remote system, make sure that you can access it using HTTP, TFTP, FTP, or scp.

Backing Up the Current Configuration Files

Before you install the new installation package, we strongly recommend that you back up your current configuration files, because the upgrade process removes all of the stored files on the switch.

To back up your current configuration files:

```
user@switch# save filename
```

Executing this command saves a copy of your configuration files to a remote location such as an external USB device.

Installing the Software

NOTE: On the switch, use the **force-host** option to force-install the latest version of the Host OS. However, by default, if the Host OS version is different from the one that is already installed on the switch, the latest version is installed without using the **force-host** option.

The switch contains two routing engines, so you will need to install the software on each routing engine (re0 and re1).

If the installation package resides locally on the switch, execute the **request system software add *<pathname><source>* (re0 | re1)** command.

To install the software on re0:

```
user@switch> request system software add
/var/tmp/jinstall-qfx-10-m-flex-15.1X53-D30-secure-domestic-signed.tgz re0
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* re0** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-qfx-10-m-flex-15.1X53-D30-secure-domestic-signed.tgz re0
```

To install the software on re1:

```
user@switch> request system software add
/var/tmp/jinstall-qfx-10-m-flex-15.1X53-D30-secure-domestic-signed.tgz re1
```

If the Install Package resides remotely from the switch, execute the **request system software add *<pathname><source>* re1** command.

For example:

```
user@switch> request system software add
ftp://ftpserver/directory/jinstall-qfx-10-m-flex-15.1X53-D30-secure-domestic-signed.tgz re1
```

Reboot both routing engines.

For example:

```
user@switch> request system reboot both-routing-engines
```

After the reboot has finished, verify that the new version of software has been properly installed by executing the **show version** command.

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

Related Documentation

- New and Changed Features for QFX10000 Switches on page 3
- Changes in Behavior and Syntax for QFX10000 Switches on page 14
- Known Behavior for QFX10000 Switches on page 14
- Known Issues for QFX10000 Switches on page 16
- Resolved Issues for QFX10000 Switches on page 20

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

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.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

4 October 2016—Revision 2, Junos OS for QFX10000 switches, Release 15.1X53-D32—update to Known Behavior for QFX Series

1 September 2016—Revision 1, Junos OS for QFX10000 switches, Release 15.1X53-D34.