Release Notes: Junos® OS 15.1X53-D40 for NFX250 Network Services Platform

April 8, 2016

These release notes accompany Junos OS Release 15.1X53-D40 for NFX250 Network Services Platform.

Contents

Release Notes: Junos® Release Notes for NFX 250 Network Services Platform

These release notes accompany Junos OS Release 15.1X53-D40 for NFX250. They describe new and changed features, limitations, and known problems in the hardware and software. You can also find these release notes on the Juniper Networks Junos OS Documentation web page, located at www.juniper.net/techpubs

New and Changed Features for NFX250 Network Services Platform

This section describes the new features of the NFX250 platform, and enhancements to existing features in Junos OS Release 15.1X53-D40 for NFX250.

Hardware

- **NFX250 Platform**—The NFX250 devices constitute Juniper Network's secure, automated, software-driven customer premises equipment (CPE) devices that deliver virtualized network and security services on demand. Leveraging Network Functions Virtualization (NFV) and built on the Juniper Cloud CPE solution, NFX250 enables service providers to deploy and service chain multiple, secure, high-performance virtualized network functions (VNFs) in a single device.

  NFX250 devices are available in two compact 1-U models that provide VNF and Packet Forwarding Engine (PFE) capacity, and a rich set of Layer 2 and Layer 3 features. The performance of the control plane running on NFX250 devices is enhanced by the 1.9 GHz, 6-core Intel CPU. The NFX250-S1 has 16 GB of memory and 100 GB of solid-state drive (SSD) storage and the NFX250-S2 has 32 GB of memory and 400 GB of SSD storage.

  NFX250 has 10 1-gigabit LAN ports, two SFP WAN ports, two SFP+ WAN ports, and one management port. The NFX250 is shipped with with built-in fans and power supplies.

- **Transceivers**—NFX250 supports the following optics:

  - 10-gigabit SFP+ transceivers: EX-SFP-10GE-USR, EX-SFP-10GE-SR, EX-SFP-10GE-LR, EX-SFP-10GE-ER, EX-SFP-10GE-ZR
  - 1G-gigabit SFP transceivers: EX-SFP-1GE-SX, EX-SFP-1GE-SX-ET, EX-SFP-1GE-LX, EX-SFP-1GE-LH, EX-SFP-1GE-T, EX-SFP-1GE-LX40K, EX-SFP-GE10KT13R14,

EX-SFP-GE10KT14R13, EX-SFP-GE10KT13R15, EX-SFP-GE10KT15R13, EX-SFP-GE40KT13R15, EX-SFP-GE40KT15R13, EX-SFP-GE80KCW1470, EX-SFP-GE80KCW1490, EX-SFP-GE80KCW1510, EX-SFP-GE80KCW1530, EX-SFP-GE80KCW1550, EX-SFP-GE80KCW1570, EX-SFP-GE80KCW1590, EX-SFP-GE80KCW1610

- **Direct Attach Copper (DAC) Cables**—NFX250 supports the following DAC cables:
  - EX-SFP-10GE-DAC-1M
  - EX-SFP-10GE-DAC-3M
  - EX-SFP-10GE-DAC-5M

Juniper Device Manager

The Juniper Device Manager (JDM) is a low-footprint Linux container that provides these functions:

- Virtual machine (VM) life cycle management
- Device management and isolation of host OS from user installations
- NIC , single-root I/O virtualization (SR-IOV), and virtual input/output (VirtIO) interface provisioning
- Support for the Network Service Orchestrator module to connect to Network Service Activator
- Inventory and resource management
- Internal network and image management
- Service chaining—provides building blocks such as virtual interfaces and bridges for users to implement service chaining polices
- Virtual console access to VNFs including vSRX and vjunos

Network Service Orchestrator

- Network Service Orchestrator is a client included in the base software of the NFX250, and connects to the Network Service Activator deployed on a cloud or server. The Network Service Activator application intelligently automates service life cycle management of managed VPN networks, in-region secured Internet connections, and out-of-region IPsec connections on NFX250. This application enables the booting and configuration of the NFX250 device when it first powered on.

vSRX

- vSRX offers the same capabilities as Juniper Networks SRX Series Services Gateways in a virtual form factor, providing perimeter security, IPsec connectivity, and filtering for malicious traffic without sacrificing reliability, visibility, and policy control. This virtual security and routing appliance ensures reliability for each application.

NOTE: **By default, vSRX version 15.1X49-D40 is pre-loaded on NFX250 Network Services platform. You can upgrade it whenever a newer if vSRX is available.**

Junos Control Plane

Junos Control Plane (JCP) is the Junos VM running on the hypervisor. By default, JCP runs as vjunos0 on NFX250. You can use JCP to configure the network ports of the NFX250 device. You can log in to JCP from JDM by using the SSH service and CLI, which is similar to the Junos OS CLI. The JCP supports the following features in Junos OS release 15.1X53-D40:

- **Link aggregation**—Link aggregation enables you to use multiple network cables and ports in parallel to increase link speed and improve redundancy.
- **Support for Layer 3 logical interfaces**—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 an NFX250 device to a Layer 2 switch. Only one physical connection is required between the NFX250 device and the switch.
- **VLAN support**—VLANs enable you to divide one physical broadcast domain into multiple virtual domains.
- **Link Layer Discovery Protocol (LLDP) support**—LLDP enables a switch to advertise its identity and capabilities on a LAN, and to receive information about other network devices.
- **Q-in-Q tunneling support**—This feature enables service providers on Ethernet access networks to extend a Layer 2 Ethernet connection between two customer sites. 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), and VLAN Spanning Tree Protocol (VSTP) support**—These protocols enable a switch to advertise its identity and capabilities on a LAN and receive information about other network devices.
- **OSPF support**—The IPv4 OSPF protocol is an interior gateway protocol (IGP) for routing traffic within an autonomous system (AS). NFX devices support OSPFv1 and OSPFv2. You can configure OSPF at the **[edit protocols ospf]** hierarchy level.
- **Bidirectional Forwarding Detection (BFD) support for static routes and the OSPF and RIP protocols**—BFD uses control packets and shorter detection time limits to rapidly detect failures in a network. Hello packets are sent at a specified, regular interval by routing devices. A neighbor failure is detected when a routing device stops receiving a reply after a specified interval.
- **Virtual Router Redundancy Protocol (VRRP) support**—VRRP enables you to provide alternative gateways for end hosts that are configured with static default routes. You can implement VRRP to provide a highly available path to a gateway without needing to configure dynamic routing or router discovery protocols on end hosts.
- **Internet Group Management Protocol (IGMP) support**—IGMP manages the membership of hosts and routers in multicast groups. IP hosts use IGMP to report their multicast group memberships to multicast routers that are their immediate neighbors . Multicast routers use IGMP to learn, for each of their attached physical networks, which groups have members.
- **IGMP Snooping support**—IGMP snooping regulates multicast traffic in a switched network. With IGMP snooping enabled, a LAN switch monitors the IGMP transmissions between a host (a network device) and a multicast router, keeping track of the multicast groups and associated member interfaces. The switch uses that information to make intelligent multicast-forwarding decisions and forward traffic to the intended destination interfaces.
- **Protocol Independent Multicast (PIM) sparse mode support**—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.
- **SNMP support**—SNMP includes versions 1, 2, and 3 for monitoring system activity.
- **System logging (syslog) support**—Syslog enables you to log system messages into a local directory on the switch or to a system log server.
- **Port mirroring support**—Port mirroring copies packets entering or exiting a port or entering a VLAN and sends the copies to a local interface for local monitoring. You can use port mirroring to send traffic to applications that analyze traffic for purposes such as monitoring compliance, enforcing policies, detecting intrusions, monitoring and predicting traffic patterns, and correlating events.
- **Firewall filter support**—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**—You can use policing to apply limits to traffic flow and to set consequences for packets that exceed those limits.
- **Storm control support**—You can enable the switch to monitor traffic levels and take a specified action when a specified traffic level—called the storm control level—is exceeded, preventing packets from proliferating and degrading service. You can configure a switch to drop broadcast and unknown unicast packets, shut down interfaces, or temporarily disable interfaces when a traffic storm occurs.
- **Class of service (CoS)**—When a packet traverses a switch, the switch provides the appropriate level of service to the packet using either default class-of-service(CoS) settings or the CoS settings that you configure. On ingress ports, the switch classifies packets into appropriate forwarding classes and assigns a loss priority to the packets. On egress ports, the switch applies packet scheduling and any rewrite rules to re-mark packets.

NOTE: **WRED profiles are not supported for this release.**

- **Class-of-service (CoS) rewrite rules and classifier support**—You can use rewrite rules to set the value of the CoS bits within a packet header, so you can alter the CoS settings of incoming packets. Packet classification maps incoming packets to a particular class-of-service (CoS) servicing level. You can use classifiers to map packets to a forwarding class and a loss priority and to assign packets to output queues based on the forwarding class.
- **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.

Related Documentation

- Known Behavior for NFX250 Network Services Platform on page 9
- Known Issues in NFX250 Network Services Platform on page 9
- Changes in Behavior and Syntax for NFX250 Network Services Platform on page 6

Changes in Behavior and Syntax for NFX250 Network Services Platform

This section lists the changes in behavior of Junos OS features and changes in the syntax of Junos OS statements and commands from Junos OS Release 15.1X53-D40 for NFX250.

- Firewall Filter Support on page 6

Firewall Filter Support

- Layer 2 filters with L3 or L4 match conditions applied at the egress interface is not supported.
- **Match Condition Support**—The table lists the match conditions supported on NFX250:

Table 1: Match Condition Support

Firewall family ethernet-switching				
Match Condition	IPACL	IVACL	EPACL	EVACL
arp-type	Yes	Yes	Yes	Yes
destination-mac-address	Yes	Yes	Yes	Yes
destination-port	Yes	Yes	No	No
destination-port-except	Yes	Yes	No	No
destination-prefix-list	Yes	Yes	Yes	Yes
dscp	Yes	Yes	No	No
dscp-except	Yes	Yes	No	No
ether-type	Yes	Yes	Yes	Yes
ether-type-except	Yes	Yes	Yes	Yes
fragment-flags	Yes	Yes	No	No
icmp-code	Yes	Yes	No	No
icmp-code-except	Yes	Yes	No	No
icmp-type	Yes	Yes	No	No
icmp-type-except	Yes	Yes	No	No
Interface	Yes	Yes	Yes	Yes
ip-destination-address	Yes	Yes	No	No
ip-precedence	Yes	Yes	No	No
ip-precedence-except	Yes	Yes	No	No
ip-protocol	Yes	Yes	No	No
ip-protocol-except	Yes	Yes	No	No
ip-source-address	Yes	Yes	No	No
ip-version	NA-	NA	NA	NA

Table 1: Match Condition Support *(continued)*

Firewall family ethernet-switching				
Match Condition	IPACL	IVACL	EPACL	EVACL
is-fragment	Yes	Yes	No	No
l2-encap-type	Yes	Yes	Yes	Yes
learn-vlan-1p-priority	Yes	Yes	Yes	Yes
learn-vlan-1p-priority-except	Yes	Yes	Yes	Yes
learn-vlan-id	Yes	Yes	Yes	Yes
learn-vlan-id-except	Yes	Yes	Yes	Yes
Port	Yes	Yes	No	No
port-except	Yes	Yes	No	No
source-mac-address	Yes	Yes	Yes	Yes
source-port	Yes	Yes	No	No
source-port-except	Yes	Yes	No	No
source-prefix-list	Yes	Yes	Yes	Yes
tcp-established	Yes	Yes	No	No
tcp-flags	Yes	Yes	No	No
tcp-initial	Yes	Yes	No	No
user-vlan-1p-priority	Yes	Yes	Yes	Yes
user-vlan-1p-priority-except	Yes	Yes	Yes	Yes
user-vlan-id	Yes	Yes	Yes	Yes
user-vlan-id-except	Yes	Yes	Yes	Yes

NOTE: Firewall family inet does not have any restrictions mentioned in table above.

- The Firewall action **reject** configured at the egress is not supported for both inet and inet6 filter.
- Firewall action modifiers log and syslog applied at the egress interface is not supported for PACL, VACL, and RACL/RACLv6.
- You cannot configure all three ACL parameters (PACL, + VACL, + RACL) configured at the same time, due to limited TCAM space.

Related Documentation

- New and Changed Features for NFX250 Network Services Platform on page 2
- Known Behavior for NFX250 Network Services Platform on page 9
- Known Issues in NFX250 Network Services Platform on page 9

Known Behavior for NFX250 Network Services Platform

This section lists known behavior, system maximums, and limitations in hardware and software in Junos OS Release 15X53-D40 for NFX250.

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

- JDM

JDM

- JDM shell configurations of interfaces override JDM CLI configurations. As a workaround, use the JDM CLI to configure interfaces. [PR1155749]
- SR-IOV interfaces do not support more than 64 VLANs on NFX250. [PR1156348]
- The **set interfaces** CLI command is not supported on JDM. As a workaround, you can use the **set interface** command. [PR1156957]

Related Documentation

- New and Changed Features for NFX250 Network Services Platform on page 2
- Known Issues in NFX250 Network Services Platform on page 9
- Changes in Behavior and Syntax for NFX250 Network Services Platform on page 6

Known Issues in NFX250 Network Services Platform

This section lists the known issues in hardware and software in Junos OS Release 15X53-D40 for NFX250.

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

- JDM
- JCP on page 11

JDM

- When a Virtual Function (VF) interface is hotplugged into a VM, the MAC address that is derived is not from the JDM MAC pool. [PR1145809]
- Rebooting NFX250 from the JDM shell is not supported. Use the **request system reboot** command from the JDM CLI. [PR1146229]
- You might not be able to specify a definite interval for the **request system reboot** command. By default, the device waits for 30 seconds before rebooting. [PR1150400]
- There might be no checks when you configure the IP address on different logical units of interfaces. The commit will go through, and will be displayed in the configuration. [PR1150512]
- When configuring SR-IOV interfaces, there might not be any checks when a configuration is committed to JDM in the following scenarios:
  - When a VF interface is attached to a VM and the VM instance is removed, the stray configuration for all the interfaces attached to the VM still remains without any warning or error being displayed.
  - A warning or error message might not be displayed when VF interfaces, that are being used by other VNFs, are reattached.
  - A warning or error message is not displayed when a VF is attached to a non-existent VNF.
  - A message is not displayed when a JDM with attached VFs is reused.
  - VFs are assigned MAC addresses by default, and there is no option to specify the address using the CLI.

  [PR1152989]
- Host forwarding across VF interfaces assigned to different SR-IOV NICs is not supported. [PR1154345]
- The following commands are not supported:
  - **clear system reboot** and **clear system commit**
  - **request system reboot at** and **request system reboot in**. The **request system reboot** command is supported.
  - **restart gracefully**, **restart immediately**, **restart init**, and **restart soft**

  [PR1154819]
- On JDM, SSH connectivity using **host-os** and **jcp** options might not work. [PR1155475]
- User defined login class is not supported. The configuration commit might be successful, but login attempts will not work. [PR1155965]
- While spawning a container, VF interfaces cannot be used in the VNF descriptor XML file. Only virtIO interfaces are supported for containers. [PR1156897]
- When you use the **netconf** command to display system information details such as model and OS, the system OS is displayed as QFX. [PR1160055]

- **ping** command when initiated with **record route** option on virtIO interfaces, returns no results. [PR1162659]
- BIOS upgrade with jloader is not supported. As a workaround, upgrade from host using the **rpm** file. [PR1165759]
- The **show host** command to resolve hosts on JDM is not supported. [PR1167964]
- Clients that are connected via the front panel ports are assigned the default gateway 10.10.10.254 by Network Service Activator. [PR1168284]
- When there are insufficient MAC pool resources available on JDM for container creation, the configuration commit for the container will fail. Subsequent to the commit failure, even if necessary MAC pool resources become available, the container configuration commit might not succeed. [PR1168595]
- Ubuntu package does not successfully install on the JDM container. As a workaround, install the package **passwd** by using the **sudo apt-get install passwd** command, which enables the **useradd** command again. [PR1168680]
- With hostname configured on JDM, after NFX250 reboots, **host.named** core file is generated on the host for NFX250 devices. [PR1169490]
- The CLI to configure the time zone is not functional. [PR1169675]
- NETCONF configuration for port, and limiting number of connections and rate for sessions are not supported. [PR1169898]
- SNMP traps are not supported on JDM. [PR1173216]
- When you configure a static route on JDM, there might not be an explicit check to validate the IP address. [PR1173039]

JCP

Infrastructure

- The Alarm LED might not reflect the link state of the management port. [PR1146307]
- You cannot configure a transmit rate of **0** for class-of-service schedulers. [PR1158085]
- If a cable is not connected to the front panel RJ-45 ports, the status led will blink. [PR1168054]
- Configuring DSCP and DSCPv6 classifiers together on a Layer 2 interface is not supported. [PR1169529]
- SFP-T transceivers are not supported. [PR1151575, PR1166808, PR1168203]
- Class-of-service loss priority set to **medium-high** is not supported. Therefore, tricolor configuration is not supported. [PR1166422, PR1168393]
- When the option **accept-source-mac mac-address** is configured on an interface and then deleted, no additional MAC's will be learnt on the interface. Only the MAC's which were earlier configured will be available. [PR1168197]
- When LLDP is configured on vjunos0 on an NFX250 Network Services platform, the system name TLV(5) might not be advertised. [PR1169479]

Related Documentation

- New and Changed Features for NFX250 Network Services Platform on page 2
- Known Behavior for NFX250 Network Services Platform on page 9
- Changes in Behavior and Syntax for NFX250 Network Services Platform on page 6