

Release Notes: Junos[®] OS Release 16.1X65D35 for PTX1000 Packet Transport Routers

Release 16.1X65D35
Revision 1

Contents

Junos OS Release Notes for PTX1000 Packet Transport Routers	3
New and Changed Features	3
Hardware	4
Interfaces and Chassis	4
Junos OS XML API and Scripting	6
Layer 2 Features	6
Layer 3 Features	6
Layer 3 Logical Interfaces	7
Multicast Protocols	7
MPLS	8
VPN	10
Network Management and Monitoring	10
Security	10
System Management	11
Traffic Management	11
Services	12
Upgrade Instructions for PTX1000 BIOS	12
Introduction	12
Software and BIOS Image Locations	12
Determining your software upgrade needs	13
BIOS Upgrade Process for PTX1000 with Junos 15.1X Software Installed . . .	13
BIOS Upgrade Process for PTX1000 with Junos 16.1X Software Installed . . .	13
Upgrading the BIOS	14
Upgrade Back to Junos 16.1 with the Upgraded BIOS	15
Upgrade Instructions for PTX1000 B1 Software	16
Introduction	16
Step 1: For all testers - Create the bootable USB device	16
For PTX1000 units which have 15.1X software	16

For PTX1000 units which have 16.1X software	17
Known Behavior	18
General Routing	18
Known Issues	18
General Routing	18
Interfaces and Chassis	19
Product Compatibility	19
Hardware Compatibility	19
Documentation Feedback	19
Requesting Technical Support	19
Revision History	19

Junos OS Release Notes for PTX1000 Packet Transport Routers

These release notes accompany Junos OS Release 16.1X65D35 for Juniper Networks PTX1000 Packet Transport Routers. They describe new and changed features, limitations, and known and resolved problems in the hardware and software.

These release notes along with [Feature Explorer](#) can be used to know the list of features supported on PTX1000 routers. For detailed information about how to use the features, refer the feature guides.

New and Changed Features

This section describes the new features and enhancements to existing features in Junos OS Release 16.1X65D35 for PTX1000 routers.

- [Hardware on page 4](#)
- [Interfaces and Chassis on page 4](#)
- [Junos OS XML API and Scripting on page 6](#)
- [Layer 2 Features on page 6](#)
- [Layer 3 Features on page 6](#)
- [Layer 3 Logical Interfaces on page 7](#)
- [Multicast Protocols on page 7](#)
- [MPLS on page 8](#)
- [VPN on page 10](#)
- [Network Management and Monitoring on page 10](#)
- [Security on page 10](#)
- [System Management on page 11](#)
- [Traffic Management on page 11](#)
- [Services on page 12](#)

Hardware

- **PTX1000 router**—The Juniper Networks PTX1000 Packet Transport Router is a fixed-configuration router that supports 10-Gbps, 40-Gbps, and 100-Gbps port speeds in a compact 2U form factor, enabling service providers to organically distribute peering points throughout the network. All of the 72 network ports on the port panel support quad small form-factor pluggable plus (QSFP+) transceivers. By default, each port is configured as four 10-Gigabit Ethernet interfaces, for a maximum of 288 10-Gigabit Ethernet ports. You can also configure the 72 ports as 40-Gigabit Ethernet interfaces, for a maximum of 72 40-Gigabit Ethernet ports. And 24 of the 72 network ports can be configured as 100-Gigabit Ethernet interfaces that use QSFP28 transceivers.

Interfaces and Chassis

- **Support for channelizing the 40-Gigabit Ethernet ports on PTX1000**—PTX1000 Packet Transport Router supports 10-Gbps, 40-Gbps, and 100-Gbps port speeds, enabling service providers to organically distribute peering points throughout the network. The default port speed on all 72 network ports is 40 Gbps. However, you can channelize four 10-Gigabit Ethernet interfaces from the 40-Gigabit Ethernet interfaces. By default, the 40-Gigabit Ethernet interfaces are named **et-fpc/pic/port**. The names of the channelized 10-Gigabit Ethernet interfaces appear in the format: **et-fpc/pic/port:channel**, where **channel** is a value from 0 through 3.

To configure a port speed of 40-Gbps or 10-Gbps, use the **set chassis fpc slot pic pic-slot port 0..71 channel-speed (10g|40g)** command.

You can also configure 24 out of the 72 ports to operate at 100-Gbps speed.

- **Support for configuring multiple port speeds on PTX1000**—PTX1000 Packet Transport Router supports 10-Gbps, 40-Gbps, and 100-Gbps port speeds, enabling service providers to organically distribute peering points throughout the network. To configure the port speed, use the **speed [10G | 40G | 100G]** statement at the **[edit chassis fpc slot-number pic pic-number port port-number]** hierarchy level. The default port speed is 10G.
- **Support for configuring local loopback on PTX1000**—To enable the local loopback, use the **loopback local** configuration statement on PTX1000 interfaces. The PTX1000 supports only local loopback, not remote loopback. Configure the statement at the **[edit interfaces interface-name gigether-options]** hierarchy level.
- **Support for Packet forwarding features (PTX1000)**—The PTX1000 Packet Transport Router supports the following key packet forwarding features:
 - Basic Layer 2 features and protocols
 - Class-of-service (CoS)
 - Firewall filters and policers
 - Hash Enhancement
 - Large scaling IPv4/v6 Forwarding information base(FIB)
 - Layer 3 VPNs

- MPLS
- Sampling and Port Mirroring
- **Support for Aggregated Ethernet**—The Junos OS implementation of 802.3ad balances traffic across the member links within an aggregated Ethernet bundle based on the Layer 3 information carried in the packet. This implementation uses the same load-balancing algorithm used for per-flow load balancing.
- **Support for DCU accounting and SCU accounting on PTX1000 routers**—The destination class usage (DCU) accounting and source class usage (SCU) accounting are supported on PTX1000 routers.

You can maintain packet counts based on the entry and exit points for traffic passing through your network. Entry and exit points are identified by source and destination prefixes grouped into disjoint sets, which are defined as source classes and destination classes. SCU counts packets sent to customers by performing lookups on the IP source address and the IP destination address. SCU accounting enables you to track traffic originating from specific prefixes on the provider core and destined for specific prefixes on the customer edge. DCU counts packets from customers by performing lookups of the IP destination address. DCU accounting enables you to track traffic originating from the customer edge and destined for specific prefixes on the provider core router.



NOTE: DCU accounting and SCU accounting are supported only if the enhanced-mode statement is configured at the [edit chassis network-services] hierarchy level.

- **Chassis management**—The following CLI operational mode commands are supported on PTX1000 router:
 - show chassis hardware
 - show chassis temperature-thresholds
 - show chassis environment
 - show chassis firmware

Junos OS XML API and Scripting

- **Support for Python language for commit, event, op, and SNMP scripts (PTX1000)**—You can author commit, event, op, and SNMP scripts in Python on devices that include the Python extensions package in the software image. Creating automation scripts in Python enables you to take advantage of Python features and libraries, as well as leverage Junos PyEZ APIs to perform operational and configuration tasks on devices running Junos OS. Supported Python versions include Python 2.7.x.

[See [Understanding Python Automation Scripts for Devices Running Junos OS](#) and [Requirements for Executing Python Automation Scripts on Devices Running Junos OS.](#)]

Layer 2 Features

- **VLAN**—VLANs enable you to divide one physical broadcast domain into multiple virtual domains.
- **Link Layer Discovery Protocol (LLDP)**—LLDP enables a router to advertise its identity and capabilities on a LAN, as well as receive information about other network devices.

Layer 3 Features

- **BGP**—BGP is an exterior gateway protocol (EGP) for routing traffic between autonomous systems (AS). You can configure BGP at the **[edit protocols bgp]** hierarchy level.
- **OSPF**—The IPv4 OSPF protocol is an interior gateway protocol (IGP) for routing traffic within an autonomous system (AS). PTX1000 routers support OSPFv1, OSPFv2, and OSPFv3. You can configure OSPF at the **[edit protocols ospf]** hierarchy level.
- **Synchronization between OSPF and LDP**—LDP distributes labels in non-traffic-engineered applications. Labels are distributed along the best path determined by OSPF. If the synchronization between LDP and OSPF is lost, the label-switched path (LSP) goes down. Therefore, LDP and IS-IS synchronization is beneficial.

To advertise the maximum cost metric until LDP is operational for LDP synchronization, include the **ldp-synchronization** statement at the **[edit protocols ospf interface interface-name]** hierarchy.

- **Bidirectional Forwarding Detection (BFD) support for static routes and for the BGP, IS-IS, OSPF, PIM, and RIP protocols**—The 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 a PTX1000 router, you can configure BFD for static routes and for the BGP, IS-IS, OSPF, PIM, and RIP protocols.

- **IS-IS**—The IS-IS protocol is an interior gateway protocol (IGP) for routing traffic within an autonomous system.
- **Synchronization between IS-IS and LDP**—LDP distributes labels in non-traffic-engineered applications. Labels are distributed along the best path determined by IS-IS. If the synchronization between LDP and IS-IS is lost, the label-switched path (LSP) goes down. Therefore, LDP and IS-IS synchronization is beneficial.

To advertise the maximum cost metric until LDP is operational for LDP synchronization, include the **ldp-synchronization** statement at the **[edit protocols isis interface interface-name]** hierarchy.

Layer 3 Logical Interfaces

- **Layer 3 logical interfaces**—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 PTX1000 router to a Layer 2 switch.
- **Generic routing encapsulation (GRE)**—You can use GRE tunneling services to encapsulate any network layer protocol over an IP network. Acting as a tunnel source router, the encapsulates a payload packet that is to be transported through a tunnel to a destination network. The router 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 router 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.

Multicast Protocols

- **Protocol Independent Multicast sparse mode**—PIM sparse mode enables efficient routing to multicast groups with receivers 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)**—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.

MPLS

- **LDP**—The Label Distribution Protocol (LDP) is a protocol for distributing labels in non-traffic-engineered applications. LDP enables routers to establish label-switched paths (LSPs) through a network by mapping network-layer routing information directly to data link layer-switched paths. For more information, see the *MPLS Applications Feature Guide for Routing Devices*.
- **RSVP**—RSVP is a resource reservation setup protocol that is used by both network hosts and routers. Hosts use RSVP to request a specific class of service (CoS) from the network for particular application flows. Routers use RSVP to deliver CoS requests to all routers along the data path. RSVP also can maintain and refresh states for a requested CoS application flow. For more information, see the *MPLS Applications Feature Guide for Routing Devices*.
- **IPv6 tunneling over an MPLS-based IPv4 network**—Tunneling enables you to connect IPv6 sites over an IPv4 MPLS-enabled backbone. IPv6 packets are carried over an IPv4 MPLS tunnel. To enable this service, you need to deploy provider edge (PE) routers that can run IPv4, MPLS, and BGP toward the core and IPv6 toward the edge.

[See [Example: Tunneling IPv6 Traffic over MPLS IPv4 Networks](#)]

- **Egress peer engineering of service labels (such as BGP and MPLS) and egress peer protection for BGP-LU**—You can enable traffic engineering of service traffic, such as MPLS LSP traffic between autonomous systems (ASs), by using BGP-labeled unicast for optimum utilization of the advertised egress routes. You can specify one or more backup devices for the primary egress AS boundary router. Junos OS installs the backup path in addition to the primary path in the MPLS forwarding table, which enables MPLS fast reroute (FRR) when the primary link fails. It provides support for the FRR protection backup scheme to perform an IP lookup to determine a new egress interface.

[See [Configuring Egress Peer Traffic Engineering by Using BGP Labeled Unicast and Enabling MPLS Fast Reroute](#)]

- **ECMP (64-way) with configurable Layer 3 hash options**—Allows you to configure 64 equal-cost multipath (ECMP) next hops for RSVP and LDP LSPs. To configure the maximum limit for ECMP next hops, include the **maximum-ecmp next-hops** statement at the **[edit chassis]** hierarchy level.

To view the details of the ECMP next hops, issue the **show route** command. The **show route summary** command also shows the current configuration for the maximum ECMP limit.

- **MPLS capabilities**—MPLS provides both label edge router (LER) and label switch router (LSR) and provides the following capabilities:
 - 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 FRR

- 6PE and 6VPE devices
- Layer 3 VPNs for both IPv4 and IPv6
- **Support for IS-IS segment routing**—IS-IS segment routing support is enabled through MPLS. Currently, label advertisements are supported for IS-IS only. IS-IS creates an adjacency segment per adjacency, per level, and per address family (one each for IPv4 and IPv6). Junos OS IS-IS implementation allocates node segment label blocks in accordance with the IS-IS protocol extensions for supporting segment routing node segments and provides a mechanism to the network operator to provision an IPv4 or IPv6 address family node segment index. To configure segment routing, use the following configuration statements at the **[edit protocols isis]** hierarchy level:
 - **source-packet-routing**—Enable the source packet routing feature.
 - **node-segment**—Enable source packet routing at all levels.
 - **use-source-packet-routing**—Enable use of source packet routing node segment labels for computing backup paths for normal IPv4 or IPv6 IS-IS prefixes and primary IS-IS source packet routing node segments.
 - **no-advertise-adjacency-segment**—Disable advertising of the adjacency segment on all levels for a specific interface.
- **Support for filter-based GRE for IPv4 and IPv6 tunneling on PTX Series routers**—The filter-based generic routing encapsulation (GRE) for IPv4 and IPv6 tunneling uses firewall filters to provide de-encapsulation of GRE traffic. The configuration of filter-based GRE de-encapsulation supports the **routing-instance** statement as one of the attributes.



NOTE: Configuring filter-based GRE for IPv4 and IPv6 tunneling is supported only when the enhanced-mode statement is configured at the **[edit chassis network-services]** hierarchy level.

VPN

- **Layer 3 VPN**—A Layer 3 VPN is a set of sites that share common routing information and whose connectivity is controlled by a collection of policies. The sites that make up a Layer 3 VPN are connected over a provider's existing Internet backbone.

In Junos OS, Layer 3 VPNs are based on RFC 4364, *BGP/MPLS IP Virtual Private Networks (VPNs)*. This RFC defines a mechanism by which service providers can use their IP backbones to provide Layer 3 VPN services to their customers.

[See [Understanding Layer 3 VPNs](#)]

Network Management and Monitoring

- **System logging (syslog)**—Syslog enables you to log system messages into a local directory on the router or to a syslog server.
- **Junos Space Service Now**—Junos Space Service Now is an application that runs on the Junos Space Network Management Platform to automate fault management and accelerate issue resolution.

[See [Junos Space Service Now](#)]

- **Support for SNMP on PTX1000**—SNMP versions 1, 2, and 3 are supported on the PTX1000. SNMP enables you to monitor network devices from a central location. Junos OS includes an SNMP agent that provides remote management applications with access to detailed information about the devices on the network.
- **Port mirroring**—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.
- **Support for inline active flow monitoring on PTX1000**—You can use the export capabilities of inline active flow monitoring with IP Flow Information Export (IPFIX) to define a flow record template suitable for IPv4 or IPv6 traffic. The flow record template provides the flexibility for future enhancements and the ability to add new attributes to inline active flow monitoring without changing to a newer version.

Security

- **Support for Firewall on PTX1000**—You can configure a firewall filter with match conditions for Internet Protocol version 4 (IPv4) traffic (family inet).
- **Filter-based forwarding**—For IPv4 traffic only, you can use stateless firewall filters in conjunction with forwarding classes and routing instances to control how packets travel in a network. This is called filter-based forwarding (FBF).
- **Policing support**—You can use policing to apply limits to traffic flow and set consequences for packets that exceed those limits.

System Management

- **Fabric management**—You can set up and manage the fabric connections between the Packet Forwarding Engines in the router. You can use the operational mode command **show chassis fabric sibs** to display the summary status information for the fabric SIBs.
- **System utilization alarms**—This feature provides system alarms to alert you of high disk usage in the **/var** partition on the router. 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 of more than 90 percent indicates that the partition is full and raises a major alarm condition.

Traffic Management

- **Support for Class of Service (CoS)**—Class of Service is the assignment of traffic flows to different service levels. Service providers can use router-based Class of Service features to define service levels that provide different delay, jitter (delay variation), and packet loss characteristics to particular applications served by specific traffic flows.

On a PTX1000 router, you can divide traffic into classes and offer various levels of throughput and packet loss when congestion occurs.

- **CoS rewrite rules**—You can use rewrite rules to set the value of the CoS bits within a packet header and, therefore, you can alter the CoS settings of incoming packets. Supported rewrite rules are IEEE 802.1p, DSCP, and MPLS EXP.
- **BA classification**—Packet classification associates incoming packets with a particular CoS servicing level. Behavior aggregate (BA) classifiers examine the Differentiated Services code point (DSCP or DSCP IPv6) value, the IEEE 802.1p CoS value, or the MPLS EXP value in the packet header to determine the CoS settings applied to the packet. BA classifiers enable you to set the forwarding class and loss priority of a packet based on the incoming CoS value.
- **Multifield classification**—Multifield classification refers to a method of packet classification that uses a standard stateless firewall filter to set the forwarding class or PLP for packets entering or exiting the interface based on multiple fields in the IP packet. You can configure multifield classifier that specifies match conditions based on CoS values (such as DSCP value, MPLS EXP bits, or IEEE 802.1p bits).
- **CoS-based forwarding**—Class-of-service (CoS)-based forwarding (CBF) enables you to control next-hop selection based on a packet's class of service and, in particular, the value of the IP packet's precedence bits. For example, you might want to specify a particular interface or next hop to carry high-priority traffic while all best-effort traffic takes some other path. When a routing protocol discovers equal-cost paths, it can pick a path at random or load-balance across the paths through either hash selection or round robin. CBF allows path selection based on class.

Services

- **Routing instance**—You can configure one the following routing instances for currently supported protocols (OSPF, IS-IS, and BGP):
 - **forwarding**—Provides support for filter-based forwarding, where interfaces are not associated with instances.
 - **no-forwarding**—This is the default routing instance. Do not create a corresponding forwarding instance. Use this routing instance type when a separation of routing table information is required.
 - **vrf**—VPN routing and forwarding (VRF) instance. Provides support for Layer 3 VPNs, where interface routes for each instance go into the corresponding forwarding table only.
- **DHCPv6 relay agent**—The DHCPv6 relay agent enhances the DHCP relay agent by providing support in an IPv6 network. The DHCPv6 relay agent passes messages between the DHCPv6 client and the DHCPv6 server, similar to the way a DHCP relay agent supports an IPv4 network.

To configure the DHCPv6 relay agent on the router (or switch), you include the **dhcpv6** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level.

- **IPv6 Neighbor Discovery Protocol**—This protocol allows nodes on the same link to advertise their existence to their neighbors and to learn about the existence of their neighbors. Neighbor Discovery Protocol is built on top of Internet Control Message Protocol version 6 (ICMPv6). It replaces the following IPv4 protocols: Router Discovery (RDISC), Address Resolution Protocol (ARP), and ICMPv4 redirect.

Upgrade Instructions for PTX1000 BIOS

Introduction

The primary upgrade path between Junos 15.1X and 16.1X releases for PTX1000 at this time is through a USB bootable drive. During the PTX1000 beta program, Juniper is continually making improvements to all aspects of the system. One of these improvements is with the BIOS running on the PTX1000. Juniper has an updated BIOS which can now support netboot functionality and also fixes a potential boot device order issue. This section explains you the BIOS upgrade process.

There are two separate procedures described in this section based upon the current software version running on the PTX1000 in your lab.

Software and BIOS Image Locations

The software is posted to the production download servers, you can pull down the most recent software from that website (ie: www.juniper.net -> support). After FRS, if you discover that you do need to upgrade the BIOS on your PTX1000, you may need to contact JTAC.

Determining your software upgrade needs

If you are running Junos 16.1X65D20 software (if you participated in the beta program) and you wish to upgrade to 16.1X65D30 released software, then you may only need to perform a CLI upgrade. Please use the table matrix below to establish your upgrade path.

Starting Release	Target Release	Current BIOS Version	Upgrade Action
15.1X	16.1X65-D30	18.8	Upgrade via CLI to 15.1X53-D33 on the PTX1000, then upgrade BIOS via CLI, then upgrade via USB to 16.1X65-D30
15.1X	16.1X65-D30	18.8Y	Upgrade via USB to 16.1X65-D30
16.1X65-D20	16.1X65-D30	18.8	Downgrade via USB to 15.1X53-D33, then upgrade BIOS via CLI, then upgrade via USB to 16.1X65-D30
16.1X65-D20	16.1X65-D30	18.8Y	Upgrade via CLI to 16.1X65-D30

BIOS Upgrade Process for PTX1000 with Junos 15.1X Software Installed

- If the PTX1000 is currently running Junos 15.1X53D33 software, the system is ready for the BIOS upgrade. Please skip to the "Upgrading the BIOS" section.
- If the PTX1000 is running a version of software earlier than Junos 15.1X53D33, then please go to the beta website above and download the jinstall upgrade package. You can simply use **request system software add** to add the package and reboot. After this is completed, please skip to the "Upgrading the BIOS" section.

BIOS Upgrade Process for PTX1000 with Junos 16.1X Software Installed

If the PTX1000 is running 16.1X software, to upgrade the BIOS you must first downgrade to Junos 15.1 through a USB downgrade, then update the BIOS. If you recall, during the Junos 16.1 USB upgrade, you were required to enter into the BIOS upon bootup and modify a few settings. For the downgrade to 15.1, these settings will need to be reversed.

Following are the steps to prepare the router for the BIOS upgrade when running Junos 16.1:

1. Save your configuration to a location off the PTX1000 as the configuration not be saved across the downgrade/upgrade process.
2. Plug the USB drive into the machine you are using to create the bootable USB.
3. Download a copy of Junos 15.1X53D33 software from the beta website listed above.
4. Unzip the install image.
5. Create a bootable USB drive. Example unix command: "dd if=filename of=/dev/da0 bs=4M", where /dev/da0 is the plugged usb drive - your command may differ based upon your OS.

6. After the copy is completed, please type "sync" (if Unix) to ensure all writing to the USB is completed. If you are not using a Unix based OS, your command may be different, but please make sure all writing is done to the USB drive.
7. Insert the USB drive into the PTX1000.
8. Log into the console of the PTX1000.
9. Reboot the PTX1000 and press ESC to enter the BIOS.
10. Select "Setup Utility".
11. Select "Boot" tab.
12. Change Boot Type to "Legacy Boot Type".
13. Change EFI Device First" to "Enabled".
14. Change Network 0 Boot to "Enabled".
15. Change Network 1 Boot to "Enabled".
16. Exit the BIOS and save changes.
17. Reboot the PTX1000 to ensure the BIOS changes take effect.
18. Reboot the PTX1000 and press ESC to enter the BIOS.
19. At the BIOS menu, select "Boot Manager"
20. Select "USB Device" - Press Enter to Boot the USB device.
21. You should eventually see the GRUB console - press "Y" to install the image on the SSD. Note: this "[Y/n]" prompt may be hidden by some log messages, but the PTX will wait a few minutes for some input
22. After the upgrade is completed, remove the USB drive before rebooting the PTX1000.
23. The PTX1000 should be running Junos 15.1X53D33 software at this time. Please now follow the steps in the "Upgrading the BIOS" section.

Upgrading the BIOS

The PTX1000 should be running Junos 15.1X53D33 based software. Please follow the steps below:

1. Download BIOS image from
<https://www.juniper.net/support/beta/index.page?p=beta14#software>
2. Copy this software package in /var/tmp/ on the PTX1000
3. On the PTX1000, run the command "request system software add "package_name" reboot. This command will upgrade the BIOS and perform a reboot

Once the BIOS upgrade is done, you will notice a couple of things, don't be alarmed. The default mode for the new BIOS is UEFI mode. Previously it was legacy (default)

1. You may not see your Hard drives in the BIOS manager. This is because you still have the 15.1X53 image which is legacy and is not recognized in the UEFI.
2. From here, you have the option of upgrade to the 16.1 Image via either a USB or a Netboot (if PXE server is set up).
3. Upon successful installation of the 16.1 image, you will now be able to see the Hard drives in your BIOS manager.
4. The next boot device is controlled primarily from JunOS and the user is not expected to change this settings so don't be alarmed. If you need to change this, let us know and we will share details on how to do so from BIOS.
5. It is recommended to upgrade to 16.1X65D20.3 code posted on the beta website listed above. If you upgrade to earlier code, the next boot order may not work correctly.

Upgrade Back to Junos 16.1 with the Upgraded BIOS

The steps to upgrade back to Junos 16.1 using a USB drive are as follows:

1. Download the Junos 16.1X65D-20.3 install image from the beta website.
2. Insert a USB drive into the machine you are using to create the bootable USB.
3. Unzip the Junos 16.1X65-D20.3 install image.
4. Create the bootable drive with the following command (if using unix): "dd if=filename of=/dev/da0 bs=4M", where /dev/da0 is the plugged usb drive - your command may differ based upon your OS.
5. After the copy is completed, please type "sync" (if Unix) to ensure all writing to the USB is completed. If you are not using a Unix based OS, your command may be different.
6. Insert the USB drive into the PTX1000.
7. Log into the console of the PTX1000.
8. Reboot the PTX1000 and from the console, press ESC to enter the BIOS.
9. In the BIOS, go to "Setup Utility".
10. Next, go to the "Boot" tab.
11. Make sure "Boot type" is set to UEFI.
12. Make sure "EFI Device First" is set to enabled.
13. Change "Network 0 Boot" to disabled.
14. Change "Network 1 Boot" to disabled.
15. Go to the Exit tab and select "Exit Saving Changes".
16. Power cycle the router to load the new BIOS settings.
17. Reboot again and press ESC to enter the BIOS menu again.
18. Select "Boot Manager", then Select "boot from USB".

19. After a while, there will be a "copy image to...[Y/n]" question which may be somewhat hidden due to some of the logging. Please keep an eye out for this question because if "Y" is not hit within a certain time period, the PTX will boot on the existing software and the USB upgrade will not be completed.

20. When installation is complete, remove the USB and reboot.

For any queries or reporting an issue, email to beta-eng@juniper.net.

Upgrade Instructions for PTX1000 B1 Software

Introduction

The current software for PTX1000 B1 is Junos 16.1X65-D10.1.

All sites will need to upgrade to this software and the currently supported upgrade path is via a USB install. Some PTX1000 devices will have 15.1X based software while others may have 16.1X based software. The upgrade steps will depend upon which version of software is on the PTX1000 at your site. Please note that the PTX1000 is just starting the beta period and we are still making changes to the system BIOS and the software. Because of this, we will request that an upgrade will go deeper into the system than we normally request. These upgrade issues will be removed at FRS of the product and after FRS, you will simply use the standard Juniper "request system software..." command for an upgrade. If you have any concerns or issues with the upgrade, the beta team will be happy to assist in the upgrade of the unit. If possible, console access to the beta team may help with the upgrade.

Step 1: For all testers - Create the bootable USB device

1. Insert an 8GB or larger USB drive into the machine you are building the bootable device.
2. Run the command (unix example) "dd if=junos-vmhost-install-usb-x86-64-16.1X65-D10.1.img.gz of=/dev/da0 bs=4M, where /dev/da0 is the plugged usb drive (your OS may need a different command).
3. When the prompt comes back, type "sync" to ensure writing is complete. "sync" is a unix command to make sure all disk writes are complete. Please use a command specific to your OS.
4. When the sync is complete, unplug the USB and move over to the PTX10000.

For PTX1000 units which have 15.1X software

To upgrade the system from Junos 15.1 software, the following is required:

- BIOS changes will need to be made, saved and the PTX rebooted.
- Console access to the PTX1000 is required.

Following are the individual steps required to upgrade:

1. Plug the bootable USB drive into the PTX1000.
2. Log into the console of the PTX1000.
3. Reboot the PTX1000 and from the console, press ESC to enter the BIOS.
4. In the BIOS, go to "Setup Utility".
5. Next, go to the "Boot tab".
6. Select "Boot type" to UEFI.
7. Change "EFI Device First" to enabled.
8. Change "Network 0 Boot" to disabled.
9. Change "Network 1 Boot" to disabled.
10. Go to the Exit tab and select "Exit Saving Changes".
11. Power cycle the router to load the new BIOS settings.
12. Reboot again and press ESC to enter the BIOS menu again.
13. Select "Boot Manager".
14. Select "EFI USB Device" - Press Enter to Boot the EFI USB device.
15. You should see the GRUB console - press "Y" to install the image on the SSD.
16. After the upgrade is completed, remove the USB drive before rebooting the PTX1000.
17. The PTX1000 should come up running Junos 16.1X65-D10.1 software.

For PTX1000 units which have 16.1X software

To upgrade the system from Junos 16.1 software, the following is required:

- BIOS changes will need to be made, saved and the PTX rebooted.
- Console access to the PTX1000 is required.

Following are the individual steps required to upgrade:

1. Plug the bootable USB drive into the PTX1000.
2. Log into the console of the PTX1000.
3. Reboot the PTX1000 and from the console, press ESC to enter the BIOS.
4. From the BIOS menu, select "Boot Manager".
5. Select "EFI USB Device" - Press Enter to Boot the EFI USB device.
6. You should see the GRUB console - press "Y" to install the image on the SSD.
7. After the upgrade is completed, remove the USB drive before rebooting the PTX1000.
8. The PTX1000 should come up running Junos 16.1X65-D10.1 software.

Known Behavior

This section lists known behavior and limitations in hardware and software in Junos OS Release 16.1RX65D35 for PTX1000 routers.

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

- [General Routing on page 18](#)

General Routing

- The following **request** commands are not available on the PTX1000:

- **request system partition**
- **request system power off**
- **request system power on**
- **request system snapshot**

The scope of functionality of the following commands is limited to Junos OS guest level:

- **request system reboot**
- **request system software add**
- **request system zeroize**
- The guest Junos OS and the host OS on the PTX1000 use different time zones. Therefore, there is a difference between the timestamps in the system log files of Junos OS and the host OS. As a workaround, you can calculate the current difference between the time zones used by Junos OS and the host OS and work with logs that show this difference in time.

Known Issues

This section lists the known issues in hardware and software in Junos OS Release 16.1RX65D35 for PTX1000 routers.

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

- [General Routing on page 18](#)
- [Interfaces and Chassis on page 19](#)

General Routing

- Observing sheaf leak messages continuously on PTX1000. [PR 1246652]
- CM ERROR codes on TOE module are registered/reported on wrong PFE number. [PR 1227749]

- A minimum of 2 power supplies have to be present and online. Otherwise, the system should be powered off. [PR 1214414]

Interfaces and Chassis

- rpd core in if_addr_link @if_api.c:2338 during interface flap test. [PR 1251114]
- rpd core in io_mem_free @io_utils.c:1073. [PR 1253185]
- High ping times between PTX1000 chassis. [PR 1212120]
- Interfaces disappeared on PTX1K chassis during interface flap test. [PR 1252397]

Product Compatibility

- [Hardware Compatibility on page 19](#)

Hardware Compatibility

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

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.

Revision History

15 February 2017—Revision 2, Junos OS for PTX1000 Packet Transport Routers, Release 16.1X65D35

20 January 2017—Revision 1, Junos OS for PTX1000 Packet Transport Routers, Release 16.1X65D30

Copyright © 2017, Juniper Networks, Inc. All rights reserved.

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

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