Junos® OS 12.3X54 Release Notes

Release 12.3X54
18 July, 2014
Revision 1

These release notes accompany ACX Series Universal Access Routers Release 12.3X54 of the Junos operating system (Junos OS). They describe device documentation and known problems with the software. Junos OS runs on all Juniper Networks ACX Series routers.

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

You can also find these release notes on the Juniper Networks Junos OS Documentation Web page, which is located at https://www.juniper.net/techpubs/software/junos/.

Contents

Junos OS Release Notes for ACX Series Routers

New Features in Junos OS Release 12.3X54 for ACX Series Routers

Powered by Junos OS, the ACX Series Universal Access Routers provide superior management for rapid provisioning to the access network. They are designed to support residential, mobile, and business access. The ACX Series routers include the ACX1000, ACX1100, ACX2000, ACX2100, and ACX4000 routers.

The following are the key features of the ACX Series routers:

- High performance: Up to 10-Gigabit Ethernet capable
- Seamless MPLS traffic engineering for optimal paths and per-customer quality of service in the access layer
- Built-in Precision Timing Protocol (PTP) and Synchronized Ethernet to eliminate dropped calls and data retransmissions
- Environmentally hardened with 65–W Power over Ethernet Plus (PoE+)

NOTE: **PoE is not supported on the ACX1000, ACX1100, and ACX2100 routers.**

- Carrier Ethernet services

The following features have been added to Junos OS Release 12.3X54 for the ACX Series Universal Access Routers. Following the description is the title of the manual or manuals to consult for further information:

Class of Service (CoS)

- **CoS for PPP and MLPPP Interfaces**—CoS functionalities are supported on PPP and MLPPP interfaces. Up to four forwarding classes and four queues are supported per logical interface for PPP and MLPPP packets.

  The following restrictions apply when you configure CoS on PPP and MLPPP interfaces on ACX Series routers:

  - For interfaces with PPP encapsulation, you can configure interfaces to support only the IPv4, Internet Protocol Control Protocol (IPCP), PPP Challenge Handshake Authentication Protocol (CHAP), and Password Authentication Protocol (PAP) applications.
  - Drop timeout is not supported.
  - Loss of traffic occurs during a change of scheduling configuration; you cannot modify scheduling attributes instantaneously.
  - Buffer size is calculated in terms of number of packets, with 256 bytes considered as the average packet size.
  - Only two loss priority levels, namely low and high, are supported.

- **Support for MLPPP encapsulation**—You configure multilink bundles as logical units or channels on the link services interface lsq-0/0/0. With MLPPP, multilink bundles are configured as logical units on lsq-0/0/0—for example, lsq-0/0/0.0 and lsq-0/0/0.1. After creating multilink bundles, you add constituent links to the bundle.

  MLPPP is supported on ACX1000, ACX2000, ACX2100 routers, and with Channelized OC3/STM1 (Multi-Rate) MICs with SFP and 16-port Channelized E1/T1 Circuit Emulation MIC on ACX4000 routers. With multilink PPP bundles, you can use PPP Challenge Handshake Authentication Protocol (CHAP) and Password Authentication Protocol (PAP) for secure transmission over the PPP interfaces.

  To configure MLPPP encapsulation, include the **encapsulation multilink-ppp** statement at the **[edit interfaces lsq-fpc/pic/port unit *logical-unit-number*]** hierarchy level. To aggregate T1 links into a an MLPPP bundle, include the **bundle** statement at the **[edit interfaces t1-fpc/pic/port unit *logical-unit-number* family mlppp]** hierarchy level:

- **Support for configuring the shared buffer size**—Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers enable you to control the amount of shared packet buffer a given queue can consume. Using this feature, you can ensure that important queues have a higher chance of using the shared buffers than by not so important queues. To achieve this, you can configure lower values for **shared-buffer maximum** CLI statement for the not so important queues, and higher values for the **shared-buffer maximum** CLI statement for the important queues.

  You can explicitly configure the **shared-buffer maximum** CLI statement at the **[edit class-of-service]** hierarchy level.

  

  NOTE: **The default value for shared-buffer maximum is 66%.**

You can override the default reserved **buffer-size** assigned per queue at the following configuration:

```
set class-of-service {
  schedulers {
    <scheduler-name> {
      buffer-size (percentage percentage | remainder | temporal);
    }
  }
}
```

NOTE: When there is no shared buffer, the minimum reserved buffer should be equal to MTU worth of cells (12 cells), which means the configured reserved buffer value should be in the range of 20 percentage to 100 percentage.

Interfaces and Chassis

- **Support for logical tunnels**—Logical tunnel (**lt-**) interfaces provide quite different services depending on the host router. On ACX Series routers, logical tunnel interfaces enable you to connect a bridge domain and a pseudowire.

  To create tunnel interfaces, an FPC and the corresponding Packet Forwarding Engine on an ACX Series router must be configured to be used for tunneling services at the **[edit chassis]** hierarchy level. The amount of bandwidth reserved for tunnel services must also be configured.

  To create logical tunnel interfaces and the bandwidth in gigabits per second to reserve for tunnel services, include the **tunnel-services bandwidth (1g | 10g)** statement at the **[edit chassis fpc *slot-number* pic *number*]** hierarchy level.

  [*ACX Series Universal Access Router Configuration Guide]*]

- **Support for PPP encapsulation on Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP**—On ACX4000 routers, you can configure Point-to-Point Protocol (PPP) encapsulation on physical interfaces on Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP. PPP provides a standard method for transporting multiprotocol datagrams over a point-to-point link. PPP uses the High-Speed Data Link Control (HDLC) protocol for its physical interfaces and provides a packet-oriented interface for the network-layer protocols.

  On ACX Series routers, E1, T1, and *N*xDS0 interfaces support PPP encapsulation.

  IP class of service (CoS) is not supported on PPP interfaces. All the traffic is sent to the best effort queue (queue 0) and CoS code points are not processed. Also, fixed classifiers are not supported. PPP is supported only for IPv4 networks.

  [*ACX Series Universal Access Router Configuration Guide*]

- **Support for dual-rate SFP+ modules**—ACX2000, ACX2100, and ACX4000 routers support the dual-rate SFP+ optic modules. These modules operate at either 1 Gbps or 10 Gbps speeds. When you plug in the module to the small form-factor pluggable plus (SFP+) slot, the module can be set at either 1 Gbps or 10 Gpbs.

ACX Series routers use the 2-port 10-Gigabit Ethernet (LAN) SFP+ MIC in the following two combinations:

- 2-port 10-Gigabit Ethernet (LAN) SFP+ uses BCM84728 PHY on ACX 2100/ACX4000 routers.
- 2-port 10-Gigabit Ethernet (LAN) SFP+ uses BCM8728/8747 on ACX2000 routers.

To configure an **xe** port in 1-Gigabit Ethernet mode , use the **set interfaces xe-x/y/z speed 1g** statement. To configure an **xe** port in 10-Gigabit Ethernet mode, use the **set interfaces xe-x/y/z speed 10g** statement. The default speed mode is 1-Gigabit Ethernet mode.

[*ACX Series Universal Access Router Configuration Guide*]

- **Support for NAT**—Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers supports Network Address Translation (NAT). NAT is a method for modifying or translating network address information in packet headers. Either or both source and destination addresses in a packet may be translated. NAT can include the translation of port numbers as well as IP addresses. ACX Series routers support only source NAT for IPv4 packets. Static and destination NAT types are currently not supported on the ACX Series routers.

  NOTE: In ACX Series routers, NAT is supported only on the ACX1100 AC-powered router.

  [*ACX Series Universal Access Router Configuration Guide*]

- **Support for inline service interface**—Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers supports inline service interfaces. An inline service interface (si-) is a virtual physical interface that resides on the Packet Forwarding Engine. The **si-** interface makes it possible to provide NAT services without a special services PIC.

  To configure inline NAT, you define the service interface as a type **si-** (service-inline) interface. You must also reserve adequate bandwidth for the inline interface. This enables you to configure both interface and next-hop service sets used for NAT.

  NOTE: In ACX Series routers, you can configure only one inline services physical interface—si-0/0/0—as an anchor interface for NAT sessions.

  [*ACX Series Universal Access Router Configuration Guide*]

- **Support for inverse multiplexing for ATM (IMA) on Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP**—Starting in Release 12.3X54, you can configure inverse multiplexing for ATM (IMA) on the Channelized OC3/STM1 (Multi-Rate) Circuit Emulation MIC with SFP (model number: ACX-MIC-4COC3-1COC12CE) on ACX Series routers. You can configure four OC3/STM1 ports or one OC12/STM4 port on this rate-selectable MIC.

[*ACX Series Universal Access Router Configuration Guide*]

- **Support for TDR for diagnosing cable faults**--Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers supports Time Domain Reflectometry (TDR), which is a technology used for diagnosing copper cable states. This technique can be used to determine whether cabling is at fault when you cannot establish a link. TDR detects the defects by sending a signal through a cable, and reflecting it from the end of the cable. Open circuits, short circuits, sharp bends, and other defects in the cable reflects the signal back at different amplitudes, depending on the severity of the defect. TDR diagnostics is supported only on copper interfaces and not on fiber interfaces.

  TDR provides the following capabilities that you can use to effectively identify and correct cable problems:

  - Display detailed information about the status of a twisted-pair cable, such as cable pair being open or short-circuited.
  - Determine the distance in meters at which open or short-circuit is detected.
  - Detect whether or not the twisted pairs are swapped.
  - Identify the polarity status of the twisted pair.
  - Determine any downshift in the connection speed.

  [*ACX Series Universal Access Router Configuration Guide*]

Layer 2 Services

- **Support for Ethernet ring protection switching**--Starting in Release 12.3X54, you can configure Ethernet ring protection switching (ERPS) on ACX Series routers to achieve high reliability and network stability. The basic idea of an Ethernet ring is to use one specific link, called the ring protection link (RPL), to protect the whole ring. Links in the ring will never form loops that fatally affect the network operation and services availability.

  ACX Series routers support multiple Ethernet ring instances that share the physical ring. Each instance has its own control channel and a specific data channel. Each ring instance can take a different path to achieve load balancing in the physical ring. When no data channel is specified, ERP operates only on the VLAN ID associated with the control channel. G.8032 open rings are supported.

  ACX Series routers do not support aggregate Ethernet–based rings.

  To configure Ethernet ring protection switching, include the **protection-ring** statement at the **[edit protocols]** hierarchy level.

  [*ACX Series Universal Access Router Configuration Guide*]

- **Support for RFC 2544-based benchmarking tests for Layer 2 and Layer 3 Ethernet services**—ACX Series routers support the RFC 2544 benchmarking tests to measure performance characteristics and efficiency of the routers, such as throughput, bursty frames, frame loss, and latency.

  - You can configure RFC 2544 tests on the following underlying services:
    - Between two IPv4 endpoints.

- Between two user-to-network interfaces (UNIs) of Ethernet Virtual Connection (EVC), Ethernet Private Line (EPL, also called E-LINE), Ethernet Virtual Private Line (EVPL), EVC (EPL, EVPL).

RFC 2544 tests are supported only in the egress direction or the user-to-network interface (UNI) direction of Ethernet line or LAN service parameters in a bridge domain between two routers for unicast traffic.

You can run RFC 2544 benchmarking inet tests on Layer 3 VPN or virtual router.

To configure a benchmarking test to detect and measure performance attributes for E-LINE, ELAN, and EVPL services, you must configure a test profile and reference the test profile in a unique test name that defines the parameters for the test to be performed on a certain ACX Series router. To configure a test profile, include the **test-profile *profile-name*** statement at the **[edit services rpm rfc2544-benchmarking]** hierarchy level. To configure a test name, include the **test-name *test-name*** statement at the **[edit services rpm rfc2544-benchmarking]** hierarchy level.

[*ACX Series Universal Access Router Configuration Guide*]

- **Support for hybrid mode**—Starting in Junos OS Release 12.3X54, hybrid mode is supported on ACX Series routers. The combined operation of Synchronous Ethernet and Precision Time Protocol (PTP) is also known as hybrid mode. In hybrid mode, the synchronous Ethernet equipment clock (EEC) on the router derives the frequency from Synchronous Ethernet and the phase and time of day from PTP. Time synchronization includes both phase synchronization and frequency synchronization.

  Synchronous Ethernet supports hop-by-hop frequency transfer, where all interfaces on the trail must support Synchronous Ethernet. PTP (also known as IEEE 1588v2) synchronizes clocks between nodes in a network, thereby enabling the distribution of an accurate clock over a packet-switched network.

  To configure the router in hybrid mode, you must configure Synchronous Ethernet options at the **[edit chassis synchronization]** hierarchy level and configure PTP options at the **[edit protocols ptp]** hierarchy level. Configure hybrid mode options by including the **hybrid** statement at the **[edit protocols ptp slave]** hierarchy level.

  [*ACX Series Universal Access Router Configuration Guide*]

- **Support for integrated routing and bridging**—Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers supports integrated routing and bridging (IRB) functionality. IRB provides routing capability on a bridge domain. To enable this functionality, you need to configure an IRB interface as a routing interface in a bridge domain and then configure a Layer 3 protocol such as IP or ISO on the IRB interface.

  ACX Series routers support IRB for routing IPv4 packets. IPv6 and MPLS packets are not supported.

  [*ACX Series Universal Access Router Configuration Guide*]

- **Support for IGMP snooping**—Starting in Release 12.3X54, Junos OS for ACX Series routers support IGMP snooping functionality. IGMP snooping functions by snooping at the IGMP packets received by the switch interfaces and building a multicast database similar to that a multicast router builds in a Layer 3 network. Using this database, the switch can forward multicast traffic only to the downstream interfaces of interested

receivers. This technique allows more efficient use of network bandwidth, particularly for IPTV applications. You configure IGMP snooping for each bridge on the router.

[*ACX Series Universal Access Router Configuration Guide*]

- **Support for unicast RPF**—For interfaces that carry IPv4 or IPv6 traffic, you can reduce the impact of denial-of-service (DoS) attacks by configuring unicast reverse path forwarding (RPF). Unicast RPF helps determine the source of attacks and rejects packets from unexpected source addresses on interfaces where unicast RPF is enabled.

  Reverse path forwarding is not supported on the interfaces that you configure as tunnel sources. This limitation affects only the transit packets exiting the tunnel.

  To configure unicast reverse path forwarding, issue the **rpf-check** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family inet]** hierarchy level. RPF fail filters are not supported on ACX Series routers. The RPF check to be used when routing is asymmetrical is not supported.

  [*ACX Series Universal Access Router Configuration Guide]*]

- **Support for disabling local switching in bridge domains**—In a bridge domain, when a frame is received from a customer edge (CE) interface, it is flooded to the other CE interfaces and all of the provider edge (PE) interfaces if the destination MAC address is not learned or if the frame is either broadcast or multicast.

  To prevent CE devices from communicating directly include the **no-local-switching** statement at the **[edit bridge-domains *bridge-domain-name*]** hierarchy level. Configure the logical interfaces in the bridge domain as core-facing (PE interfaces) by including the **core-facing** statement at the **[edit interfaces *interface-name* unit *logical-unit-number* family *family*]** hierarchy level to specify that the VLAN is physically connected to a core-facing ISP router and ensure that the network does not improperly treat the interface as a client interface. When local switching is disabled, traffic from one CE interface is not forwarded to another CE interface.

  [*ACX Series Universal Access Router Configuration Guide]*]

- **Support for hierarchical VPLS**—Hierarchical LDP-based VPLS requires a full mesh of tunnel LSPs between all the PE routers that participate in the VPLS service. Using hierarchical connectivity reduces signaling and replication overhead to facilitate large-scale deployments. In a typical IPTV solution, IPTV sources are in the public domain and the subscribers are in the private VPN domain.

  For an efficient delivery of multicast data from the IPTV source to the set-top boxes or to subscribers in the private domain using the access devices (ACX Series routers in this case), P2MP LSPs and MVPN are necessary. Because VPLS and MVPN are not supported on ACX routers, an alternative approach is used to achieve hierarchical VPLS (HPVLS) capabilities. The subscriber devices are connected to a VPLS or a Layer 3 VPN domain on the ACX Series (access) router and they are configured to import the multicast routes. The support for PIM snooping in Layer 3 interfaces, IGMP snooping in Layer 2 networks, IRB interfaces, and logical tunnel interfaces enables HVPLS support.

  [*ACX Series Universal Access Router Configuration Guide]*]

- **Support for Ethernet link aggregation**--Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers support Ethernet link aggregation for Layer 2 bridging.

Ethernet link aggregation is a mechanism for increasing the bandwidth of Ethernet links linearly and improving the links' resiliency by bundling or combining multiple full-duplex, same-speed, point-to-point Ethernet links into a single virtual link. The virtual link interface is referred to as a link aggregation group (LAG) or an aggregated Ethernet interface. The LAG balances traffic across the member links within an aggregated Ethernet interface and effectively increases the uplink bandwidth. Another advantage of link aggregation is increased availability, because the LAG is composed of multiple member links. If one member link fails, the LAG continues to carry traffic over the remaining links.

[*ACX Series Universal Access Router Configuration Guide*]

- **Support for IEEE 802.1ag and ITU-T Y.1731 OAM protocols on up MEPs**—Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers supports IEEE 802.1ag configuration fault management (CFM) and ITU-T Y.1731 performance-monitoring OAM protocols on up maintenance association end points (MEPs). CFM OAM protocol is supported on link aggregation group (LAG) or aggregated Ethernet (AE) interfaces. The ITU-T Y.1731 protocol supports delay measurement on up MEPs but does not support loss measurement on up MEPs.

  NOTE: ACX Series routers do not support ITU-T Y.1731 OAM protocol on AE interfaces.

  [*ACX Series Universal Access Router Configuration Guide*]

- **Support for Ethernet alarm indication signal**—Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers support ITU-T Y.1731 Ethernet alarm indication signal function (ETH-AIS) to provide fault management for service providers. ETH-AIS enables you to suppress alarms when a fault condition is detected. Using ETH-AIS, an administrator can differentiate between faults at the customer level and faults at the provider level. When a fault condition is detected, a maintenance end point (MEP) generates ETH-AIS packets to the configured client levels for a specified duration until the fault condition is cleared. Any MEP configured to generate ETH-AIS packets signals to a level higher than its own. A MEP receiving ETH-AIS recognizes that the fault is at a lower level and then suppresses alarms at current level the MEP is in.

  ACX Series routers support ETH-AIS PDU generation for server MEPs on the basis of the following defect conditions:

  - Loss of connectivity (physical link loss detection)
  - Layer 2 circuit or Layer 2 VPN down

  [*ACX Series Universal Access Router Configuration Guide*]

Firewall Filter

- **Hierarchical policers on ACX Series routers**—On ACX Series routers, two-level ingress hierarchical policing is supported. With single-level policers, you cannot administer the method using which the committed information rate (CIR) and the excess information rate (EIR) values specified in the bandwidth profile are shared across different flows. For example, in a certain network deployment, you might want an equal or even

distribution of CIR across the individual flows. In such a scenario, you cannot accomplish this requirement using single-level policers and need to configure aggregate or hierarchical policers.

Aggregate policers operate in peak, guarantee, and hybrid modes. You can configure an aggregate policer by including the **aggregate-policer** *aggregate-policer-name* statement at the **[edit firewall policer** *policer-name* **if-exceeding]** hierarchy level. You can specify the mode of the aggregate policer by including the **aggregate-sharing-mode [guarantee | peak | hybrid]** statement at the **[edit firewall policer** *policer-name* **if-exceeding aggregate-policer** *aggregate-policer-name***]** hierarchy level.

- **Enhancement to support additional match capabilities under [edit firewall family] hierarchy level**—Starting in Release 12.3X54, Junos OS for ACX Series router supports additional match capabilities at the **[edit firewall family ccc filter]** and **[edit firewall family inet filter]** hierarchy levels.

  The existing firewall do not support Layer 2, Layer 3, and Layer 4 fields at the **[edit firewall family ccc filter]** hierarchy level. With additional matching fields, ACX Series routers support all the available Layer 2, Layer 3, and Layer 4 fields on the user-to-network interface side (ethernet-ccc/vlan-ccc).

  At the **[edit firewall family inet filter]** hierarchy level, the **fragment-flags** match field has been removed to accommodate the following Layer 2 and Layer 3 fields:

Table 1: Fields added to [edit firewall family inet filter] hierarchy level

Field	Description
first-fragment	Matches if packet is the first fragment
is-fragment	Matches if packet is a fragment

  The scale for **inet** and **ccc** in the firewall family filter has been reduced from 250 hardware entries to 122 hardware entries.

  [*ACX Series Universal Access Router Configuration Guide*]

Management

- **Support for VRRP version 2**—Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers supports Virtual Router Redundancy Protocol (VRRP) version 2 configuration. VRRP enables hosts on a LAN to make use of redundant routers on that LAN without requiring more than the static configuration of a single default route on the hosts. Routers running VRRP share the IP address corresponding to the default route configured on the hosts. At any time, one of the routers running VRRP is the master (active) and the others are backups. If the master fails, one of the backup routers becomes the new master router, providing a virtual default router and enabling traffic on the LAN to be routed without relying on a single router. Using VRRP, a backup router can take over a failed default router within a few seconds. This is done with minimum VRRP traffic and without any interaction with the hosts.

  The maximum number of VRRP groups that can be configured in ACX Series routers is 32.

[*ACX Series Universal Access Router Configuration Guide*]

- **Support for DHCP client and DHCP server**—Starting in Junos OS Release 12.3X54, ACX Series routers can be enabled to function as DHCP clients and extended DHCP local servers. An extended DHCP local server provides an IP address and other configuration information in response to a client request in the form of an address-lease offer. An ACX Series router configured as a DHCP client can obtain its TCP/IP settings and the IP address from a DHCP local server.

  [*ACX Series Universal Access Router Configuration Guide*]

- **Support for TWAMP**—Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers supports Two-Way Active Measurement Protocol (TWAMP). TWAMP provides a method for measuring round-trip IP performance between two devices in a network. ACX Series routers support only the reflector side of TWAMP.

  [*ACX Series Universal Access Router Configuration Guide*]

Security

- **Support for IP and MAC address validation**—Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers supports IP and MAC address validation. This feature enables the ACX Series router to validate that received packets contain a trusted IP source and an Ethernet MAC source address. Configuring MAC address validation can provide additional validation when subscribers access billable services. MAC address validation provides additional security by enabling the router to drop packets that do not match, such as packets with spoofed addresses.

  [*ACX Series Universal Access Router Configuration Guide*]

Network Management

- **Support for hybrid mode of autoinstallation**—Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers support hybrid mode of autoinstallation. The autoinstallation mechanism allows the router to configure itself out-of-the-box with no manual intervention, using the configuration available on the network, locally through a removable media, or using a combination of both. ACX Series routers support the retrieval of partial configuration from an external USB storage device plugged into the router's USB port during the autoinstallation process. This partial configuration in turn facilitates the network mode of autoinstallation to retrieve the complete configuration file from the network. This method is called hybrid mode of autoinstallation.

  [*ACX Series Universal Access Router Configuration Guide*]

Routing

- **Support for ECMP flow-based forwarding**—Starting in Release 12.3X54, Junos OS for ACX Series Universal Access Routers supports equal-cost multipath (ECMP) flow-based forwarding. An ECMP set is formed when the routing table contains multiple next-hop addresses for the same destination with equal cost. If there is an ECMP set for the active route, Junos OS uses a hash algorithm to choose one of the next-hop addresses in the ECMP set to install in the forwarding table. You can configure Junos OS so that multiple next-hop entries in an ECMP set are installed in the forwarding table. On ACX Series routers, per-flow load balancing can be performed to spread traffic across multiple paths between the routers.

  [*ACX Series Universal Access Router Configuration Guide*]

Related Documentation

- Changes in Default Behavior and Syntax in Junos OS Release 12.3X54 for ACX Series Routers on page 14
- Known Limitations in Junos OS Release 12.3X54 for ACX Series Routers on page 14
- Upgrade and Downgrade Instructions for Junos OS Release 12.3X54 for ACX Series Routers on page 25

Changes in Default Behavior and Syntax in Junos OS Release 12.3X54 for ACX Series Routers

This section lists the changes in default behavior and syntax in Junos OS Release 12.3X54 for ACX Series routers.

Interfaces and Chassis

- **Connectivity fault management MEPs on Layer 2 circuits and Layer 2 VPNs**—On interfaces configured on ACX Series routers, you no longer need to configure the **no-control-word** statement at either the **[edit protocols l2circuit neighbor *neighbor-id* interface *interface-name*]** or the **[edit routing-instances *routing-instance-name* protocols l2vpn]** hierarchy level for Layer 2 circuits and Layer 2 VPNs over which you are running CFM maintenance association end points (MEPs). This configuration is not needed because ACX Series routers support the control word for CFM MEPs. The control word is enabled by default.

  [*ACX Series Universal Access Router Configuration Guide*]

- In the output of the **show interfaces** command under the **MAC Statistics** section, any packet whose size exceeds the configured MTU size is considered as an oversized frame and the value displayed in the **Oversized frames** field is incremented. The value displayed in the **Jabber frames** field is incremented when a bad CRC frame size is between 1518 bytes and the configured MTU size.

- **Support for chained composite next hop in Layer 3 VPNs**—Next-hop chaining (also known as chained composite next hop) is a composition function that concatenates the partial rewrite strings associated with individual next hops to form a larger rewrite string that is added to a packet. To configure the router to accept up to one million Layer 3 VPN route updates with unique inner VPN labels, include the **l3vpn** statement at the **[edit routing-options forwarding-table chained-composite-next-hop ingress]** hierarchy level. The **l3vpn** statement is disabled by default.

Related Documentation

- New Features in Junos OS Release 12.3X54 for ACX Series Routers on page 3
- Known Limitations in Junos OS Release 12.3X54 for ACX Series Routers on page 14
- Upgrade and Downgrade Instructions for Junos OS Release 12.3X54 for ACX Series Routers on page 25

Known Limitations in Junos OS Release 12.3X54 for ACX Series Routers

The following software limitations currently exist in Juniper Networks ACX Series Universal Access Routers. The identifier following the descriptions is the tracking number in the Juniper Networks Problem Report (PR) tracking system.

Class of Service

- When the **rewrite-rules** statement is configured with the **dscp** or the **inet-precedence** options at the [**edit class-of-service interfaces**] hierarchy level, the expectation is that the DiffServ code point (DSCP) or IPv4 precedence rewrite rules take effect only on

IP packets. However, in addition to the IP packets, the DSCP or IPv4 rewrite takes effect on the IP header inside the Ethernet pseudowire payload as well. This is not applicable for ACX4000 router. [PR664062: This is a known limitation.]

- In an ACX4000 router, whenever the scheduling and shaping parameters of a port or any of its queues are changed, the entire scheduling configuration on the port is erased and the new configuration is applied. During the time when such a configuration change is taking place, the traffic pattern does not adhere to user parameters. It is recommended that the scheduling configurations are done much earlier before live traffic. [PR840313: This is a known limitation.]
- The VLAN packet loss priority (PLP) is incorrectly set when untagged VLAN frames are received on the ingress interface with DSCP or IP precedence classification enabled and the NNI (egress) interface does not contain IEEE 802.1p rewrite rules. [PR949524: This is a known limitation.]

CoS limitations on PPP and MLPPP interfaces—The following are the common and specific CoS limitations on PPP and MLPPP interfaces for ACX Series Universal Access Routers.

The following are the common limitations on PPP and MLPPP interfaces:

- Traffic loss is observed when a CoS configuration is changed.
- Scheduling and shaping feature is based on CIR-EIR model and not based on weighted fair queuing (WFQ) model.
- The minimum transmit rate is 32 Kbps and the minimum supported rate difference between transmit rate and shaping rate is 32 Kbps.
- Buffer size is calculated based on the average packet size of 256 bytes.
- **Low** and **High** are the only loss priority levels supported.
- The mapping between forwarding class and queue is fixed as follows:
  - **best-effort** is queue *0*
  - **expedited-forwarding** is queue *1*
  - **assured-forwarding** is queue *2*
  - **network-control** is queue *3*

The following are the specific CoS limitations on MLPPP interfaces:

- Percentage rate configuration is not supported for shaping and scheduling. Rate configuration is only supported in terms of bits per second.
- Buffer size is calculated based on a single member link (T1/E1) speed and is not based on the number of member links in a bundle.
- Supports only **transmit-rate exact** configuration without fragmentation-map. Shaping and priority will not be supported without fragmentation-map.

- If fragmentation-map configured, shaping is supported on forwarding class with different priorities. If two or more forwarding classes are configured with the same priority, then only **transmit-rate exact** is supported for the respective forwarding class.
- Supports only one-to-one mapping between a forwarding class and a multiclass. A forwarding class can only send traffic corresponding to one multiclass.

The following is the specific CoS limitation on PPP interfaces:

- The distribution of excess rate between two or more queues of same priority happens on a first-come first-served basis. The shaping rate configured on the respective queue remains valid.

Layer 2 Services

Limitations on Layer 2 bridging—The following Layer 2 bridging limitations apply for ACX Series Universal Access Routers:

- A bridge domain cannot have two or more logical interfaces that belong to the same physical interface.
- A bridge domain with dual VLAN ID tag is not supported.
- The following input VLAN map functions are not supported because the bridge domain should have a valid service VLAN ID after normalization:
  - **pop-pop** on double-tagged logical interface.
  - **pop** on a single-tagged logical interface.
  - VLAN map with VLAN ID value set to 0.
- **swap-push** and **pop-swap** VLAN map functions are not supported.
- The maximum number of supported input VLAN maps with TPID **swap** is 64.
- MAC learning cannot be disabled at the logical interface level.
- MAC limit per logical interface cannot be configured.
- All STP ports on a bridge domain must belong to the same MST (multiple spanning tree) instance.
- If a logical interface is configured with Ethernet bridge encapsulation with **push-push** as the input VLAN map, normalization does not work when single-tagged or double-tagged frames are received on the logical port. Untagged frames received on the logical interface are normalized and forwarded correctly.
- On a priority-tagged logical interface with the output VLAN map function **pop**, egress VLAN filter check does not work.
- Output VLAN map function **push** cannot work on a dual-tagged frame egressing a logical interface.
- In a bridge domain configured with **vlan-id** statement, when a dual-tagged frame enters a non-dual-tagged logical interface and exits a dual-tagged logical interface, the VLAN tags are not translated correctly at egress.

Limitations on integrated routing and bridging—The following are the limitations on integrated routing and bridging (IRB) for ACX Series Universal Access Routers.

At the IRB device level, the following limitations apply:

- Behavior aggregate (BA) classifiers are not supported
- Statistics are not supported.

On an IRB logical interface, the following limitations apply:

- Statistics and Layer 2 policers are not supported
- Only inet and iso families are supported

On an IRB logical interface family inet, the following limitations apply:

- Policer, rpf-check, and dhcp-client are not supported

When firewall is applied on an IRB logical interface family inet, the following limitations apply:

- Default (global) filters are not supported.
- Supports only accept, forwarding-class, and loss-priority actions.
- Supports only input filters

Firewall Filters

- Bridge family filters are supported on ACX Series routers. These filters can be scaled up to 124 hardware entries. Filter attachment at the bridge-domain level and port mirroring support will be added in a future release.
- In ACX Series routers, the following Layer 2 control protocols packet are not matched (with **match-all** term) by using the bridge family firewall filter applied on a Layer 2 interface:
  - Slow-Protocol/LACP MAC (01:80:c2:00:00:02)
  - E-LMI MAC ((01:80:c2:00:00:07)
  - IS-IS L2 MAC (01:80:c2:00:00:14/09:00:2B:00:00:14)
  - STP BPDU (01:80:c2:00:00:00)
  - VSTP BPDU (01:00:0C:CC:CC:CD)
  - LLDP/PTP (01:80:c2:00:00:0E)

  When layer rewrite is configured:

  - VTP/CDP (01:00:0C:CC:CC:CC)
  - L2PT RW MAC (01:00:0C:CD:CD:D0)
  - MMRP (01:80:C2:00:00:20)
  - MVRP (01:80:C2:00:00:21)

As a workaround, to match the Layer 2 control packet flows with a bridge family filter term, you must explicitly specify the destination MAC match (along with other MAC matches) in the firewall filter term and in the match term. [PR879105: This is a known software limitation.]

- In ACX Series routers, a firewall filter cannot be applied to a logical interface configured with **vlan-id-list** or **vlan-range**. As a workaround, you can configure the interface-specific statement, which can be applied to the **bridge**, **inet**, or **mpls** family firewall filter. [PR889182: This is a known software limitation.]
- In ACX Series routers, packet drops in the egress interface queue are also counted as *input packet rejects* under the **Filter statistics** section in the output of the **show interface input-interfaces extensive** command when the command is run on the ingress interface. [PR612441: This is a known software limitation.]
- When the **statistics** statement is configured on a logical interface—for example, [**edit interface name-X unit unit-Y**]; the (**policer** | **count** | **three-color-policer**) statements are configured in a firewall filter for the **family any**—for example, [**edit firewall family any filter filter-XYZ term term-T then**] hierarchy level; and the configured **filter-XYZ** is specified in the **output** statement of the logical interface at the [**edit interface name-X unit unit-Y filter**] hierarchy level, the counters from the configuration of another firewall family filter on the logical interface do not work. [PR678847: This is a known limitation.]
- The policing rate can be incorrect if the following configurations are applied together:
  - The **policer** or **three-color-policer** statement configured in a firewall filter—for example, **filter-XYZ** at the [**edit firewall family any filter filter-XYZ term term-T then**] hierarchy level, and **filter-XYZ** is specified as an ingress or egress firewall filter on a logical interface—for example, **interface-X unit-Y** at the [**edit interface interface-X unit unit-Y filter (input|output) filter-XYZ**] hierarchy level.
  - The **policer** or **three-color-policer** statement configured in a firewall filter—for example, **filter-ABC** at the [**edit firewall family name-XX filter filter-ABC term term-T then**] hierarchy level, and **filter-ABC** is configured as an ingress or egress firewall filter on a family of the same logical interface **interface-X unit-Y** at the [**edit interface interface-X unit unit-Y family name-XX filter (input|output) filter-ABC**] hierarchy level.

  NOTE: If one of these configurations is applied independently, then the correct policer rate can be observed.

  [PR678950: This is a known limitation.]

Interfaces and Chassis

- Egress maximum transmission unit (MTU) check value of an interface is different for tagged and untagged packets. If an interface is configured with CLI MTU value as *x*, then the following would be the checks depending on outgoing packet type:
  - Egress MTU value for unatagged packet = x – 4
  - Egress MTU value for single-tagged packet = x

- Egress MTU value for double-tagged packet = x + 4

NOTE: **The ingress MTU check is the same for all incoming packet types.**

There is no workaround available. [PR891770: This is a known limitation.]

- In ACX Series routers, when STP is configured on an interface, the detailed interface traffic statistics show command output does not show statistics information but displays the message **Dropped traffic statistics due to STP State**. However, the drop counters are updated. There is no workaround available. [PR810936: This is a known limitation.]
- When the **differential-delay** *number* option is configured in the **ima-group-option** statement at the [**edit interfaces at-***fpc/pic/ima-group-no*] hierarchy level, with a value less than 10, some of the member links might not come up and the group might remain down resulting in traffic loss. A workaround is to keep the differential delay value above 10 for all IMA bundles. [PR726279: This is a known limitation.]
- The ACX Series routers support logical interface statistics, but do not support the address family statistics. [PR725809: This is a known limitation.]
- BERT error insertion and bit counters are not supported by the IDT82P2288 framer. [PR726894: This is a known limitation.]
- All 4x supported TPIDs cannot be configured on different logical interfaces of a physical interface. Only one TPID can be configured on all logical interfaces of a physical interface. But different physical interfaces can have different TPIDs. As a workaround, use TPID rewrite. [PR738890: This is a known limitation.]
- The ACX Series routers do not support logical interface statistics for logical interfaces with **vlan-list** or **vlan-range** configured. [PR810973: This is a known limitation.]
- CFM up-MEP session (to monitor pseudowire service) does not come up when output VLAN map is configured as **push** on AC logical interface. This is due to hardware limitation in ACX4000 router. [PR832503: This is a known limitation.]
- For ATM interfaces with **atm-ccc-cell-relay** and **atm-ccc-vc-mux** encapsulation types configured, and with shaping profile configured on the interfaces, traffic drop is observed when the configured shaping profile is changed. This problem occurs with 16-port Channelized E1/T1 Circuit Emulation MICs on ACX4000 routers. As a workaround, you must stop the traffic on the Layer 2 circuit before changing any of the traffic shaping profile parameters. [PR817335: This is a known limitation]
- In the case of normalized bridge domain, with double-tagged aggregated Ethernet interface as ingress, the classification based on inner tag does not work for ACX4000. To do classification based on inner tag, configure the bridge domain with explicit normalization and configure input and output VLAN map to match the behavior. [PR869715: This is a known limitation.]
- The MAC counter behavior of 10-Gigabit Ethernet is different compared to 1-Gigabit Ethernet.

On 1-Gigabit Ethernet interfaces, if the packet size is greater than 1518 bytes, irrespective of whether the packet is tagged or untagged, the **Oversized** counter gets incremented. If the packet has a CRC error, then the **Jabber** counter gets incremented.

On 10-Gigabit Ethernet interfaces, if the packet is size is greater than 1518 bytes and the packet is untagged, then the **Oversized** counter gets incremented. If the packet has a CRC error, then the **Jabber** counter gets incremented.

If the packet is tagged (TPID is 0x8100), then the **Oversized** counter is incremented only if the packet size is greater than 1522 bytes (1518 + 4 bytes for the tag). The **Jabber** counter is incremented only if the packet size is greater than 1522 bytes and the packet has a CRC error.

The packet is considered as tagged if the outer TPID is 0x8100. Packets with other TPIDs values (for example, 0x88a8, 0x9100, or 0x9200) are considered as untagged for the counter. There is no workaround available. [PR940569: This is a known limitation.]

- Layer 2 RFC2544 benchmarking test cannot be configured to generate dual-tagged frames when the UNI interface is configured for the QnQ service. This occurs when the input VLAN map **push** is configured on the UNI interface. There is no workaround available. [PR946832: This is a known limitation.]
- After running RFC2544 tests, PTP stops working when the tests are performed on the same router. A workaround is to reboot FEB after running the RFC2544 tests. PR944200: This is a known limitation.]
- When an ACX1100 router with AC power is configured as PTP slave or boundary clock, the router does not achieve PTP accuracy within the specification (1.5 us), even if the PTP achieves the state **Phase Aligned**. [PR942664: This is a known limitation.]
- Layer 2 RFC2544 benchmark test fails for packet sizes 9104 and 9136 when the test bandwidth is less than 10-MB and the NNI interface link speed is 10-MB. This behavior is also seen when the 10-MB policer or shaper is configured on the NNI interface. The issue will not be seen if the egress queue is configured with sufficient queue buffers.[PR939622: This is a known limitation.]

Limitations on logical tunnel interfaces—The following limitations apply when you configure logical tunnel (LT) interfaces in ACX Series Universal Access Routers:

- ACX router supports a total of two LT interfaces in a system, one of bandwidth 1G and another of bandwidth 10G.
- The bandwidth configured on the LT interface is shared between upstream and downstream traffic on that interface. The effective available bandwidth for the service is half the configured bandwidth.
- Supported encapsulations on LT interface are **ethernet-bridge, ethernet-ccc, vlan-bridge, vlan-ccc**.
- Total number of LT logical interfaces supported on a router is 30.
- If an LT interface with bandwidth 1G is configured and port-mirroring is also configured on the router, then LT physical interface statistics may not be accurate for that LT interface.

- Default classifiers are not available on the LT interface if a non-Ethernet PIC is used to create the LT interface.
- LT interfaces do not support protocol configuration.

Statistics

- ACX Series routers do not support route statistics per next hop and per flow for unicast and multicast traffic. Only interface-level statistics are supported.
- The **show multicast statistics** command is not supported on ACX Series routers. [PR954273: This is a known limitation.]

MPLS Applications

- The scaling numbers for pseudowires and MPLS label routes published for the ACX Series routers are valid only when the protocols adopt graceful restart. In case of non-graceful restart, the scaling numbers would become half of the published numbers. [PR683581: This is a known limitation.]

Network Management

- In a connectivity fault management (CFM) up-mep session, when a remote-mep error is detected, the local-mep does not set the RDI bit in the transmitted continuity check messages (CCM). This problem is not seen in ACX4000 routers and in down-mep sessions. There is no workaround available. [PR864247: This is a known limitation.]
- The ACX Series routers do not support the configuration of RPM probes to a routing instance along with the configuration of the **hardware-timestamp** statement at the [**edit services rpm probe *owner* test *test-name***] hierarchy level. [PR846379: This is a known limitation.]

Timing and Synchronization

- When you use the **replace *pattern*** command to toggle from a secure slave to an automatic slave or vice versa in the PTP configuration of a boundary clock, the external slave goes into a freerun state. The workaround is to use the **delete** and **set** commands instead of the **replace *pattern*** command. [PR733276: This is a known limitation.]

Integrated Routing and Bridging

The following are the limitations on integrated routing and bridging (IRB) for ACX Series Universal Access Routers.

At the IRB device level, the following limitations apply:

- Behavior aggregate (BA) classifiers are not supported
- Statistics are not supported.

On an IRB logical interface, the following limitations apply:

- Statistics and Layer 2 policers are not supported

- Only inet and iso families are supported

On an IRB logical interface family inet, the following limitations apply:

- Policer, rpf-check, and dhcp-client are not supported

When firewall is applied on an IRB logical interface family inet, the following limitations apply:

- Default (global) filters are not supported.
- Supports only accept, forwarding-class, and loss-priority actions.
- Supports only input filters

Interface Limitations—IRB configurations supports a maximum of 1000 logical interfaces on a box.

Class-of-service Limitations—The following are CoS limitations for IRB:

- Maximum of 16 fixed classifiers are supported. Each classifier consumes two filter entries and is shared with RFC 2544 sessions. Total number of shared filter entries is 32.
- Maximum of 64 multifield filter classifiers are supported. Each classifier takes two filter entries. Total 128 entries are shared between family inet based classifiers on IRB and normal Layer 3 logical interfaces.
- Maximum 24 forwarding class and loss priority combinations can be rewritten. Each rewrite rule takes single entry from egress filters. Total of 128 entries are shared by rewrite-rules and all other output firewall filters.
- IRB rewrite is supported only on ACX 4000 Series router.

Firewall Limitations—The following are the firewall limitations for IRB:

- IRB supports only family inet filters.
- Only interface-specific and physical-interface specific filters are supported.
- Only forwarding-class and loss-priority actions are supported, other actions are not supported.

Related Documentation

- New Features in Junos OS Release 12.3X54 for ACX Series Routers on page 3
- Changes in Default Behavior and Syntax in Junos OS Release 12.3X54 for ACX Series Routers on page 14
- Upgrade and Downgrade Instructions for Junos OS Release 12.3X54 for ACX Series Routers on page 25

Errata and Changes in Documentation for Junos OS Release 12.3X54 for ACX Series Routers

- Errata on page 23
- Changes to the Junos OS ACX Documentation on page 24

Errata

- Support for multifield classifiers is incorrectly omitted from the ACX documentation. Multifield classifiers allow fine grained classification by examination of multiple fields in the packet header—for example, the source and destination address of the packet, and the source and destination port numbers of the packet. A multifield classifier typically matches one or more of the six packet header fields: destination address, source address, IP protocol, source port, destination port, and DSCP. Multifiled classifiers are used when a simple BA classifier is insufficient to classify a packet.

  In the Juniper Networks Junos operating system (Junos OS), you configure a multifield classifier with a firewall filter and its associated match conditions. This enables you to use any filter match criteria to locate packets that require classification. From a CoS perspective, multifield classifiers (or firewall filter rules) provide the following services:

  - Classify packets to a forwarding class and loss priority. The forwarding class determines the output queue. The loss priority is used by schedulers in conjunction with the random early discard (RED) algorithm to control packet discard during periods of congestion.
  - Police traffic to a specific bandwidth and burst size. Packets exceeding the policer limits can be discarded, or can be assigned to a different forwarding class, to a different loss priority, or to both.

  

  NOTE: You police traffic on input to conform to established CoS parameters, setting loss handling and forwarding class assignments as needed. You shape traffic on output to make sure that router resources, especially bandwidth, are distributed fairly. However, input policing and output shaping are two different CoS processes, each with their own configuration statements.

  To configure multifield classifiers, include the following statements at the [**edit firewall**] hierarchy level:

```
[edit firewall]
family family-name {
     filter filter-name {
          term term-name {
               from {
                    match-conditions;
               }
               then {
                    dscp 0;
                    forwarding-class class-name;
                    loss-priority (high | low);
               }
          }
     }
     simple-filter filter-name {
          term term-name {
               from {
                    match-conditions;
```

```
                }
                then {
                     forwarding-class class-name;
                     loss-priority (high | low | medium);
                }
           }
     }
}
```

The minimum configuration required to define a multifield classifier is the following:

```
[edit firewall]
family family-name {
     simple-filter filter-name {
          term term-name {
               then {
                    forwarding-class class-name;
                    loss-priority (high | low | medium);
               }
          }
     }
}
```

After defining the multified classifier, you can apply the multified classifier to an individual interface with the following configuration:

```
[edit interfaces]
interface-name{
     unit logical-unit-number{
          family family {
               filter {
                    input filter-name;
               }
          }
     }
}
```

[ACX Series Universal Access Router Configuration Guide]

- The *Configuring Load Balancing Based on MPLS Labels on ACX Series Routers* topic fails to explicitly state that load balancing using MPLS labels is supported only for aggregated Ethernet (ae) or LAG interfaces and not for equal-cost multipath (ECMP) links. To load-balance based on the MPLS label information for LAG interfaces, configure the **family mpls** statement at the **[edit forwarding-options hash-key]** hierarchy level.

  [*ACX Series Universal Access Router Configuration Guide*]

- In the *ACX2000 and ACX2100 DC Power Specifications* topic of the ACX2000 and ACX2100 Router Hardware Guide, the DC input voltages row in the table presented in the topic incorrectly mentions that the range is 18 to 30 VDC. The correct DC input voltage range for a nominal 24 volt operation is 20 to 30 VDC.

Changes to the Junos OS ACX Documentation

There are no changes to the ACX Documentation in Junos OS Release 12.3X54.

Related Documentation

- New Features in Junos OS Release 12.3X54 for ACX Series Routers on page 3
- Changes in Default Behavior and Syntax in Junos OS Release 12.3X54 for ACX Series Routers on page 14
- Known Limitations in Junos OS Release 12.3X54 for ACX Series Routers on page 14
- Upgrade and Downgrade Instructions for Junos OS Release 12.3X54 for ACX Series Routers on page 25

Upgrade and Downgrade Instructions for Junos OS Release 12.3X54 for ACX Series Routers

This section discusses the following topics:

Basic Procedure for Upgrading to Release 12.3X54

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

NOTE: Before upgrading, back up the file system and the currently active Junos configuration so that you can recover to a known, stable environment in case the upgrade is unsuccessful. Issue the following command:

```
user@host> request system snapshot
```

The installation process rebuilds the file system and completely reinstalls Junos OS. Configuration information from the previous software installation is retained, but the contents of log files might be erased. Stored files on the routing platform, such as configuration templates and shell scripts (the only exceptions are the **juniper.conf** and **ssh** files), might be removed. To preserve the stored files, copy them to another system before upgrading or downgrading the routing platform. For more information, see *Understanding System Snapshot on an ACX Series Router*.

The download and installation process for Junos OS Release 12.3X54 is different from previous Junos OS releases.

1. Using a Web browser, navigate to the **All Junos Platforms** software download URL on the Juniper Networks web page:

   http://www.juniper.net/support/downloads/

2. Select the name of the Junos platform for the software that you want to download.

3. Select the release number (the number of the software version that you want to download) from the **Release** drop-down list to the right of the Download Software page.
4. Select the **Software** tab.
5. In the **Install Package** section of the **Software** tab, select the software package for the release.
6. Log in to the Juniper Networks authentication system using the username (generally your e-mail address) and password supplied by Juniper Networks representatives.
7. Review and accept the End User License Agreement.
8. Download the software to a local host.
9. Copy the software to the routing platform or to your internal software distribution site.
10. Install the new **jinstall** package on the routing platform.

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

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

```
user@host> request system software add validate reboot
source/jinstall-ppc-12.3X54-D10.6-domestic-signed.tgz
```

All other customers use the following command:

```
user@host> request system software add validate reboot
source/jinstall-ppc-12.3X54-D10.6-export-signed.tgz
```

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

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

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

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

Rebooting occurs only if the upgrade is successful.

NOTE: After you install a Junos OS Release 12.3X54 jinstall package, you cannot issue the request system software rollback command to return to the previously installed software. Instead you must issue the request system software add validate command and specify the jinstall package that corresponds to the previously installed software.

Upgrade and Downgrade Support Policy for Junos OS Releases

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

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

Release 10.3 (a non-EEOL release) to Junos OS Release 11.4 or directly downgrade from Junos OS Release 11.4 to Junos OS Release 10.3.

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

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

Downgrade from Release

To downgrade from Release 12.3X54 to another supported release, follow the procedure for upgrading, but replace the 12.3X54 **jinstall** package with one that corresponds to the appropriate release.

NOTE: **You cannot downgrade more than three releases. For example, if your routing platform is running Junos OS Release 11.4, you can downgrade the software to Release 10.4 directly, but not to Release 10.3 or earlier; as a workaround, you can first downgrade to Release 10.4 and then downgrade to Release 10.3.**

For more information, see the *Installation and Upgrade Guide*.

Related Documentation

- New Features in Junos OS Release 12.3X54 for ACX Series Routers on page 3
- Changes in Default Behavior and Syntax in Junos OS Release 12.3X54 for ACX Series Routers on page 14
- Known Limitations in Junos OS Release 12.3X54 for ACX Series Routers on page 14

Junos OS Documentation and Release Notes

For a list of related Junos OS documentation, see http://www.juniper.net/techpubs/software/junos/.

If the information in the latest release notes differs from the information in the documentation, follow the *Junos OS Release Notes*.

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Juniper Networks supports a technical book program to publish books by Juniper Networks engineers and subject matter experts with book publishers around the world. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration using the Junos operating system (Junos OS) and Juniper Networks devices. In addition, the Juniper Networks Technical Library, published in conjunction with O'Reilly Media, explores improving network security, reliability, and availability using Junos OS configuration techniques. All the books are for sale at technical bookstores and book outlets around the world. The current list can be viewed at http://www.juniper.net/books.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document name
- Document part number
- Page number
- Software release version

Requesting Technical Support

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

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the JTAC User Guide located at http://www.juniper.net/customers/support/downloads/710059.pdf.
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/.

- JTAC Hours of Operation —The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

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

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- 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

18 July, 2014—Revision 1, Junos OS 12.3X54 – ACX Series Routers.