Junos® OS 12.3X54–D20 Release Notes

Release 12.3X54-d20
16 November, 2015
Revision 1

These release notes accompany Release 12.3X54–D20 of the Junos operating system (Junos OS) for Juniper Networks ACX Series Universal Access Routers. 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–D20 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, ACX2200, ACX4000, and ACX500 routers.

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

- High performance: Capable of providing up to 10-Gbps speed on Ethernet links
- Seamless MPLS traffic engineering for optimal paths and per-customer quality of service in the access layer
- Built-in Precision Timing Protocol (PTP) and Synchronous Ethernet to eliminate dropped calls and data retransmissions
- Environmentally hardened with 32–W Power over Ethernet (PoE) and 65-W Power over Ethernet Plus Plus (PoE++)

NOTE: **PoE is not supported on the ACX1000, ACX1100, ACX2100, ACX2200, ACX500-O-AC, and ACX500-O-DC routers.**

- Carrier Ethernet services

The following features have been added to Junos OS Release 12.3X54–D20 for the ACX Series Universal Access Routers. Following the description is the title of the manual or manuals to consult for further information:

Hardware

- **New ACX500 Universal Access Routers**—Starting in Release 12.3X54-D20, Junos OS supports the new ACX500 routers: ACX500-AC, ACX500-DC, ACX500-O-AC, ACX500-O-DC, ACX500-O-POE-AC, and ACX500-O-POE-DC. These routers enable a wide range of business and residential applications and services, including microwave

cell site aggregation, MSO mobile backhaul service cell site deployment, and service provider or operator cell site deployment. These ACX500 routers can be deployed as indoor or outdoor units. The ACX500 routers support the use of Gigabit Ethernet SFP transceivers and RJ-45 and PoE ports.

The ACX500 routers have the following variants:

- ACX500 Indoor small-cell router (model number: ACX500-AC, ACX500-DC)
- ACX500 outdoor small-cell router (model number: ACX500-O-AC, ACX500-O-DC)
- ACX500 outdoor small-cell router with PoE support (model number: ACX500-O-POE-AC, ACX500-O-POE-DC)

The key features of the ACX500 routers are as follows:

- Has an integrated GPS receiver
- Complies with IP65 environmental standard rating
- Supports advanced security features such as IP Security (IPsec) encryption, Network Address Translation (NAT) for IP addresses, and Media Access Control Security (MACsec)
- Supports Two-Way Active Measurement Protocol (TWAMP)
- Supports RFC2544-based benchmarking tests
- Has a fanless, conduction cooling design
- Environmentally temperature hardened to operate between –40° C and +65° C
- Supports PoE (ACX500-O-POE-AC and ACX500-O-POE-DC)
- Deployable on utility, telephone, or electrical poles, and on standard side walls (ACX-O-AC, ACX-O-DC, ACX-O-POE-AC, and ACX-O-POE-AC)

Software

- **Support for PTP grandmaster clock**—Starting in Release 12.3X54–D20, Junos OS supports the PTP grandmaster clock functionality on ACX500 routers. For an ACX500 router to act as a PTP grandmaster clock, the router needs to receive the timing information from a GPS receiver.

  [*ACX Series Universal Access Router Configuration Guide*]

- **PHY timestamping for grandmaster clock**—Starting in Release 12.3X54–D20, Junos OS for ACX Series Universal Access Routers supports timestamping at the physical layer, also known as PHY timestamping, for the grandmaster clock. To enable PHY timestamping on ACX Series routers, configure **clock-mode** (ordinary clock, boundary clock, or grandmaster clock) along with the **transparent-clock** statement at the [**edit protocols ptp**] hierarchy level.

  [*ACX Series Universal Access Router Configuration Guide*]

- **Integrated Global Navigation Satellite System (GNSS)**—Starting in Release 12.3X54–D20, Junos OS for ACX500 line of routers supports the integrated GNSS receiver, eliminating the need for an external GPS receiver. However, you still need a

GPS antenna. The ACX500 line of routers support GNSS input through the SubMiniature version A (SMA) connector. You can configure the GNSS port and its associated parameters at the [**edit chassis synchronization**] hierarchy level. You can configure the GNSS port by including the **constellation** [**gps | glonass | gps-and-glonass**] CLI statement at the [**edit chassis synchronization port gnss**] hierarchy level. If you do not specify a constellation option, then the **gps** constellation option is considered by default.

[*ACX Series Universal Access Router Configuration Guide*]

- **Support for dynamic ternary content addressable memory (TCAM)**—Starting in Release 12.3X54–D20, Junos OS for ACX Series Universal Access Routers supports the dynamic allocation of TCAM space that efficiently allocates the available TCAM resources for various filter applications. In the dynamic TCAM model, various filter applications (such as IPv4 firewall, bridge firewall, CFM filters, and so on) can optimally utilize the available TCAM resources as and when required. Dynamic TCAM resource allocation is usage driven and the resources are dynamically allocated for filter applications as required. When a filter application no longer uses the TCAM space, the resource is freed and made available for use by other applications. This dynamic TCAM model caters to a higher scale of TCAM resource utilization based on an application's demand.

  [*ACX Series Universal Access Router Configuration Guide*]

- **Support for 4096 network address or port translations**—Starting in Release 12.3X54–D20, Junos OS for ACX Series Universal Access Routers supports up to 4096 network address or port translations at a time.

  [*ACX Series Universal Access Router Configuration Guide*]

- **Ethernet loopback support for RFC 2544-based benchmarking test**—Starting in Release 12.3X54–D20, Junos OS for ACX Series Universal Access Routers supports configuring Ethernet loopback for performing the RFC 2544-based benchmarking test. Ethernet loopback can be used for verifying the connectivity and identifying or isolating faults in a network. This feature can be used for performance measurements where packets are looped back to measuring device. Ethernet loopback on ACX Series routers is supported in the egress user-to-network interface (UNI) direction for a **bridge** family configuration. In ACX Series routers, Ethernet loopback is associated with logical interfaces.

  [*ACX Series Universal Access Router Configuration Guide*]

- **Existing ACX Series feature support in ACX500 router**—Starting in Release 12.3X54-D20, Junos OS for ACX500 Universal Access Router also supports the following ACX Series router features:

  - Layer 2 and Layer 3 routing
  - Class of service (CoS)
  - Firewall filters
  - Operation, Administration, and Maintenance (OAM)
  - Precision Timing Protocol (PTP) and synchronous Ethernet
  - MPLS

[*ACX Series Universal Access Router Configuration Guide*]

Related Documentation

- Changes in Default Behavior and Syntax in Junos OS Release 12.3X54–D20 for ACX Series Routers on page 6
- Known Limitations in Junos OS Release 12.3X54–D20 for ACX Series Routers on page 7
- Upgrade and Downgrade Instructions for Junos OS Release 12.3X54–D20 for ACX Series Routers on page 17

Changes in Default Behavior and Syntax in Junos OS Release 12.3X54–D20 for ACX Series Routers

This section lists the changes in default behavior and syntax in Junos OS Release 12.3X54–D20 for ACX Series routers.

- Interfaces and Chassis on page 6

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–D20 for ACX Series Routers on page 3
- Known Limitations in Junos OS Release 12.3X54–D20 for ACX Series Routers on page 7
- Upgrade and Downgrade Instructions for Junos OS Release 12.3X54–D20 for ACX Series Routers on page 17

Known Limitations in Junos OS Release 12.3X54–D20 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** option 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 affecting 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 an 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. We recommend that the scheduling configurations be 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 the CIR-EIR model and not based on the 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 supported only in terms of bits per second.
- Buffer size is calculated based on the speed on a single member link (T1/E1) 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 are not supported without **fragmentation-map**.
- If **fragmentation-map** is configured, shaping is supported on forwarding classes 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 send traffic corresponding to only one multiclass.

The following is the specific CoS limitation on PPP interfaces:

- The distribution of excess rate between two or more queues of the same priority happens in the order in which the queues arrive. 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 a 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 exiting a logical interface.
- In a bridge domain with the **vlan-id** statement configured, 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.

Firewall Filters

- ACX Series routers support **bridge** family filters. These filters can be scaled up to 124 hardware entries.
- In ACX Series routers, the following Layer 2 Control Protocol packets 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 are the checks depending on outgoing packet type:
  - Egress MTU value for untagged 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 Spanning Tree Protocol (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.]
- The CFM up-MEP session (to monitor pseudowire service) does not come up when output VLAN map is configured as **push** on a logical interface. This is due to hardware limitation in the 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 the 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 a normalized bridge domain, with double-tagged aggregated Ethernet interface as ingress, the classification based on inner tag does not work for ACX4000. To make the classification based on inner tag work, 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 that of 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 untagged for the counter. There is no workaround available. [PR940569: This is a known limitation.]

- Layer 2 RFC 2544-based benchmarking test cannot be configured to generate dual-tagged frames when the UNI interface is configured for the Q-in-Q 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 RFC 2544-based benchmarking 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-based benchmarking 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 is not 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 interfaces on ACX Series Universal Access Routers:

- The router supports a total of two logical tunnel interfaces in a system, one of bandwidth 1 Gbps and another of bandwidth 10 Gbps.
- The bandwidth configured on the logical tunnel interface is shared between upstream and downstream traffic on that interface. The effective available bandwidth for the service is half the configured bandwidth.
- The supported encapsulations on logical tunnel interfaces are **ethernet-bridge, ethernet-ccc, vlan-bridge**, and **vlan-ccc**.
- The total number of logical tunnel logical interfaces supported on a router is 30.
- If a logical tunnel interface with bandwidth 1 Gbps is configured and port mirroring is also configured on the router, then logical tunnel physical interface statistics might not be accurate for that logical tunnel interface.
- Default classifiers are not available on the logical tunnel interface if a non-Ethernet PIC is used to create the logical tunnel interface.
- Logical tunnel 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 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.]
- An ACX500 router, acting as PTP grandmaster, intermittently fails maximum time interval error (MTIE) and time deviation (TDEV) requirements of the grandmaster clock for long duration tests. [PR1039424: 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 filters are applied on an IRB logical interface family **inet**, the following limitations apply:

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

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:

- A maximum of 16 fixed classifiers are supported. Each classifier consumes two filter entries and is shared with RFC 2544 sessions. The total number of shared filter entries is 32.
- A maximum of 64 multifield filter classifiers are supported. Each classifier takes two filter entries. A total of 128 entries are shared between family **inet** based classifiers on IRB and normal Layer 3 logical interfaces.
- A maximum of 24 forwarding class and loss priority combinations can be rewritten. Each rewrite rule takes a single entry from egress filters. A total of 128 entries are shared by rewrite rules and all other output firewall filters.
- IRB rewrite is supported only on the ACX4000 Series router.

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

- IRB supports only family **inet** filters.
- Only 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–D20 for ACX Series Routers on page 3
- Changes in Default Behavior and Syntax in Junos OS Release 12.3X54–D20 for ACX Series Routers on page 6
- Upgrade and Downgrade Instructions for Junos OS Release 12.3X54–D20 for ACX Series Routers on page 17

Errata and Changes in Documentation for Junos OS Release 12.3X54–D20 for ACX Series Routers

- Errata on page 15
- Changes to the Junos OS ACX Documentation on page 16

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–D20.

Related Documentation

- New Features in Junos OS Release 12.3X54–D20 for ACX Series Routers on page 3
- Changes in Default Behavior and Syntax in Junos OS Release 12.3X54–D20 for ACX Series Routers on page 6
- Known Limitations in Junos OS Release 12.3X54–D20 for ACX Series Routers on page 7
- Upgrade and Downgrade Instructions for Junos OS Release 12.3X54–D20 for ACX Series Routers on page 17

Upgrade and Downgrade Instructions for Junos OS Release 12.3X54–D20 for ACX Series Routers

This section discusses the following topics:

- Basic Procedure for Upgrading to Release 12.3X54–D20 on page 17
- Upgrade and Downgrade Support Policy for Junos OS Releases on page 19
- Downgrade from Release on page 20

Basic Procedure for Upgrading to Release 12.3X54–D20

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*.

On ACX Series router, you can take a snapshot of the existing Junos OS by inserting an external USB storage device and executing the **request system snapshot slice alternate** command. This command takes a snapshot of the current running Junos OS on to the external USB storage device.

The download and installation process for Junos OS Release 12.3X54–D20 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-D20.9-domestic-signed.tgz
```

All other customers use the following command:

```
user@host> request system software add validate reboot
source/jinstall-ppc-12.3X54-D20.9-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–D20 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–D20 to another supported release, follow the procedure for upgrading, but replace the 12.3X54–D20 **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–D20 for ACX Series Routers on page 3
- Changes in Default Behavior and Syntax in Junos OS Release 12.3X54–D20 for ACX Series Routers on page 6
- Known Limitations in Junos OS Release 12.3X54–D20 for ACX Series Routers on page 7

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

16 November, 2015—Revision 1, Junos OS 12.3X54–D20 – ACX Series Routers.