

Junos[®] OS Release 15.1X54–D60 Release Notes

Release 15.1X54–D60
5 December, 2016
Revision 1

These release notes accompany Release 15.1X54–D60 of the Junos operating system (Junos OS) for Juniper Networks ACX5000 Universal Access Routers. They describe device documentation and known problems with the software. Junos OS runs on all 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	3
New Features in Junos OS Release 15.1X54–D60 for ACX Series Routers	3
Software	4
Known Limitations in Junos OS Release 15.1X54–D60 for ACX Series Routers	6
Interfaces and Chassis	6
Class of Service	8
VPN	8
VPLS	8
Firewall	9
Operations Administration and Maintenance	9
ISSU	10
Transparent Clock	10
Messages	10
Errata and Changes in Documentation for Junos OS Release 15.1X54–D60 for ACX Series Routers	13
Errata	13
Changes to the Junos OS ACX Documentation	14

Upgrade and Downgrade Instructions for Junos OS Release 15.1X54-D60 for ACX Series Routers	15
Basic Procedure for Upgrading to Release 15.1X54-D60	15
Upgrade and Downgrade Support Policy for Junos OS Releases	17
Junos OS Documentation and Release Notes	19
Documentation Feedback	19
Requesting Technical Support	19
Revision History	21

Junos OS Release Notes for ACX Series Routers

- [New Features in Junos OS Release 15.1X54–D60 for ACX Series Routers on page 3](#)
- [Known Limitations in Junos OS Release 15.1X54–D60 for ACX Series Routers on page 6](#)
- [Errata and Changes in Documentation for Junos OS Release 15.1X54–D60 for ACX Series Routers on page 13](#)
- [Upgrade and Downgrade Instructions for Junos OS Release 15.1X54–D60 for ACX Series Routers on page 15](#)

New Features in Junos OS Release 15.1X54–D60 for ACX Series Routers

Powered by Junos OS, the ACX5000 Universal Access Routers are low-cost, high-density, high-capacity, low-power consumption aggregation routers that support 1-Gigabit Ethernet, 10-Gigabit Ethernet, and 40-Gigabit Ethernet interfaces and provide E-LINE, E-LAN, and IP-VPN services for Metro and Carrier Ethernet aggregation environments. The ACX5000 routers are available in AC and DC power variants.

The following are the key features of the ACX5048 router:

- Forty-eight 10-Gigabit Ethernet SFP+ ports that can be configured as 1-Gigabit Ethernet ports that support 1-gigabit small form-factor pluggable transceivers (SFP)
- Six 40-Gigabit Ethernet ports with quad form-factor pluggable plus transceivers (QSFP+)
- Aggregate throughput of up to 1.44 Tbps
- Maximum power requirement of up to 350 W (with optical SFPs)
- Supports channelized 40-Gigabit Ethernet interfaces to 10-Gigabit Ethernet interfaces



NOTE: You can configure one 40-Gigabit Ethernet interface to be channelized into four 10-Gigabit Ethernet interfaces.

The following are the key features of the ACX5096 router:

- Ninety-six 10-Gigabit Ethernet SFP+ ports that can be configured as 1-Gigabit Ethernet ports and support 1-gigabit small form-factor pluggable transceivers (SFP)
- Eight 40-Gigabit Ethernet ports with quad form-factor pluggable plus transceivers (QSFP+)
- Aggregate throughput of up to 2.56 Tbps
- Maximum power requirement of up to 550 W (with optical SFPs)
- Supports channelized 40-Gigabit Ethernet interfaces to 10-Gigabit Ethernet interfaces

**NOTE:**

- You can configure one 40-Gigabit Ethernet interface to be channelized into four 10-Gigabit Ethernet interfaces.
- When channelizing the 40-Gigabit Ethernet interfaces on the ACX5096 router, the router's Packet Forwarding Engine is expected to reboot.

The following features have been added to Junos OS Release 15.1X54–D60 for the ACX5000 line of universal access routers. Following the description is the title of the manual or manuals to consult for further information:

- [Software on page 4](#)

Software

- **Mesh group for VPLS routing**—Starting in Release 15.1X54–D60, Junos OS for ACX5000 Universal Access Routers supports mesh group configuration for VPLS routing instance. A mesh group within the routing instance is a group of PE interfaces members with common forwarding attributes. The following are the default member attributes in a mesh group:
 - **no-local-switching**—Traffic will not switch between members of the same mesh group (known-unicast, multicast, broadcast, unknown-unicast).
 - **flood-to-all-other-mesh-group**—Traffic can flow from a member of one mesh group to any set of members of other mesh-groups.

You can configure mesh group and its attributes at the `[edit routing-instances routing-instance-name protocols vpls]` hierarchy level as shown below:

```
mesh-group mesh-group-name {
  local-switching;
  mac-flush [ explicit-mac-flush-message-options ];
  neighbor address {...}
  peer-as all;
  pseudowire-status-tlv;
  route-distinguisher (as-number:id | ip-address:id);
  vpls-id number;
  vrf-export [ policy-names ];
  vrf-import [ policy-names ];
  vrf-target {
    community;
    import community-name;
    export community-name;
  }
}
```



NOTE: The maximum number of user-defined mesh groups in a single VPLS routing instance is 8.

[ACX Series Universal Access Router Configuration Guide]

- **Support for In-Service Software Upgrade (ISSU)**—Starting in Release 15.1X54–D60, Junos OS for ACX5000 Universal Access Routers supports ISSU, the ability to do software upgrades between two different software releases with minimal disruption to network traffic and no disruptions in the control plane.

As a prerequisite, you need to have the graceful Routing Engine switchover (GRES), nonstop active routing (NSR), and nonstop bridging (NSB) enabled in the routing engine to support ISSU on ACX5000 line of routers.

To understand how ISSU works, see

http://www.juniper.net/techpubs/en_US/junos15.1/topics/concept/issu-oveview.html

[*ACX Series Universal Access Router Configuration Guide*]

- **Support for remote loop-free alternate (LFA) over LDP tunnels in IS-IS and OSPF networks**—Starting in Release 15.1X54–D60, Junos OS for ACX5000 Universal Access Routers supports remote LFA over LDP tunnels in an IS-IS and OSPF network. Remote LFA increases the backup coverage for IS-IS and OSPF routes and provides protection especially for Layer 1 metro-rings. The IS-IS protocol creates a dynamic LDP tunnel to reach the remote LFA node from the point of local repair (PLR). The PLR uses this remote LFA backup path when the primary link fails.

[*ACX Series Universal Access Router Configuration Guide*]

- **Support for pseudowire cross-connect**—Starting in Release 15.1X54–D60, Junos OS for ACX5000 Universal Access Routers supports pseudowire cross-connect. The pseudowire cross-connect feature enables virtual circuit (VC) to terminate locally on a router and supports local switching of Layer 2 circuits. Layer 2 circuits allows the creation of point-to-point Layer 2 connections over an IP and MPLS-based network. Physical circuits with the same Layer 2 encapsulations can be connected together across such a network.

ACX5000 line of routers supports VLAN and Ethernet encapsulations. VLAN map operations are supported on logical interfaces. Multiple logical interfaces of the same physical interface can be cross-connected.

You can terminate a Layer 2 circuit locally on an ingress PE router. To configure a locally terminated circuit, include the **local-switching** statement at the [edit protocols l2circuit] hierarchy level. Select the Layer 2 circuit interfaces you want to connect locally, specify any APS protect interfaces, and configure an end interface.

To select the Layer 2 circuit interfaces that are connected locally, include the **interface** statement at the [edit protocols l2circuit local-switching] hierarchy level.

To configure an end interface, include the **end-interface** statement at the [edit protocols l2circuit local-switching interface *interface-name*] hierarchy level.

To specify APS protect interfaces, include the **protect-interface** statement at the [edit protocols l2circuit local-switching interface *interface-name*] or at the [edit protocols l2circuit local-switching interface *interface-name* end-interface *interface-name*] hierarchy levels.

[*ACX Series Universal Access Router Configuration Guide*]

- **Support for hot-standby option for pseudowire redundancy**—Starting in Release 15.1X54–D60, Junos OS for ACX5000 Universal Access Routers supports to configure

pseudowire (Layer 2 circuit) redundancy where Layer 2 and Layer 3 segments are interconnected. Configure pseudowire to the specified backup neighbor as the **hot-standby**. When you configure the **hot-standby** statement, traffic flows over both the active and hot-standby pseudowires to the backup device (either a CE device or PE router). The backup device drops the traffic from the hot-standby pseudowire, unless the active pseudowire fails. If the active pseudowire fails, the backup device automatically switches to the hot-standby pseudowire. The pseudowire status-tlv is used to communicate the status of a pseudowire back and forth between two PE routers. The pseudowire status-tlv is configurable for each pseudowire connection and is disabled by default.

[*ACX Series Universal Access Router Configuration Guide*]

- **Support for automatic bandwidth allocation for label-switched paths (LSPs)**—Starting in Release 15.1X54-D60, Junos OS for ACX5000 Universal Access Routers supports automatic bandwidth allocation for LSPs. Automatic bandwidth allocation allows an MPLS tunnel to automatically adjust its bandwidth allocation based on the volume of traffic flowing through the tunnel. You can configure an LSP with minimal bandwidth, and this feature can dynamically adjust the LSP's bandwidth allocation based on current traffic patterns. The bandwidth adjustments do not interrupt traffic flow through the tunnel.

To enable automatic bandwidth allocation on an LSP, include the **auto-bandwidth** CLI statement at the [**edit protocols mpls**] hierarchy level.

To collect statistics related to automatic bandwidth, include the **auto-bandwidth** CLI statement at the [**edit protocols mpls statistics**] hierarchy level.

Related Documentation

- [Known Limitations in Junos OS Release 15.1X54-D60 for ACX Series Routers on page 6](#)
- [Upgrade and Downgrade Instructions for Junos OS Release 15.1X54-D60 for ACX Series Routers on page 15](#)

Known Limitations in Junos OS Release 15.1X54-D60 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.

Interfaces and Chassis

- The counters for oversized frames and jabber frames does not increment properly. This happens in the case of a tagged interface for a packet size between 1519 and 1522 bytes. [PR1060169](#)

- A commit error is not seen while configuring channelization in the following scenario:

If you configure channelization on a port, the configuration should throw a commit error when the channelization on the port is configured individually and as well as configured as a part of port-range as shown below:

```
[edit chassis]
fpc 0 {
  pic 0 {
```

```

    port 53 {
      channel-speed 10g;
    }
    port 54 {
      channel-speed 10g;
    }
    port-range 53 54 {
      channel-speed 10g;
    }
  }
}

```

PR1051245

- On ACX5000 routers, whenever a **force switch** command is issued on the ring protection link, the status of ring protection link shows unblocked. This happens when ERPS is in idle state. [PR1070583](#)
- When you configure VRRP on ACX5000 routers, the master router gets toggled on IRB interfaces. [PR1131595](#)
- On ACX5000 router, the Integrated Routing and Bridging (IRB) interface goes down whenever you delete a data channel VLAN from an ERPS RPL owner followed by Forwarding Engine Board (FEB) restart. [PR1135534](#)
- Whenever you make a configuration change to the VLAN ID on a logical interface having **vlan-id-list** encapsulation, the output stats shows incorrect information. [PR1176530](#)
- When ACX5000 Series router is acting as an label-switching router (LSR),
 - Traffic belonging to same CCC/VPLS pseudowire cannot be load balanced based on L2/L3/L4 fields.
 - Traffic belonging to multiple CCC pseudowire sessions can be load balanced but traffic belonging to multiple VPLS pseudowire sessions cannot be load balanced.

PR1181853

- Whenever a node failure occurs, a high IPv6 traffic loss is seen even with BGP PIC. [PR1191304](#)
- A high traffic loss is seen during reversion in ring topologies when BGP PIC and remote LFA are configured together. [PR1210479](#)
- Whenever you add or delete the statistics knob, stale entries are seen under the AE logical interface. [PR1212392](#)
- Whenever you deactivate and activate an AE interface, an ambiguous behavior is seen with the AE input and output stats. [PR1204427](#)
- The status display for Layer 2 circuit connection protection with local switching (show l2circuit connection) is not correct for standby while protection is active, that is when the main link is down and switchover happened to backup neighbor. This has no functionality impact [PR1202445](#)

Class of Service

- When the **show class-of-service scheduler-map** CLI command is run, the output does not show the drop profiles attached to a non-TCP traffic. Drop profiles attached to only TCP traffic are displayed. [PR1048408](#)
- Weighted random early detection (WRED) profiles do not have any effect on multicast, unknown unicast, broadcast, and mirrored packets. WRED profiles affect only queue tail drops.
- ACX5048 and ACX5096 routers do not support DSCP classification for MPLS packets received from core on routing instance configured with BGP for per-prefix-label.
- On ACX5048 and ACX5096 routers, whenever scheduler parameters are changed while the traffic is flowing with shaping applied, the entire traffic on the egress physical interface is blocked temporarily.
- When the **show class-of-service interface *interface-name*** CLI command is run, the output may not display the classifier bound to an interface. You can instead use the request PFE execute command **show cos classifier bindings target fpc0** to see the classifier bindings for the interfaces present on the device. This has no impact to the BA classifier functionality. [PR1224777](#)

VPN

- When the router restores from fast reroute (FRR) link failures, less than 1 millisecond traffic loss is seen on few Layer 3 VPNs. [PR1017210](#)

VPLS

- When the **show vpls statistics** CLI command is run, the statistics for various output fields show value as 0. [PR1057240](#)
- The **ping vpls** CLI command is not supported on ACX5048 and ACX5096 routers. [PR1065202](#)
- The shaping rate for VPLS flood cases with bidirectional traffic does not work correctly. [PR1078664](#)
- When a VLAN tagged traffic is sent on a logical interface with Ethernet-VPLS encapsulation configured, only single VLAN tagged traffic is received instead of dual tagged traffic. This occurs when you configure Ethernet-VPLS encapsulation and VLAN-VPLS encapsulation on logical interfaces that are part of a VPLS routing instance configured with `vlan-id none`. [PR1100255](#)
- Load balancing does not work at LSR with multiple CCC/VPLS sessions. [PR1198435](#)
- Failover times are high for MPLS services when fiber pullout is carried to verify the convergence. [PR1214958](#)
- For the traffic flow that enters a VPLS NNI interface and goes out of another VPLS NNI interface, the output statistics on the outgoing NNI logical interface may not reflect correct or expected value. [PR1188104](#)

Firewall

- When you configure firewall on a logical interface with **native-vlan-id** configured, the configuration might erroneously match the traffic on other logical interfaces on the same physical interface. [PR1048860](#)
- On ACX5000 Series routers, **family any** egress filter will not match MPLS (VPWS/VPLS) packets. [PR1100698](#)

Operations Administration and Maintenance

- Customer edge (CE-to-CE) link fault management (LFM) session does not come up on circuit cross-connect (CCC) logical interface configured with **native-vlan** and input (push-pop) VLAN map operation. [PR1044997](#)
- When a bridge domain interface is configured with explicit VLAN map (input or output), maintenance association intermediate point (MIP) cannot be configured. [PR1058393](#)
- If you make any changes to the COS configuration after the CFM (OAM) session is up then those changes will not have any effect on the CCM (OAM) packets generated from the device. The workaround is to deactivate and activate the OAM protocol for the COS configuration changes to take effect. [PR1054908](#)
- In ACX5000 line of routers, if you configure CFM UP MEP over Layer 2 circuit, the continuity check messages (CCM) will not be transmitted causing the peer router to remain in a failed state. This issue might occur if you had configured both layer 2 circuit and CFM together and committed them at the same time. To avoid this issue, you need to first configure Layer 2 circuit and commit the configuration and then add the CFM configuration and commit the configuration. As a workaround, you need to deactivate and activate the failed OAM sessions.



NOTE: You might also notice this issue after upgrading to 15.1X54-D50.13 image. In this case, it is recommended to run the **restart ethernet-connectivity-fault-management** CLI command after upgrading or rebooting the router.

[PR1161699](#)

- Whenever you enable or disable main link interfaces, an ambiguous behavior is seen with the scale of 10 connection-protection sessions. [PR1214551](#)
- When the main link is down and the VLAN map operation is applied on the start interface, then traffic flow is blocked on the egress direction of the start interface. [PR1213434](#)
- CFM is not working on VPLS logical interface when input VLAN map push is configured. [PR1204532](#)

ISSU

- CFM session goes to a START state during ISSU upgrade. You need to deactivate the CFM session before initiating ISSU and reactivate the CFM session after completing ISSU. This is applicable for both single interface and AE interface. [PR1214869](#) and [PR1228096](#)
- Minimal IPv4 multicast traffic loss (approximately 50 milliseconds) is seen after ISSU. [PR1199964](#)
- VPLS with firewall and OAM is not compatible with ISSU. You need to deactivate all VPLS firewall or OAM configurations before initiating the ISSU process and then reactivate those configurations after completing the ISSU process. [PR1213891](#)
- Automatic bandwidth adjustment resets the LSP bandwidth to 0 during ISSU FPC WARM BOOT. You need to deactivate the autobandwidth functionality during ISSU and then reactivate it after completing ISSU. [PR1214805](#)

Transparent Clock

- When transparent clock is configured in the router and when the router resumes after reboot, the transparent clock status is shown as **ENABLED** and **ACTIVE**, instead of **ENABLED** and **INACTIVE**. This condition is transient and has no functional impact.

```
user@host# run show ptp global-information
PTP Global Configuration:
Transparent-clock-config : ENABLED
Transparent-clock-status : ACTIVE
```

[PR1051500](#)

- When you run the **restart clksyncd-service** CLI command, incorrect correction field values are seen when transparent clock is **INACTIVE**. This does not have any functional impact. [PR1067583](#)
- When transparent clock is in **ENABLED** or **DISABLED** state and if you try to add, delete, or modify any of the interfaces, the transparent clock **ENABLED** or **DISABLED** messages are seen in the packet forwarding engine (PFE). This does not have any functional impact. [PR1069516](#)
- Whenever an AE-based pseudowire flaps, the following messages are seen:

```
Ju1 2 14:37:14 acx5k11-dc fpc0
ACX_COS_HALP(acx_cos_classifier_type_bind_svp:2218): Classifier bind to IFL 559
failed
Ju1 2 14:42:52 acx5k11-dc fpc0
ACX_COS_HALP(acx_cos_bind_classifier_dscp_ifl_pvt:2288): bcm_port_dscp_map_set()
API ERROR : Entry not found
```

This does not have any functional impact. [PR1102004](#)

Messages

- The following error message is seen whenever the PFE is restarted:

```
LOG: Err] PORTDEV: OPTIC State changed for port
```

This does not have any functional impact. [PR1066899](#)

- The following error message is seen in the PFE when **firewall family ccc filter** scale is reached:

```
LOG: Info] ipc_pipe_write_wait(): Failed! (broken pipe)
```

This does not have any functional impact. [PR1098169](#)

- The following error message is seen when multiple MPLS service scale configuration is replaced with another multiple MPLS service scale configuration:

```
LOG: Err]
ACX_NH::acx_nh_mpls_tunnel_uninstall(),1142:acx_nh_mpls_tunnel_uninstall:
BCM L3 Egress destroy object failed for (-10:Operation still running),
BCM NH Obj: 0x1875a
```

This does not have any functional impact. [PR1093326](#)

- An error message is seen when aggregated Ethernet interface configuration is removed from the VPLS service. This does not have any functional impact. [PR1090923](#)
- The following messages are seen when the MPLS label-switched path (LSP) configurations are removed at scale:

```
LIBJSNMP_NS_LOG_NOTICE: NOTICE: Dropping Trap - Defer send disabled
```

This does not have any functional impact. [PR1077913](#)

- The following messages are seen when you enable fixed classification on IRB:

```
Jul 30 10:46:01 acx5k11-dc cosd[1606]: COSD_GENCFG_WRITE_FAILED: GENCFG
write failed (op, minor_type) = (add, fixed classification) for tbl 2 if
555 irb.1 Reason: File exists
```

This does not have any functional impact. [PR1109259](#)

- The following messages are seen when a Layer 3 interface (family inet) is converted to a Layer 2 interface (family Ethernet switching) with IRB:

```
Sun Feb 14 17:29:39.335 LOG: Err]
ACX_NH::acx_nh_composite_mcast_uninstall(),418:acx_nh_composite_mcast_uninstall:
nh 1739 Couldn't create multicast group: (-10:Operation still running)
```

```
[Sun Feb 14 17:29:39.336 LOG: Err] nh_composite_delete:3773Failed to uninstall
composite nh:1739
```

```
[Sun Feb 14 17:29:39.338 LOG: Err] nh_composite_delete:3773Failed to uninstall
composite nh:1742
```

This does not have any functional impact. [PR1126002](#)

- If you make any modification to a logical interface configured with **vlan-id-list** or **vlan-id-range** encapsulation, the output shows incorrect statistics.

[PR1158493](#) and [PR1176530](#)

- If you have configured label-switched paths (LSPs) as OSPF neighbors and you try to run the **show snmp mib walk decimal 1.3.6.1.2.1.14** CLI command, you will get the following message in the output and the command stops abruptly.

```
Request failed: OID not increasing: ospfNbrIpAddress.192.168.100.7.0 >=
ospfNbrIpAddress.192.168.100.7.0
```

PR1177315

- The following error messages are seen on the PFE during ISSU:

```
[Wed Sep 14 11:28:24.096 LOG: Err] CLKSYNC: Master closed connection
[Wed Sep 14 11:28:24.096 LOG: Err] CLKSYNC: Master socket closed, 0x1f955350
```

This does not have any functional impact. [PR1185856](#)

- The following error messages are seen on the PFE when IPv6 routes are scaled to 6100 routes, which is host route and Link Management Protocol (LMP) route (12200 routes in total):

```
[Fri Jul 29 05:52:15.066 LOG: Err] Failed to h/w update ip uc route entry
(status: 1000)
[Fri Jul 29 05:52:15.066 LOG: Err] Failed to install the RT entry (status:
1000)
[Fri Jul 29 05:52:15.066 LOG: Err] RT-HAL,rt_entry_add_msg_proc,3390:
rt_halp_vectors->rt_create failed
[Fri Jul 29 05:52:15.066 LOG: Err] RT-HAL,rt_entry_add_msg_proc,3451: proto
ipv6,len 126 prefix ::ffff:101:100/126 nh 1714
[Fri Jul 29 05:52:15.066 LOG: Err] RT-HAL,rt_msg_handler,688: route process
failed
[Fri Jul 29 05:52:15.068 LOG: Err] (acx_rt_ip_uc_lpm_install:LPM route add
failed) Reason : Table full
```

This does not have any functional impact. [PR1203359](#)

- The following PFE error messages are seen after deleting the AE interface configurations:

```
[Sun Oct 23 15:05:33.885 LOG: Err] pfe_acx_clear_tagged_service:IF: Failed
to delete ingress translate entry. unit 0 port -1 Error -7
[Sun Oct 23 15:05:33.890 LOG: Err] pfe_acx_clear_tagged_service:IF: Failed
to delete ingress translate entry. unit 0 port -1 Error -7
```

This does not have any functional impact. [PR1226156](#)

- The following error messages are seen after ISSU:

```
ACX_NH::acx_nh_tag_hw_uninstall(),2629:acx_nh_tag_hw_uninstall: nh 1733
egress uninstall failed: (-7:Entry not found)
ACX_NH::acx_nh_ucast_uninstall(),2755:acx_nh_ucast_uninstall: tag uninstall
failed, err: -7
ACX_NH::acx_nh_stat_add(),1783:bcm_stat_group_create failed(pc:0x883650c)
for NH:1734 HW Idx:100021proto:4(IPv4->MPLS) (-6:Table full)
ACX_NH::acx_nh_stat_add(),1783:bcm_stat_group_create failed(pc:0x88361cc)
for NH:1734 HW Idx:100022proto:4(IPv4->MPLS) (-6:Table full)
```

This does not have any functional impact. [PR1209686](#)

Related Documentation

- [New Features in Junos OS Release 15.1X54–D60 for ACX Series Routers on page 3](#)
- [Upgrade and Downgrade Instructions for Junos OS Release 15.1X54–D60 for ACX Series Routers on page 15](#)

Errata and Changes in Documentation for Junos OS Release 15.1X54-D60 for ACX Series Routers

- [Errata on page 13](#)
- [Changes to the Junos OS ACX Documentation on page 14](#)

Errata

- Support for multifield classifiers is incorrectly omitted from the ACX Series 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. Multifield 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 multifield classifier, you can apply the multifield 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]

Changes to the Junos OS ACX Documentation

There are no changes to the ACX Documentation in Junos OS Release 15.1X54-D60.

- Related Documentation**
- [New Features in Junos OS Release 15.1X54-D60 for ACX Series Routers on page 3](#)
 - [Known Limitations in Junos OS Release 15.1X54-D60 for ACX Series Routers on page 6](#)
 - [Upgrade and Downgrade Instructions for Junos OS Release 15.1X54-D60 for ACX Series Routers on page 15](#)

Upgrade and Downgrade Instructions for Junos OS Release 15.1X54-D60 for ACX Series Routers

This section discusses the following topics:

- [Basic Procedure for Upgrading to Release 15.1X54-D60 on page 15](#)
- [Upgrade and Downgrade Support Policy for Junos OS Releases on page 17](#)

Basic Procedure for Upgrading to Release 15.1X54-D60

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 ACX5000 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 15.1X54-D60 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-acx5k-15.1X54-D60.9-domestic-signed.tgz force-host
```



NOTE: In ACX5000 line of routers, you must always use the **force-host** option for a full software upgrade, which also includes the host software upgrade. An upgrade without the **force-host** option can cause unexpected behaviors and is not recommended.

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 15.1X54-D60 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>.

**Related
Documentation**

- [New Features in Junos OS Release 15.1X54–D60 for ACX Series Routers on page 3](#)
- [Known Limitations in Junos OS Release 15.1X54–D60 for ACX Series Routers on page 6](#)

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

5 December, 2016—Revision 1, Junos OS Release 15.1X54-D60 – ACX Series Routers.

Copyright © 2016, Juniper Networks, Inc. All rights reserved.

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

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