

# K.15.16.0005 Release Notes

## Abstract

This document contains supplemental information for the K.15.16.0005 release.



© Copyright 2014 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

#### **Acknowledgments**

Microsoft®, Windows®, and Windows Server® are U.S. registered trademarks of the Microsoft group of companies.

# Contents

1 K.15.16.0005 Release Notes.....	5
Description.....	5
Important information.....	5
Version history.....	5
Products supported.....	6
Compatibility/interoperability.....	7
Minimum supported software versions.....	7
Enhancements.....	8
Version K.15.16.0005.....	9
Version K.15.16.0004.....	9
BYOD (CR_0000152330).....	9
CPU (CR_0000124429).....	9
DHCPv4 (CR_0000128651).....	9
DHCPv6 (CR_0000144107).....	9
DHCPv6 (CR_0000137520).....	9
Generic header ID (CR_0000144861).....	9
IPv6 (CR_0000142294).....	9
MAC-based VLANs (CR_0000128831).....	9
OSPFv3 (CR_0000154691).....	9
Power restoration (CR_0000146344).....	10
Premium features (CR_0000151228).....	10
UDLD (CR_0000147189).....	10
VLAN (CR_0000145339).....	10
Fixes.....	10
Version K.15.16.0005.....	10
Loop protection (CR_0000160268).....	10
Version K.15.16.0004.....	10
802.1X (CR_0000149780).....	10
Authentication (CR_0000148832).....	10
CLI (CR_0000136134).....	11
CLI (CR_0000145136).....	11
CLI (CR_0000145812).....	11
CLI (CR_0000148661).....	11
CLI (CR_0000150144).....	11
CLI (CR_0000152440).....	11
Configuration (CR_0000152757).....	11
Counters (CR_0000149229).....	11
Counters (CR_0000151412).....	11
Counters (CR_0000151415).....	11
CPU utilization (CR_0000151164).....	11
Crash (CR_0000115372).....	11
Crash (CR_0000146176).....	12
Crash (CR_0000151102).....	12
Crash (CR_0000153386).....	12
Crash (CR_0000153524).....	12
Crash (CR_0000153700).....	12
Crash (CR_0000154053).....	12
Crash (CR_0000154769).....	12
Distributed trunking (CR_0000148165).....	13
Distributed trunking (CR_0000148170).....	13
Distributed trunking (CR_0000149160).....	13

Distributed trunking (CR_0000149768).....	13
Distributed trunking (CR_0000151202).....	13
File transfer (CR_0000145212).....	13
File transfer (CR_0000148584).....	13
ICMP (CR_0000155702).....	13
IGMP (CR_0000128678).....	13
IP phones (CR_0000137652).....	13
IP phones (CR_0000147849).....	13
IPv6 (CR_0000148594).....	13
Latency (CR_0000129743).....	14
Logging (CR_0000146773).....	14
Logging (CR_0000147833).....	14
Logging (CR_0000149891).....	14
Logging (CR_0000150244).....	14
Management (CR_0000149528).....	14
Management (CR_0000155717).....	14
OSPF (CR_0000147711).....	14
OSPF (CR_0000149413).....	14
OSPF (CR_0000155308).....	14
PoE (CR_0000147518).....	14
PoE (CR_0000148808).....	15
PoE (CR_0000155619).....	15
Policy based routing (CR_0000147703).....	15
Rate limiting (CR_0000147093).....	15
Routing (CR_0000151661).....	15
sFlow (CR_0000147660).....	15
SNMP (CR_0000131055).....	15
SNMP (CR_0000146616).....	15
SNMP (CR_0000149657).....	15
SNMP (CR_0000151035).....	15
SNMP (CR_0000154463).....	15
Stacking (CR_0000154380).....	15
Switch hang (CR_0000153460).....	16
Switch hang (CR_0000154152).....	16
Switch initialization (CR_0000149065).....	16
Transceivers (CR_0000146528).....	16
Web management (CR_0000149099).....	16
Web management (CR_0000149777).....	16
Upgrade information.....	16
Upgrading restrictions and guidelines.....	16
Contacting HP.....	17
HP security policy.....	17
Related information.....	17
Documents.....	17
Websites.....	18
Documentation feedback.....	18

## Description

This release note covers software versions for the K.15.16 branch of the software.

Version K.15.16.0004 was the initial release of Major version K.15.16 software. K.15.16.0004 includes all enhancements and fixes in the K.15.15.0006 software, plus the additional enhancements and fixes in the K.15.16.0004 enhancements and fixes sections of this release note.

Product series supported by this software:

- HP 3500 & 3500 yl Switch Series
- HP 5400 zl & 8200 zl Switch Series
- HP 6200yl Switch Series
- HP 6600 Switch Series

## Important information

To avoid damage to your equipment, do not interrupt power to the switch during a software update.

## Version history

All released versions are fully supported by HP, unless noted in the table.

Version number	Based on	Release date	Remarks
K.15.16.0005	K.15.16.0004	2014-11-21	Released, fully supported, and posted on the web.
K.15.16.0004	K.15.15.0006	2014-10-09	Initial release of K.15.16. Released, fully supported, and posted on the web.
K.15.15.0009	K.15.15.0008	2014-11-17	Please see the K.15.15.0009 release note for detailed information on the K.15.15 branch. Released, fully supported, and posted on the web.
K.15.15.0008	K.15.15.0007	2014-09-15	Released, fully supported, and posted on the web.
K.15.15.0007	K.15.15.0006	2014-06-26	Released, fully supported, and posted on the web.
K.15.15.0006	K.15.14.0002	2014-03-19	Initial release of K.15.15. Released, fully supported, and posted on the web.
K.15.14.0010	K.15.14.0009	2014-11-17	Please see the K.15.14.0010 release note for detailed information on the K.15.14 branch. Released, fully supported, and posted on the web.
K.15.14.0009	K.15.14.0008	2014-09-15	Released, fully supported, and posted on the web.
K.15.14.0008	K.15.14.0007	2014-07-16	Released, fully supported, and posted on the web.
K.15.14.0007	K.15.14.0006	2014-07-01	Released, fully supported, and posted on the web.
K.15.14.0006	K.15.14.0003	2014-04-01	Released, fully supported, but not posted on the web.

Version number	Based on	Release date	Remarks
K.15.14.0005		n/a	Never built
K.15.14.0004		n/a	Never built
K.15.14.0003	K.15.14.0002	2013-11-11	Released, fully supported, and posted on the web.
K.15.14.0002	First release	2013-10-18	Initial release of K.15.14

## Products supported

This release applies to the following product models:

Product number	Description
J9470A	HP 3500-24 Switch
J9471A	HP 3500-24-PoE Switch
J9472A	HP 3500-48 Switch
J9473A	HP 3500-48-PoE Switch
J8692A	HP 3500yl-24G-PWR Intelligent Edge Switch
J8693A	HP 3500yl-48G-PWR Intelligent Edge Switch
J9310A	HP 3500yl-24G-PoE+ Switch
J9311A	HP 3500yl-48G-PoE+ Switch
J8697A	HP 5406zl Intelligent Edge Switch
J9642A	HP 5406zl Switch with Premium SW
J8698A	HP 5412zl Intelligent Edge Switch
J9643A	HP 5412 zl Switch with Premium Software
J8699A	HP 5406zl-48G Intelligent Edge Switch
J8700A	HP 5412zl-96G Intelligent Edge Switch
J9447A	HP 5406zl-48G-PoE+ Switch
J9448A	HP 5412zl-96G-PoE+ Switch
J9533A	HP 5406-44G-PoE+/2XG-SFP+ v2 zl Switch
J9532A	HP 5412-92G-PoE+/2XG-SFP+ v2 zl Switch
J9539A	HP 5406-44G-PoE+/4G-SFP v2 zl Switch
J9540A	HP 5412-92G-PoE+/4G-SFP v2 zl Switch
J9866A	HP 5406 8p 10GBASE-T 8p 10GbE SFP+ v2 zl Switch with Premium Software
J8992A	HP 6200yl-24G-mGBIC Switch
J9263A	HP 6600-24G Switch
J9264A	HP 6600-24G-4XG Switch
J9265A	HP 6600-24XG Switch
J9451A	HP 6600-48G Switch
J9452A	HP 6600-48G-4XG Switch

Product number	Description
J9475A	HP 8206zl Switch
J9640A	HP 8206 v2 zl Switch with Premium Software
J8715A, J8715B	HP 8212zl Switch
J9091A	HP 8212zl Switch with fan tray
J9641A	HP 8212 v2 zl Switch with Premium Software
J9638A	HP 8206-44G-PoE+/2XG v2 zl Switch with Premium Software
J9639A	HP 8212-92G-PoE+/2XG v2 zl Switch with Premium Software

## Compatibility/interoperability

The switch web agent supports the following operating system and web browser combinations:

Operating System	Supported Web Browsers
Windows XP SP3	Internet Explorer 7, 8 Firefox 12
Windows 7	Internet Explorer 9, 10 Firefox 24 Chrome 30
Windows 8	Internet Explorer 9, 10 Firefox 24 Chrome 30
Windows Server 2008 SP2	Internet Explorer 8, 9 Firefox 24
Windows Server 2012	Internet Explorer 9, 10 Firefox 24
Macintosh OS	Firefox 24

## Minimum supported software versions

**NOTE:** If your switch or module is not listed in the below table, it runs on all versions of the software.

Product number	Product name	Minimum software version
J9546A	HP 8-port 10GBase-T v2 zl Module	K.15.04.0002
J9310A	HP 3500yl-24G-PoE+ Switch	K.15.02.0004
J9311A	HP 3500yl-48-PoE+ Switch	K.15.02.0004
J9312A	HP 2-Port SFP+/2-Port CX4 10GbE yl Module	K.15.02.0004
J9534A	HP 24-port 10/100/1000 PoE+ v2 zl Module	K.15.02.0004
J9535A	HP 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module	K.15.02.0004
J9536A	HP 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl	K.15.02.0004
J9537A	HP 24-port SFP v2 zl Module	K.15.02.0004

Product number	Product name	Minimum software version
J9538A	HP 8-port 10-GbE SFP+ v2 zI Module	K.15.02.0004
J9547A	HP 24-port 10/100 PoE+ v2 zI Module	K.15.02.0004
J9548A	HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zI Module	K.15.02.0004
J9549A	HP 20-port Gig-T / 4-port SFP v2 zI Module	K.15.02.0004
J9550A	HP 24-port Gig-T v2 zI Module	K.15.02.0004
J9637A	HP 12-port Gig-T / 12-port SFP v2 zI Module	K.15.02.0004
J9475A	HP 8206zI Switch Base System	K.14.34
J9307A	HP 24-Port 10/100/1000 PoE+ zI Module	K.14.34
J9308A	HP 20-Port 10/100/1000 PoE+/4-port MiniGBIC zI Module	K.14.34
J9478A	HP 24-port 10/100 PoE+ zI Module	K.14.34
J9447A	HP 5406zI-48G-PoE+ Switch	K.14.34
J9448A	HP 5412zI-96G-PoE+ Switch	K.14.34
J9470A	HP 3500-24 Switch	K.14.31
J9471A	HP 3500-24-PoE Switch	K.14.31
J9472A	HP 3500-48 Switch	K.14.31
J9473A	HP 3500-48-PoE Switch	K.14.31
J9451A	HP Switch 6600-48G	K.14.24
J9452A	HP Switch 6600-48G-4XG	K.14.24
J9263A	HP Switch 6600-24G	K.14.03
J9264A	HP Switch 6600-24G-4XG	K.14.03
J9265A	HP Switch 6600-24XG	K.14.03
J9154A	HP ONE Services zI Module	K.13.51
J9051A, J9052A	HP Wireless Edge Services zI Module, HP Redundant Wireless Services zI Module	K.12.43
J8715A, J8715B	HP Switch 8212zI Base System	K.12.31
J8993A, J8994A	Premium Features on Series 3500yI and 5400zI Switches	K.11.33
J8706A	HP Switch 5400zI 24p Mini-GBIC Module	K.11.33
J8708A	HP Switch 5400zI 4p 10-GbE CX4 Module	K.11.33
J8992A	HP Switch 6200yI-24G-mGBIC	K.11.33
J8694A	HP Switch 3500yI 2p 10GbE X2 + 2p CX4 Module	K.11.17

## Enhancements

This section lists enhancements found in the K.15.16 branch of the software. Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

**NOTE:** The number that follows the enhancement description is used for tracking purposes.



## Version K.15.16.0005

No enhancements are included in version K.15.16.0005.

## Version K.15.16.0004

### BYOD (CR\_0000152330)

BYOD Redirect. The switch can now be configured for BYOD (Bring Your Own Device) Redirect, which sends the device's credentials to a BYOD server such as IMC, that is configured to control network access.

### CPU (CR\_0000124429)

CPU protection during BPDU flooding. A port can receive a high volume of spanning tree BPDUs when there is a loop in the connected network. This enhancement prevents the switch CPU from being overwhelmed by limiting the rate at which those BPDUs are sent to the CPU. For more information, see the *Advanced Traffic Management Guide* for your switch.

### DHCPv4 (CR\_0000128651)

DHCPv4 server. The switch can now be configured as a DHCPv4 server. For more information, see the *Management and Configuration Guide* for your switch.

### DHCPv6 (CR\_0000144107)

DHCPv6 hardware addresses. The switch can be configured with option 79 to instruct DHCPv6 relay agents to forward client link-layer addresses. For more information, see the *Management and Configuration Guide* for your switch.

### DHCPv6 (CR\_0000137520)

DHCPv6 snooping and DIPLDv6. DHCPv6 snooping and Dynamic IP Lockdown for IPv6 (DIPLDv6) are now supported. For more information, see the *Access Security Guide* for your switch. These features are not yet supported for YB-software switches.

### Generic header ID (CR\_0000144861)

Generic header ID in configuration file. The switch now allows addition of a generic header ID to configuration files saved on a server. This is used for DHCP Option 67 download requests for configuration files. For more information, see the *Management and Configuration Guide* for your switch.

### IPv6 (CR\_0000142294)

IPv6 static route tag. When static routes are redistributed through an OSPFv3 network, a "tag" can be used to filter route redistribution using "route-map", so that only required routes are redistributed. For more information, see the "IPv6 Static Routing" chapter in the *IPv6 Configuration Guide* for your switch.

### MAC-based VLANs (CR\_0000128831)

MAC-Based VLANs (MBV) Enable/Disable. MBV enable/disable options are available using CLI and SNMP. For more information, see the "Web-based and MAC Authentication", and the "Port-Based and User-Based Access Control (802.1X)" chapters in the *Access Security Guide* for your switch.

### OSPFv3 (CR\_0000154691)

OSPFv3 trap enable/disable. The switch can be configured via CLI or SNMP to enable or disable sending of OSPFv3 traps. For more information, see the *IPv6 Configuration Guide* for your switch.

## Power restoration (CR\_0000146344)

Power restoration. When all but one power supply is disabled or removed, the switch is designed to power off the bottom six slots of a twelve-slot chassis. With this enhancement, the bottom six slots are automatically re-enabled when sufficient power is restored to the switch.

## Premium features (CR\_0000151228)

Premium features permanently enabled. The features available with a Premium License are permanently enabled when this software is loaded on a switch. These features are: OSPFv2, OSPFv3, PIM Sparse Mode, PIM Dense mode, VRRP, QinQ (IEEE 802.1ad), BGP, and VRRPv3.

## UDLD (CR\_0000147189)

UDLD Verify Before Forwarding. Unidirectional Link Detection (UDLD) has been enhanced to account for the situation when the link to the directly-connected device is up, but there is no link on one segment of the path to the remote device. For more information, see the *Management and Configuration Guide* for your switch.

## VLAN (CR\_0000145339)

VLAN Precedence. Beginning with 15.06 software, if a VLAN is added to a port while authenticated clients are connected to that port, the VLAN addition is delayed until all authenticated clients are disconnected. This enhancement allows a tagged VLAN to be applied immediately to a port that has connected authenticated clients. For more information, see the *Advanced Traffic Management Guide* for your switch.

## Fixes

This section lists released builds that include fixes. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

---

**NOTE:** The number following the fix description is used for tracking purposes.

---

## Version K.15.16.0005

### Loop protection (CR\_0000160268)

When there is a downstream network loop, the switch can learn its own port MAC address and add it to the MAC table. Normally the switch does not learn its own port MAC addresses, so this is incorrect behavior. However, this does not impact the Loop Protection feature as originally thought. Loop Protection works properly even with this incorrect MAC learning issue.

## Version K.15.16.0004

### 802.1X (CR\_0000149780)

Already-authenticated clients that send an EAPOL-Start message are de-authenticated by the switch. This situation happens if the client runs Windows Vista and later operating systems that are set to "include learning".

### Authentication (CR\_0000148832)

A switch configured with RADIUS authentication for primary login, and local authentication for secondary login fails to use local authentication when RADIUS servers do not respond. In that situation, the switch console is not accessible to valid users.

### CLI (CR\_0000136134)

After issuing the command `no ip ssh cipher cipher_option`, the entry is listed twice in the output of `show run`.

### CLI (CR\_0000145136)

When the switch is configured with the `console event critical` setting, the event log output of `show tech all` lists only the critical events. With this fix, `show tech all` lists all event log entries.

### CLI (CR\_0000145812)

A new command `tcp-push-preserve` is added. This command is enabled by default, and causes TCP packets with the "push" flag to be sent before other packets in the queue. Note that high concentrations of TCP packets with push flags under certain conditions can destabilize your network. Use the `no` form of this command to disable the feature.

### CLI (CR\_0000148661)

When the output of `show power-over-ethernet brief` displays a Detection Status of either Searching or Delivering for a port, the `show tech all "poe_status_port all"` section displays Other Fault as the "Detect Stat".

### CLI (CR\_0000150144)

The output of `show dhcp-relay bootp-gateway vlan VLAN_number` gives an incorrect BOOTP Gateway address for VLANs that are not configured for DHCP relay.

### CLI (CR\_0000152440)

The output of `show tech all` halts while displaying `lmaDbUtil traverseLmaProfTbl`, with the message `=== The command has completed with errors. ===`.

### Configuration (CR\_0000152757)

After configuring `snmp-server host` on the Commander, stack member configuration files include two lines with SNMPv3 configuration.

### Counters (CR\_0000149229)

The "Route changes" counter in the output of `show ip rip` increments with every RIP update the router receives, even if there are no route changes.

### Counters (CR\_0000151412)

The output of a query for meter statistics gives an incorrect value for OpenFlow meter duration.

### Counters (CR\_0000151415)

The output of a query for port statistics gives an incorrect value for OpenFlow statistics duration.

### CPU utilization (CR\_0000151164)

The switch occasionally reports CPU utilization of 99%. This is a false reading and does not affect switch performance.

### Crash (CR\_0000115372)

The switch might reboot unexpectedly with a message similar to `NMI event SW:IP=0x00000000 MSR:0x00000000 LR:0x00000000 cr: 0x00000000 sp:0x00000000 xer:0x00000000 Task='InetServer' Task ID=0xaad3000`.

### Crash (CR\_0000146176)

After receiving multiple route changes or route flaps in a short period of time, the switch might reboot unexpectedly with a message similar to Software exception at krt.c:2134 -- in 'eRouteCtrl', task ID = 0xa9bc400 -> Routing Stack: Assert Failed.

### Crash (CR\_0000151102)

In a rare situation, after a failover to the Standby Management Module (SMM) or the stack's Standby switch, the switch might reboot unexpectedly with a message similar to Software exception at asicMgrSlaveFilters.c:185 -- in 'mNSA', task ID = 0x1b1fea80 -> Internal Name Server Error.

### Crash (CR\_0000153386)

When a large number of 802.1X clients are being authenticated, reconfiguring port security modes such as "learn-mode" might cause the switch to reboot unexpectedly with a message similar to Software exception at multMgmtUtil.c:88 -- in 'mPpmgrCtrl', task ID = 0x13b1f940 -> Internal error.

### Crash (CR\_0000153524)

Entering the command `show ipv6 ospf3 link-state area-scope detail` might cause the switch to reboot unexpectedly with a message similar to Health Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x017cb590 IP=0x17cb590 Task='eRouteCtrl' Task ID=0xa96de00, given one of the following conditions:

- There are more than 64 OSPFv3-enabled VLANs.
- There are more than 64 neighbors on an OSPFv3-enabled broadcast link.
- There are more than 64 addresses advertised in a NAP LSA.
- There are more than 64 IPv6 addresses on an OSPFv3-enabled VLAN.

### Crash (CR\_0000153700)

Three commands are removed from the `show tech all` and `show tech route` commands (which invoke many sub-commands): `show ipv6 ospf3 link-state link-scope detail`, `show ipv6 ospf3 link-state area-scope detail`, and `show ipv6 ospf3 link-state as-scope detail`. In certain situations, issuing those commands will cause the switch to reboot unexpectedly with a message similar to Health Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x017cb590 IP=0x17cb590 Task='eRouteCtrl' Task ID=0xa96de00 sp:0x48cea20 lr:0x10086d4 msr: 0x02029200 xer: 0x20000000 cr: 0x44000400.

### Crash (CR\_0000154053)

When the switch has 802.1X-authenticated clients on a VLAN and the user deletes that VLAN, the switch might reboot unexpectedly with a message similar to Software exception at multMgmtUtil.c:151 -- in 'eChassMgr', task ID = 0x3c945800 -> Internal error.

### Crash (CR\_0000154769)

With a static IGMP group configured, after issuing the `show run` command, changing the sFlow configuration might cause the switch to reboot unexpectedly with a message similar to Health Monitor: Restr Mem Access HW Addr=0x60630015 IP=0x1045630 Task='mSnmpCtrl' Task ID=0xa98b4c0 sp:0x47ecc50 lr:0x104a0ac msr: 0x02029200 xer: 0x20000000 cr: 0x48000400.

### Distributed trunking (CR\_0000148165)

When VRRP routers have distributed trunking enabled, VRRP failovers might cause the VRRP virtual MAC addresses (and therefore remote subnets) to become unreachable.

### Distributed trunking (CR\_0000148170)

A MAC address that is learned by a distributed trunking switch and then moved to another port might be listed on the wrong port by the peer distributed trunking switch, causing that MAC address to be unreachable from the peer switch.

### Distributed trunking (CR\_0000149160)

After removing the Inter-Switch Connection (ISC) and reconfiguring it, some traffic might be dropped or switched to the wrong port.

### Distributed trunking (CR\_0000149768)

During a redundancy switchover, packets might be dropped, affecting traffic destined to MAC addresses learned on a non-distributed trunking port.

### Distributed trunking (CR\_0000151202)

After receiving a join on an Inter-Switch Connection (ISC) port, the switch does not forward joins from other ports onto the ISC.

### File transfer (CR\_0000145212)

Software downloads via SSL fail with certain browsers, including Internet Explorer versions 7, 8, and 10.

### File transfer (CR\_0000148584)

A configuration file with a blank community name in the `snmp-server host` entry cannot be downloaded to the switch. Although the switch does not allow the `snmp-server host` entry to be configured with a blank community name, earlier software bugs might cause this condition.

### ICMP (CR\_0000155702)

The switch sends a ping request to a random IP address every 20 minutes.

### IGMP (CR\_0000128678)

In certain topologies the IGMPv2 "Leave Group" from one host can cause the multicast stream to be dropped, even though there are other hosts receiving that stream.

### IP phones (CR\_0000137652)

An IP phone that uses the "Automatic Port Synchronization" feature loses its IP address and possibly drops the current call. This has been observed when the switch is configured with the command `cdp mode pre-standard-voice`, and the PC to which the phone is connected goes into hibernation. In that situation the "Automatic Port Synchronization" feature causes the phone to drop and then re-establish link with the switch.

### IP phones (CR\_0000147849)

Alcatel phones might reboot unexpectedly when connected to a switch configured to use MAC authentication for IP phones and to use 802.1X authentication for PCs.

### IPv6 (CR\_0000148594)

IPv6 router advertisements that indicate an off-link prefix are not set as "preferred" in the switch, which causes incorrect information in the output of `show ipv6`, and can affect connectivity to

hosts that use IPv6 Stateless Address Autoconfiguration. This issue also causes the sFlow "Agent Address" to be listed as 0.0.0.0.

#### Latency (CR\_0000129743)

When the switch receives a high volume of traffic for unknown destinations, the resulting ARPs sent by the switch in combination with other incoming traffic the switch must process can cause latency and dropped packets. In this situation, the event log might report `IpAddrMgr: IPAM Control task delayed due to slave message queues too full`.

#### Logging (CR\_0000146773)

In an IPv4 plus IPv6 environment, upon switch bootup the event log displays the set of source IP policy ("srcip") messages twice. With this fix, IPv6 policy messages are distinguished from IPv4 policy messages.

#### Logging (CR\_0000147833)

Some RMON events are not correctly defined for VRRP, which causes the switch to report an error such as `system: Unknown Event ID 776` when those events occur.

#### Logging (CR\_0000149891)

When a user disables layer 3 on a VLAN, the event log message might state that layer 3 was disabled for the wrong VLAN.

#### Logging (CR\_0000150244)

Some RMON events are not correctly defined for fault-finder (FFI), SSL, and virus throttling, which causes the switch to report an error such as `system: Unknown Event ID 776` when those events occur.

#### Management (CR\_0000149528)

In some situations with multiple TELNET and/or SSH sessions established, the switch does not accept additional management sessions even if some of the existing ones are killed, responding with the message `Sorry, the maximum number of sessions are active. Try again later`.

#### Management (CR\_0000155717)

After disabling the Out of Band Management (OOBM) interface, saving the config and rebooting the switch, the OOBM interface does not come up even after it is re-enabled.

#### OSPF (CR\_0000147711)

Link State Advertisements (LSAs) are retransmitted by the router before the retransmit timer expires. This improves the original OSPF fix (CR\_0000134463).

#### OSPF (CR\_0000149413)

The SPF counter for OSPFv3 increments for link-state updates even if there is no topology change.

#### OSPF (CR\_0000155308)

When a large number of routes (on the order of 9000) are updated with a better path, the better paths are not always put into the routing table, which can cause unreachable subnets.

#### PoE (CR\_0000147518)

After reboot, pre-standard detection of PoE devices does not function correctly on a 2920 or 3800 stack, if the stack commander is a non-PoE switch.

## PoE (CR\_0000148808)

After disabling PoE on one or more ports, the output of `show cpu slot <slot-number>` shows an increase in CPU utilization of 15% or more.

## PoE (CR\_0000155619)

Some Unify IP phones exhibit a PoE incompatibility with some HP switches, which might result in a hard failure of the phone. For more information see the customer advisory at <http://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=c04438506>.

## Policy based routing (CR\_0000147703)

In some situations, the switch does not allow a `service-policy` to be removed from a VLAN, responding with the error `commit failed`. Workaround: Reboot the switch, then issue the `no service-policy` command.

## Rate limiting (CR\_0000147093)

If rate limiting is applied on the port that connects adjacent OSPF routers, the adjacency is lost after a switch reboot. This issue affects v2 zl modules and 3800 switches.

## Routing (CR\_0000151661)

Packets might not be routed properly when ECMP routes are added to the routing table. This affects packets that are forwarded to an ECMP route destination through a v1 zl module.

## sFlow (CR\_0000147660)

In an IPv6-only environment with Stateless Address Autoconfiguration, sFlow incorrectly uses the link-local address as the agent ID.

## SNMP (CR\_0000131055)

The MIB object `hpicfDownloadTftpConfig(1.3.6.1.4.1.11.2.14.11.1.3.5)` in switch software has a value of 1 for enabled and 2 for disabled, but the reverse is actually correct. With this fix the MIB object to enable and disable the TFTP client on the switch is changed to `hpicfDownloadTftpClientConfig(1.3.6.1.4.1.11.2.14.11.1.3.12)`. Also, the integer values are corrected so 1 is disabled and 2 is enabled.

## SNMP (CR\_0000146616)

OSPFv3 traps are not sent by the switch.

## SNMP (CR\_0000149657)

When using the **createAndWait** mode to set parameters via SNMP, multiple RADIUS servers cannot be configured.

## SNMP (CR\_0000151035)

The switch incorrectly reports that MIB object `entPhysicalIsFRU = False` for removable fantrays, power supplies, and transceivers.

## SNMP (CR\_0000154463)

The switch incorrectly reports that MIB object `entPhysicalIsFRU = False` for transceivers for some switches. This improves the original SNMP fix (CR\_0000151035).

## Stacking (CR\_0000154380)

A failover from Commander to Standby with multiple MSTP instances in operation might cause the stack members and connected devices to be unreachable.



## Switch hang (CR\_0000153460)

Issuing the `boot system` command while VRRP traffic is being received by the switch might cause the switch to hang and not boot completely.

## Switch hang (CR\_0000154152)

If the switch is sending output to the console at the time the switch is rebooted, the switch might hang and not boot properly.

## Switch initialization (CR\_0000149065)

When the switch is rebooted, one module takes about 10 seconds longer to come online than the other modules.

## Transceivers (CR\_0000146528)

After rebooting the switch, the configuration parameter `speed-duplex auto-100` (for a J8177C gigabit-copper transceiver slot) is removed from the config file.

## Web management (CR\_0000149099)

When Spanning Tree Protocol (STP) is enabled via the Web user interface, "mstp" is shown as the default STP mode, and "mstp" is displayed as the operational mode after the user enables STP and saves the change. However, the command line interface shows that the switch operates in "rpvst" mode. Workaround: From the Web user interface, use the dropdown menu to explicitly select "mstp" from the dropdown options, then save the change.

## Web management (CR\_0000149777)

After a failover to the Standby Management Module (SMM) or the stack's standby switch, the Web user interface is not accessible via the Out of Band Management (OOBM) port.

# Upgrade information

## Upgrading restrictions and guidelines

A BootROM update is included in this release.

For more information about BootROM, see the *HP Switch Software Management and Configuration Guide* for your switch.

- ❗ **IMPORTANT:** If your switch is running a software version earlier than K.15, your BootROM will be updated when you upload K.15.16.0005 software to your switch. All switches must be running a BootROM version of K.12.17 or newer in order to load K.15 software. Do not interrupt power to the switch during this important update! A successful update to K.15 software may require multiple steps, depending on your current software and BootROM levels.

**Table 1 BootROM updates**

If your software version is:	Your next step should be:
K.11.11 through K.12.29 (BootROM K.11.00 - K.11.03)	Update and reload into software version K.12.31 or K.12.62
K.12.31 through K.13.55 (BootROM K.12.12 - K.12.14)	Update and reload into software version K.13.58 or K.13.68
K.13.58 or newer (BootROM K.12.17 or newer; use <code>show flash</code> command)	Update directly into software version K.15.16.0005 (BootROM K.15.30)



## Contacting HP

For additional information or assistance, contact HP Networking Support:

[www.hp.com/networking/support](http://www.hp.com/networking/support)

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

## HP security policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

To find security bulletins:

1. Go to the HP Support Center website at [www.hp.com/go/hpsc](http://www.hp.com/go/hpsc).
2. Enter your product name or number and click **Go**.
3. Select your product from the list of results.
4. Click the **Top issues & solutions** tab.
5. Click the **Advisories, bulletins & notices** link.

To initiate a subscription to receive future HP Security Bulletin alerts via email, sign up at:

[www4.hp.com/signup\\_alerts](http://www4.hp.com/signup_alerts)

## Related information

### Documents

To find related documents, see the HP Support Center website:

[www.hp.com/support/manuals](http://www.hp.com/support/manuals)

- Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

### Related documents

The following documents provide related information:

- *HP Switch Software Access Security Guide K/KA/KB.15.16*
- *HP Switch Software Advanced Traffic Management Guide K/KA/KB.15.16*
- *HP Switch Software Basic Operation Guide*
- *HP Switch Software IPv6 Configuration Guide K/KA/KB.15.16*

- *HP Switch Software Management and Configuration Guide K/KA/KB.15.16*
- *HP Switch Software Multicast and Routing Guide K/KA/KB.15.16*

## Websites

- Official HP Home page: [www.hp.com](http://www.hp.com)
- HP Networking: [www.hp.com/go/networking](http://www.hp.com/go/networking)
- HP product manuals: [www.hp.com/support/manuals](http://www.hp.com/support/manuals)
- HP download drivers and software: [www.hp.com/support/downloads](http://www.hp.com/support/downloads)
- HP software depot: [www.software.hp.com](http://www.software.hp.com)
- HP education services: [www.hp.com/learn](http://www.hp.com/learn)

## Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback ([docsfeedback@hp.com](mailto:docsfeedback@hp.com)). Include the document title and part number, version number, or the URL when submitting your feedback.