K.15.12.0016 Release Notes

Abstract

This document contains supplemental information for the K.15.12.0016 release.

HP Part Number: 5998-8095
Published: May 2015
Edition: 1

Acknowledgments

Contents

1 K.15.12.0016 Release Notes

Description

This release note covers software versions for the K.15.12 branch of the software.

Version K.15.12.0006 was the initial release of Major version K.15.12 software. K.15.12.0006 software was built from the same source as K.15.11.0003. K.15.12.0006 includes all enhancements and fixes in K.15.11.0003 software, plus the additional enhancements and fixes in the K.15.12.0006 enhancements and fixes section of this release note.

Product series supported by this software:

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

Version history

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

Version number	Release date	Based on	Remarks
K.15.12.0016	2014-10-06	K.15.12.0015	Released, fully supported, and posted on the web. Final release of the K.15.12 branch of software.
K.15.12.0015	2014-03-14	K.15.12.0014	Released, fully supported, and posted on the web.
K.15.12.0014	2014-01-17	K.15.12.0012	Released, fully supported, and posted on the web.
K.15.12.0013	n/a		Never built.
K.15.12.0012	2013-11-05	K.15.12.0011	Released, fully supported, and posted on the web.
K.15.12.0011	2013-10-10	K.15.12.0010	Released, fully supported, but not posted on the web.
K.15.12.0010	2013-08-13	K.15.12.0009	Released, fully supported, and posted on the web.
K.15.12.0009	2013-07-10	K.15.12.0008	Released, fully supported, but not posted on the web.
K.15.12.0008	n/a	K.15.12.0007	Never released.
K.15.12.0007	2013-03-26	K.15.12.0006	Released, fully supported, but not posted on the web.
K.15.12.0006	2013-02-28	K.15.11.0003	Released, fully supported, but not posted on the web.
K.15.11.0009	2013-07-15	K.15.11.0008	Released, fully supported, but not posted on the web.
K.15.11.0008	n/a	K.15.11.0007	Never released.
K.15.11.0007	2013-03-26	K.15.11.0005	Released, fully supported, but not posted on the web.
K.15.11.0006	n/a		Never built.

Version number	Release date	Based on	Remarks
K.15.11.0005	n/a	K.15.11.0004	Never released.
K.15.11.0004	2013-02-22	K.15.11.0003	Released, fully supported, but not posted on the web.
K.15.11.0003	2012-12-10	K.15.10.0003	Released, fully supported, but not posted on the web.
K.15.10.0025	2014-01-13	K.15.10.0024	Released, fully supported, and posted on the web.
K.15.10.0024	2013-11-14	K.15.10.0023	Released, fully supported, but not posted on the web.
K.15.10.0023	n/a	K.15.10.0022	Never released.
K.15.10.0022	2013-10-22	K.15.10.0021	Released, fully supported, and posted on the web.
K.15.10.0021	2013-09-20	K.15.10.0020	Released, fully supported, but not posted on the web.
K.15.10.0020	2013-09-20	K.15.10.0019	Released, fully supported, but not posted on the web.
K.15.10.0019	2013-08-23	K.15.10.0018	Released, fully supported, but not posted on the web.
K.15.10.0018	2013-08-08	K.15.10.0017	Released, fully supported, but not posted on the web.
K.15.10.0017	2013-08-02	K.15.10.0016	Released, fully supported, but not posted on the web.
K.15.10.0016	2013-07-11	K.15.10.0015	Released, fully supported, and posted on the web.
K.15.10.0015	2013-06-25	K.15.10.0014	Released, fully supported, and posted on the web.
K.15.10.0014	n/a	K.15.10.0013	Never released.
K.15.10.0013	n/a	K.15.10.0012	Never released.
K.15.10.0012	2013-04-22	K.15.10.0011	Released, fully supported, but not posted on the web.
K.15.10.0011	2013-03-25	K.15.10.0010	Released, fully supported, but not posted on the web.
K.15.10.0010	2013-03-12	K.15.10.0009	Released, fully supported, but not posted on the web.
K.15.10.0009	2013-02-22	K.15.10.0008	Released, fully supported, but not posted on the web.
K.15.10.0008	2013-02-04	K.15.10.0007	Released, fully supported, but not posted on the web.
K.15.10.0007	n/a	K.15.10.0006	Never released.
K.15.10.0006	2012-11-14	K.15.10.0005	Released, fully supported, but not posted on the web.
K.15.10.0005	2012-10-22	K.15.10.0004	Released, fully supported, but not posted on the web.

Version number	Release date	Based on	Remarks
K.15.10.0004	n/a	K.15.10.0003	Never released.
K.15.10.0003	2012-08-30	Initial release	Released, fully supported, but not posted on the web.

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 SW
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
J9475A	HP 8206 v2 zl Switch with Premium SW
J8715A, J8715B	HP 8212zl Switch

Product number	Description
J9091A	HP 8212zl Switch with fan tray
J9641A	HP 8212 v2 zl Switch with Premium SW
J9638A	HP 8206-44G-PoE+/2XG v2 zl Switch with Premium SW
J9639A	HP 8212-92G-PoE+/2XG v2 zl Switch with Premium SW

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

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 Module	K.15.02.0004
J9537A	HP 24-port SFP v2 zl Module	K.15.02.0004
J9538A	HP 8-port 10-GbE SFP+ v2 zl Module	K.15.02.0004
J9547A	HP 24-port 10/100 PoE+ v2 zl Module	K.15.02.0004
J9548A	HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module	K.15.02.0004

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

Enhancements

This section lists enhancements found in the K.15.12 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 precedes the enhancement description is used for tracking purposes.

Version K.15.12.0016

No enhancements were included in version K.15.12.0016.

Version K.15.12.0015

No enhancements were included in version K.15.12.0015.

Version K.15.12.0014

No enhancements were included in version K.15.12.0014.

Version K.15.12.0013

Version K.15.12.0013 was never built.

Version K.15.12.0012

No enhancements were included in version K.15.12.0012.

Version K.15.12.0011

No enhancements were included in version K.15.12.0011.

Version K.15.12.0010

No enhancements were included in version K.15.12.0010.

Version K.15.12.0009

No enhancements were included in version K.15.12.0009.

Version K.15.12.0008

Version K.15.12.0008 was never released.

Version K.15.12.0007

No enhancements were included in version K.15.12.0007.

Version K.15.12.0006

Clarify Port VLAN Tagged Status.

CR_0000123824 Clarify Port VLAN Tagged Status. This enhancement allows the identification of ports as `access`, `trunk`, or `voice`. The `show interfaces` command has added the **`status`** option, which displays tagged and untagged VLAN information for a port. See "Static Virtual LANs (VLANs)" in the *Advanced Traffic Management Guide* for your switch.

Event Log Severity Changes

0000119734 The default severity status of several event log messages has been changed from `informational` to `warning`. See the *Event Log Message Reference Guide* for more information about event log messages.

RADIUS IPv6

PR_0000072866, CR_0000077692 RADIUS IPv6. This enhancement adds IPv6 capabilities for the RADIUS client. The Network Access Server is now able to use IPv6 addresses as well as communicating with IPv6 RADIUS servers. See "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide*. See also the *IPv6 Configuration Guide* for your switch.

Readable Interface Names in Traps

CR_0000113486 The SNMP trap notification messages for linkup and linkdown events on an interface now include IfDesc and IfAlias var-bind information. For more information on SNMP traps, see "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

Strict Priority Queueing

CR_0000122671 The switches currently implement priority-to-queue mapping as defined in the IEEE 802.1D-2004 Annex G standard. Another standard, IEEE 802.1Q-2005, defines a slightly different mapping where the ordering of priorities 0-2 is changed. This enhancement allows you to configure the switch to follow either standard.

Fixes

Software fixes are listed in reverse-chronological order, from newest to oldest software version. Unless otherwise noted, each software version listed below includes all the software fixes and enhancements added in previous versions listed below.

NOTE: The number that precedes the fix description is used for tracking purposes.

Version K.15.12.0016

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.

BPDU Protection

CR_0000144148 If VLAN 1 is not enabled on the link between a switch running rapid PVST and a switch running any Spanning Tree version, a rapid PVST switch configured for BPDU protection does not shut down the port when it receives a BPDU from the neighboring switch. However, the BPDUs are correctly dropped.

CLI

CR_0000143652 The switch does not allow the `lockout-mac` command to be configured for a MAC address that is all zeros (000000-000000).

Counters

CR_0000148671 The output of `show ip counters ipv6` gives incorrect values.

Management

CR_0000155914 When rebooting the chassis many times, the Standby Management Module (SMM) may sometimes fail to boot up properly or crash during the reboot.

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.

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.

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.

RADIUS

CR_0000149657 Configuration of multiple RADIUS servers via SNMP fails if a `createAndWait` mechanism is used.

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.

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_0000147370 After using SNMP to configure a RADIUS server on the switch, the switch does not allow a login until the switch is rebooted.

CR_0000152823 Duplicate RADIUS servers are allowed if the SNMP `createAndWait` mechanism is used.

Switch Initialization

CR_0000149065 When the switch is rebooted, one module takes about 10 seconds longer to come online than the other modules.

TELNET

CR_0000142571 While a user is being authenticated by a RADIUS server, issuing the `show access-list radius all` command from a TELNET session might cause the TELNET session to hang.

Version K.15.12.0015

Counters

CR_0000141119 The output of `show ip counters` is incorrect when routing is enabled for IP, IPv6, or multicasts.

CR_0000143860 On a switch configured with rapid PVST and BPDU protection, the output of the command `show spanning-tree bpdu-protection` shows zero errant BPDUs received, even when the switch has disabled a port due to receiving a BPDU. This is a display issue only, both rapid PVST and BPDU protection function properly.

Crash

CR_0000133659 With sFlow enabled and IPv6 configured on a VLAN, the switch might reboot unexpectedly with a message similar to `Software exception at sflow.c:5563 -- in 'mEaseCtrl', task ID = 0x3c8c1680.`

CR_0000137552 With OSPF enabled, if one switch has jumbo frames enabled but the link partner does not, the switch might reboot unexpectedly with a message similar to `Software exception at block.c:1158 -- in 'SIGIO Task', task ID = 0xa94f800 -> Routing Stack: Assert.`

CR_0000141877 With MSTP enabled, when the event log receives a large number of entries in a very short time, the switch might reboot unexpectedly with a message similar to `Software exception at svc_misc.c:865 -- in 'mMstpCtrl', task ID = 0xa953140 -> Failed to calloc 700 bytes.`

CR_0000144879 The switch might reboot unexpectedly in the following situations: 1) The switch is running 15.08 or earlier software, is configured to drop frames that have a destination address

of 01:00:0c:cc:cc:cd, and has PVST filtering or PVST protection enabled. Then the switch is updated to 15.09 or later software. 2) The switch is running 15.09 or later software, is configured to drop frames that have a destination address of 01:00:0c:cc:cc:cd, and then PVST filtering or PVST protection is enabled. The switch reboots unexpectedly with a message similar to `Software exception at bttfLearn.c:2616 -- in 'mLpmgrCtrl', task ID = 0xa98a9c0 -> Mac Table Error.`

CR_0000146306 The switch uses TCP connections internally for inter-process communication. In a situation where an internal loopback TCP socket pair receives stimulus after an extended period of idle time, the switch might reboot unexpectedly with a message similar to `NMI event SW:IP=0x00e20c1c MSR:0x02029200 LR:0x00e077d0 cr: 0x44000400 sp:0x02b03c58 xer:0x00000000 Task='InetServer' Task ID=0xab31000.`

Distributed Trunking

CR_0000144697 Distributed Trunking LACP links do not come up when connected to non-HP devices such as Solaris Unix systems.

IGMP

CR_0000138408 Joins sent by clients in response to a Group Specific Query are not forwarded by the Querier, causing the clients to lose the stream.

CR_0000140514 After disabling IGMP forwarding on a port, multicast traffic incorrectly continues to flow from that port.

Mirroring

CR_0000145818 With more than one remote mirroring session configured on a VLAN, if the user deletes a VLAN with a lower number than the VLAN being mirrored, all mirrors except the lowest-numbered mirror session are removed from the mirrored VLAN.

Multicast

CR_0000138817 When a multicast stream is sent to a reserved multicast address, a General Query might not be not forwarded by the switch, causing clients to be dropped from the multicast stream.

OSPF

CR_0000134463 When the router receives multiple duplicate LSAs in a short time period, the router does not acknowledge them all in time, which causes OSPF adjacencies to be lost and then re-formed.

CR_0000147711 Link State Advertisements (LSAs) are retransmitted by the router before the retransmit timer expires. This improves the original OSPF fix (CR_0000134463).

Switch Hang

CR_0000142411 On a switch configured for Web or MAC authentication plus MSTP plus Distributed Trunking with keepalive, with high levels of reauthentication occurring on multiple ports, the switch might appear to hang and be unreachable for remote management. The console is initially accessible, but issuing a `show` command might cause the console to also hang. This affects LACP and LLDP protocols, as seen by neighboring switches.

CR_0000146247 With both authentication and accounting enabled, the switch might become unresponsive to management, requiring a reboot to recover.

TELNET

CR_0000127908 Continuous logging on and then logging off via TELNET might cause the switch to believe all TELNET sessions are in use, and no additional TELNET sessions can be established.

Version K.15.12.0014

BGP

CR_0000138230 When BGP has equal cost routes, but one route is preferred due to a higher configured weight, the outputs of `show ip bgp` and `show ip route` show that the router uses the wrong route.

CLI

CR_0000138041 The command `show ipv6 ospf3 link-state area-scope` does not display any output when more than 25 VLANs are configured on the switch.

Counters

CR_0000142198 When a trunk configured for sFlow polling is simultaneously queried via SNMP, all counter values for the trunk are zero.

Crash

CR_0000118056 The switch experiences a loss of free memory each time the `show ip ospf link-state detail` or `display ospf lsdb network` or `display ospf lsdb router` command is issued. When memory is no longer available, the switch reboots unexpectedly with a message similar to `Software exception at block.c:1165 -- in 'SIGIO Task', task ID = 0xa989fc0 -> Routing Stack: Assert.`

CR_0000141095 When a switch port is configured for MAC authentication with the `addr-moves` parameter, if a client on that port moves to a different port, the switch might reboot unexpectedly with a message similar to `Software exception at hwBp.c:218 -- in 'fault_handler', task ID = 0xa5df1c0 -> MemWatch Trigger: Offending task 'mWebAuth'. Offending IP=0xb35494.`

CR_0000142134 With outbound queue monitoring configured (`qos watch-queue <PORT>`), a switch module or port bank might reboot unexpectedly with a message similar to `Software exception at alloc_free.c:793 -- in 'mAsicUpd', task ID = 0x61e7b00 -> buf already freed by 0x061E7B00, op=0x00500079.`

CR_0000143067 Under extremely heavy traffic loads, repeated port toggling might cause the switch to reboot unexpectedly with a message similar to `Software exception at bgp_tsi.c:361 -- in 'eRouteCtrl', task ID = 0xa95fcc0 -> Routing Stack: Assert Failed.`

Display Issue

CR_0000140830 When `terminal length` is changed from the default of 24, the config file display is truncated, and the outputs of **`show logging`** and `show interfaces` might be interleaved in the output of `show tech all`.

Meshing

CR_0000143068 Multicast traffic and unicast traffic with unknown destination addresses are not routed over the mesh.

Nonstop Switching

CR_0000133990 After a management module failover of an 8200zl switch configured for Nonstop switching, one or more of the following issues might be observed:

- The output of `show system fans` displays `Fan Failed` for all fans.
- The output of `show system power-supply` displays `Not Present` for all power supply slots.
- The output of `walkmib hpicfsensortable` displays `hpicfSensorIndex.0 = 0`.

RADIUS

CR_0000138258 In some situations, the switch response to Change of Authorization and Disconnect Messages from the RADIUS server is sent from an incorrect source IP address, which the RADIUS server therefore ignores.

Spanning Tree

CR_0000143817 With a switch configured for MSTP, if the spanning tree mode is changed to `force-version rstp-operation` and then a second management module (or stack member) is inserted, the switch might reboot unexpectedly with a message similar to `Health Monitor: Read Error Restr Mem Access HW Addr=0xe59ff10c IP=0x779004c Task='mMstpCtrl' Task ID=0x13af9740 fp: 0x0d372620 sp:0x0d372604 cpsr: 0x6000001f.`

Version K.15.12.0013

Version K.15.12.0013 was never built.

Version K.15.12.0012

Config

CR_0000124808 A switch that is upgraded from K.14 to K.15 software or from W.14 to W.15 software has a tilde erroneously added to the community name specified in the `snmp-server host` command.

CR_0000138447 After a switch software update, SNMP community access privileges are incorrectly changed by the switch. The output of `show snmp-server` and the output of a `walkmib` command give different results, and neither output represents how the switch actually behaves for Manager or Operator access. This issue was introduced with CR_0000122623; if the access settings were configured on a switch without the CR_0000122623 fix, after updating to software with the CR_0000122623 fix the settings are changed.

CPU Utilization

CR_0000129968 Entering some commands such as `show flash` results in very slow console response, and switch CPU utilization of 100%.

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.`

CR_0000135900 In some situations it is possible for the switch to reboot unexpectedly with a message similar to `Software exception at alloc_free.c:646 -- in 'eDrvPoll', task ID = 0xa9a7a80 -> buf already freed by 0x0A9A7D40, op=0x0006003E.`

CR_0000137288 With SNTP configured, in a rare situation after a time update, the switch might reboot unexpectedly with a message similar to `Health Monitor: Invalid Instr`

`Misaligned Mem Access HW Addr=0x31352e30 IP=0x31352e30 Task='mDebugCtrl' Task ID=0x3c9558c0 sp:0x11f92cd0 lr:0x31352e31 msr: 0x02029200 xer: 0x00000000 cr: 0x28000800.`

CR_0000138879 After boot, a switch that has a syslog server and an IPv6 address configured might become unresponsive to management, and after a period of time the switch might reboot repeatedly with a message similar to `NMI event SW:IP=0x001517d4 MSR:0x02029200 LR:0x0015178c cr: 0x28000400 sp:0x03aae0e0 xer:0x00000000 Task='mDebugCtrl' Task ID=0xa9f8000.`

CR_0000142271 The v2 zl modules in a switch might reboot unexpectedly, or the switch itself might reboot unexpectedly, after repeated link toggling of v2 zl module ports or 3800 ports.

CR_0000142755 The switch might reboot unexpectedly after repeated link toggling of fiber ports.

Guaranteed Minimum Bandwidth

CR_0000136039 When the switch is configured to use fewer than the default of 8 queues, packets in lower-priority queues might be unintentionally dropped.

ICMP

CR_0000134682 The switch does not log an unsolicited ICMP reply unless it has first pinged some (any) IP address. Also, unsolicited ICMP reply log messages are sometimes associated with the DEFAULT_VLAN instead of the VLAN of the incoming unsolicited ICMP reply.

Jumbo Frames

CR_0000137961 When jumbo frames are enabled on any VLAN, OSPF fails to establish an adjacency after a switch reboot, and RIP updates might not be accepted by the router.

CR_0000141474 When jumbo frames are enabled on any VLAN, OSPF fails to establish an adjacency after a switch reboot, and RIP updates might not be accepted by the router. This fix improves the original Jumbo Frames fix (CR_0000137961).

Mirroring

CR_0000134191 IP connectivity to the mirror endpoint switch might be intermittent when remote mirroring is configured on the management VLAN, and mirroring is configured for traffic in `both` directions.

OSPF

CR_0000137616 When the switch is configured as an OSPF neighbor, and the neighbor changes time, OSPF adjacency temporarily drops.

Policy Based Routing

CR_0000134936 The show statistics policy counter is not reset by the `clear statistics policy` command.

sFlow

CR_0000134427 sFlow sampling of multicast packets sometimes results in duplicate packets that can cause pixelation of video or other degradation of the multicast stream.

TFTP

CR_0000132721 Certain lines in the configuration file are sometimes incorrectly changed when imported via TFTP. For example, the configuration entry `snmp-server community public unrestricted` might have the `unrestricted` parameter removed when the config file is downloaded via TFTP.

Web Management

CR_0000139666 Customers using a browser that does not support the X-Frame-Options tag, and who have an open Web management session and then initiate another browser session, could be vulnerable to cross-frame scripting.

CR_0000140379 A self-signed SSL certificate and a CA-generated certificate cannot use an organizationName, organizationalUnitName, localityName, stateOrProvinceName longer than 40 characters. With this fix, the limit is 64 characters.

Version K.15.12.0011

Accounting

CR_0000133762 If a Windows system is configured for both computer authentication and user authentication, accounting might not function properly.

DHCP

CR_0000137877 A switch acting as a DHCP relay agent sends two DHCP packets, one of which incorrectly has the source MAC address of the client instead of the switch.

Guaranteed Minimum Bandwidth

CR_0000138064 When a 10-Gigabit port on a 3800 switch or v2 zl module is operating at 1-Gigabit, low priority queues might become "starved" and drop traffic.

PIM-SM

CR_0000135871 In some cases, a "join" from a remote host is not properly processed by the switch and the multicast traffic is not forwarded. This has been observed after a host on the same subnet as the multicast source has joined the stream, and a remote host leaves the multicast stream.

RADIUS Accounting

CR_0000137793 An interim-update status request generates incorrect accounting information in the RADIUS server.

Web Management

CR_0000137792 A self-signed SSL certificate generated via the Web interface cannot use a common name (CNAME) longer than 40 characters. With this fix, the limit is 90 characters.

Version K.15.12.0010

CLI

CR_0000137287 The output of `show run vlan <VLAN_ID>` omits the `no` in the configuration entry `no ip igmp fastleave`. Note that the output of `show run` gives correct information.

Config

CR_0000131054 Setting an operator or manager password on the switch causes four features to be disabled: auto run, DHCP-based config file download from an external tftp server, DHCP-based software image download from an external tftp server, and tftp server functionality within the switch. With this fix, more accurate messages are sent regarding the specific features that are disabled by setting the operator or manager password.

CR_0000135481 After boot, a config file that has a trap destination community name with an open parenthesis "(" or a close parenthesis ")" cannot be downloaded to the switch.

Crash

CR_0000127791 In a rare situation the switch might reboot unexpectedly with a message similar to `Software exception at rt_table.c:.`

CR_0000130339 In some situations, executing the command `show snmp-server traps` might cause the switch to reboot unexpectedly with a message similar to `Software exception at cli_snmpv2_action.c:9634 -- in mSess2', task ID = 0x13ab0 -> ASSERT: failed`.

CR_0000131604 Configuring Mac Authentication with a 256-client limit might cause the switch or stack member to reboot unexpectedly.

CR_0000131959 With MAC Authentication configured on stacking ports, the switch might reboot unexpectedly with a message similar to `Software exception at highAvailHelper.c:1040 -- in 'mRdHelper', task ID = 0x3c9389c0`.

Distributed Trunking

CR_0000135353 With Distributed Trunking and VRRP enabled, when both the VRRP master and backup routers reboot together, the VRRP master might not be reachable by the Distributed Trunking switches.

Event Log

CR_0000127436 After the switch uptime reaches 497 days, the timestamp entries in the event log become erratic with gaps of several hours or days. In some cases the timestamps revert to previous months and years, even though SNTP updates with those wrong timestamps report the correct date and time.

IGMP

CR_0000132149 Although the RFC requires that the switch with the lowest IP address becomes querier, a switch that is acting as querier stops being querier when it receives a query from a switch with a higher IP address.

CR_0000135527 A non-querier switch that receives a Join from the querier fails to send further Joins to the querier, resulting in loss of multicast traffic.

CR_0000136013 After the switch becomes querier, it does not update the table that defines the querier port, and continues to forward IGMP packets out of the port that previously led to the querier.

Latency

CR_0000132667 After a switch reboot, traffic that flows through the J9538A 8-port 10GbE SFP+ v2 zl Module experiences poor performance.

Link

CR_0000137549 Gigabit fiber transceivers operate in auto-negotiation mode even if the port is configured for 1000 Mbps full-duplex operation (`speed-duplex 1000-full`). If both sides of the link are configured as 1000-full, the link goes down after the switch at one side of the link is updated with affected software. This issue was introduced in software version 15.12.0006.

MAC Authentication

CR_0000129991 MAC Authentication fails when the `peap-mschapv2` parameter is included in the `aaa authentication` CLI command.

Menu

CR_0000135171 With the Menu interface, if the user navigates to **Switch Configuration** → **IP Configuration** and selects **Save** without changing anything on that screen, OSPF settings are removed from every VLAN.

OpenFlow

CR_0000134471 OpenFlow flows are not programmed correctly when RPVST+ is disabled on the OpenFlow member VLAN.

Passwords

CR_0000134358 Navigating to the security wizard page on a switch that has manager and operator credentials set, a tool such as firebug allows the admin to view passwords in the `secwiz.js` file. (The admin would have to be logged in with valid credentials to view the passwords.)

PIM

CR_0000134883 High CPU utilization from PIM message exchanges causes dropped multicast streams.

Routing

CR_0000123230 The switch does not forward traffic to a host that has a static route configured with a 32-bit subnet mask. Traces show that the switch never sends an ARP request for that host.

sFlow

CR_0000128439 When an sFlow-sampled inbound packet is to be routed, the sFlow data gives the wrong output port on the switch.

SNMP

CR_0000123582 Including the `detail` parameter in the command `show ipv6 ospf3 link-state areascope detail` might cause infinite output. This affects the `show tech all` command, which includes the detail parameter.

Web Management

CR_0000135883 The **Rx Errors** column is missing from the Web user interface.

Version K.15.12.0009

Distributed Trunking

CR_0000135388 When a MAC address moves from a Distributed Trunk port to a non-Distributed Trunk port, the switch MAC tables sometimes show that MAC address on the wrong port. This fix improves the original Distributed Trunking fix (CR_0000132286).

Version K.15.12.0008

Authentication

CR_0000134114 With both 802.1X and MAC Authentication configured on a port, it is possible for an already-authenticated client to be erroneously moved to the unauthenticated VLAN.

Banner MOTD

CR_0000132198 The login banner is not displayed if the user logs into the switch via the standby or member switch instead of the active or commander switch.

CLI

CR_0000128124 The output of `show monitor` and `show monitor <mirror_destination_number>` displays information only for mirror destination #1.

Config

CR_0000129797 A config file that has the entry `ipv6 ospf3 passive` on a tunnel cannot be downloaded to the switch.

Crash

CR_0000120116 With OSPF configured, in a rare situation the switch might reboot unexpectedly with a message similar to `Software exception at rt_table.c:4453 -- in 'eRouteCtrl', task ID = 0xa9c4c00 -> Routing Stack: Assert Failed.`

CR_0000126777 With a combination of interface state changes along with IPV6 address configuration changes, it is possible for the switch to reboot unexpectedly with a message similar to `SubSystem 0 went down: 01/24/13 13:31:29, Invalid Instr HW Addr=0x000004a8 IP=0x4a8, Task='mIpCtrl' Task ID=0xa9ca140 sp:0x470aab0 lr:0x723f4c, msr: 0x02029200 xer: 0x20000000 cr: 0x48000400.`

CR_0000129047 When running commands from multiple simultaneous CLI sessions the switch may reboot with the error message `Software exception at hwBp.c:218.`

Distributed Trunking

CR_0000132286 When a MAC address moves from a Distributed Trunk port to a non-Distributed Trunk port, the switch MAC tables sometimes show that MAC address on the wrong port.

CR_0000132900 With a switch configured for both Distributed Trunking and MSTP, a MAC address learned on a VLAN that is not part of the Inter-Switch Connection (ISC) might not appear in the MAC table, or might appear on the wrong port. This issue has been observed when all the Distributed Trunk ports are down on the switch that learns the MAC address.

Dynamic ARP Protection

CR_0000132073 When a VLAN is configured for dynamic ARP protection and also DHCP snooping, ARP packets should be forwarded, but are incorrectly dropped when the arp-protect configuration does not include the `validate ip` option.

Fastboot

CR_0000127452 With fastboot enabled, TCP traffic experiences poor performance through ports 4, 5, and 6 of the J9538A 8-port 10GbE SFP+ v2 zl Module.

GVRP

CR_0000129917 When the switch receives its own GVRP frames, it learns from them instead of dropping the frames.

CR_0000130090 After rebooting the switch, the configuration `unknown-vlans disable` does not work on trunks.

LEDs

CR_0000133898 PoE faults cause the DIM Status LED to blink instead of the PoE Status LED.

Loop Protection

CR_0000127150 Loop protection fails to detect a loop on a port configured for 802.1X authentication, if 802.1X is not enabled globally.

Management

CR_0000134091 Disabling write access to an SNMP community via the Web user interface might cause the switch to become unresponsive to command input. The switch must be rebooted to regain management access.

OSPF

CR_0000123661 OSPFv3 packets do not include the differentiated services information that should be in the Traffic Class field of the IPv6 header.

Passwords

CR_0000130921 If the switch is configured with a username and password, changing the password causes the username to also change. The username is changed to the default **`manager`** or **`operator`**, depending on which password is changed.

CR_0000134675 The switch does not automatically create a default username of **`manager`** or **`operator`** when a password is configured for those levels of access.

PIM

CR_0000128681 After a large number of multicast streams are added and old streams time out, the switch might get into a state where it is unable to add new multicast streams, responding with a message similar to `IpAddrMgr: Failed to allocate new SW IP multicast group, table full FIB entry`.

CR_0000130353 The switch might send duplicate multicast packets when sFlow is enabled and the multicast packets are routed by software.

SNMP

CR_0000122623 After rebooting a switch configured for SNMP with the parameters operator `unrestricted`, the switch does not allow the user to set any read/write MIB objects.

Stacking

CR_0000121075 When stacking is enabled, the switch is accessible via the Web even after disabling the Web server, and via TELNET even after disabling TELNET.

TFTP

CR_0000129475 A switch config that has certain lines in the config file cannot be downloaded to the switch via TFTP. For example, attempting to download a config file with the valid statement distributedtrunking `peer-keepalive udp-port 6400` results in the error message UDP port 6400 is already in use.

Transceivers

CR_0000129775 The switch does not turn off the laser when a port is administratively disabled, which might result in the link partner still seeing the link. This has been observed with X2-SC SR Optics (J8436A) that have MYxxxxxxxx serial numbers.

CR_0000132781 Software does not allow the dual-speed J8177C Gigabit-copper transceiver to be configured for 100 Mbps operation, responding with a message such as `Value auto-100 is not applicable to port A21`.

CR_0000133023 100-Megabit transceivers might have one or more of these symptoms: 1) Link LED is lit but link is down, 2) No Link after the transceiver is hot-swapped, 3) Transceiver fails self test.

Version K.15.12.0007

Crash

CR_0000127335 In some situations, issuing the `show tech all` command might cause the switch to reboot unexpectedly with a message similar to `Length Corruption`.

Display Issue

CR_0000128256 When the `display modules` command is run, the slot designation that should be in column 1 of the output is missing for OA or ONE blades.

Uplink Failure Detection

CR_0000127868 On a switch that is configured for uplink failure detection where the link to monitor (LtM) or link to disable (LtD) is an LACP trunk, after reboot, the link to monitor is listed as down in the output of `show uplink-failure-detection`, and the link to disable is taken down by the switch.

Version K.15.12.0006

Accounting

CR_0000123330 Accounting request of `Status-Type = Interim-Update` incorrectly includes session traffic counters.

ACLs

CR_0000122535 When configuring an ipv4 or ipv6 prefix-list, it is not possible to add an entry to permit/deny 'any'.

BootROM

CR_0000124997 This software version includes a BootROM update to BootROM version K.15.30.

Crash

CR_0000122568 With SSL enabled, an attempt to download software via the Web interface might cause the switch to reboot unexpectedly with a message similar to: `NMI event SW:IP=0x006d1538 MSR:0x02029200 LR:0x006d19e4, cr: 0x28000800 sp:0x05197088 xer:0x20000000, Task=tHttpd Task ID=0xa955000.`

CR_0000126799 Under unusual stress conditions, the switch might reboot unexpectedly with a message similar to `Software exception at fileTransfer.c:1144 -- in 'tHttpd', task ID = 0xa9389c0 -> Could not open file.`

DHCP Snooping

CR_0000126311 The CLI entry `dhcp-snooping option 82 untrusted-policy keep` is not included in the config file if **`no dhcp-snooping option 82`** is also configured. If the config file is saved to a TFTP server, it does not function properly when subsequently loaded on a switch.

Distributed Trunking

CR_0000124473 The switch does not allow DHCP server responses to cross the Inter-Switch Connection (ISC).

CR_0000125623 After rebooting a switch participating in a distributed LACP trunk, a distributed trunk port that is disconnected does not link after it is connected.

CR_0000127096 When the Inter-Switch Connection (ISC) is brought down, clients connected via Distributed Trunk links cannot be reached from one of the Distributed Trunking switches.

Event Log

CR_0000127230 Successful manager/operator login generates a trap and log event with severity `Warning`, where `Informational` is expected.

IGMP

CR_0000105902 IGMPv2 LEAVE processing functionality no longer works for a multicast group after receipt of IGMPv1 group specific membership query (GSMQ) packet when operating in IGMPv2 mode, even when `ip igmp forcedfastleave 1-24` is enabled.

CR_0000127628 In a topology where the host connects to a querier, the querier connects to a non-querier switch, the non-querier switch connects to a router, and the multicast source is beyond the router, the host might not receive the multicast stream. This happens because a "join" from the host that is received by the querier is not forwarded by the non-querier switch.

CR_0000127974 If a switch receives a PIM packet while it is in the querier election state, the switch gives up the querier role and does not forward multicast traffic.

Include Credentials

CR_0000127700 With include credentials enabled, a config file that is saved to a TFTP server does not contain the SNMPv3 credentials.

LEDs

CR_0000115489 After a PoE error is resolved, the switch turns off the PoE LED but continues to flash the Fault LED.

Loop Protection

CR_0000109506 In some cases, loop protection fails to disable the port.

Policy Based Routing

CR_0000125847 After configuring a policy and applying it to a VLAN, the IP next-hop is unreachable until the switch is rebooted.

Power

CR_0000117394 With J9306A power supplies that have serial numbers beginning with TH in power slots 1 and 2, the bottom 6 interface slots fail to power up, resulting in `tombstone` errors on interface slots G through L.

CR_0000126058 With J9306A power supplies that have serial numbers beginning with TH in power slots 1 and 2, the bottom 6 interface slots fail to power up, resulting in `tombstone` errors on interface slots G through L. This improves the original Power fix (CR_0000117394).

Routing

CR_0000128007 ARP replies from a Microsoft Network Load Balancing (NLB) cluster operating in multicast mode cause the switch to use software routing. This affects v2 zl modules and 3800 switches.

sFlow

CR_0000128567 The switch uses the IP address of the source VLAN as the sFlow packet source, instead of the configured source-interface.

SNMP

CR_0000122658 General MIB file cleanup. Removal of ieee80211.mib and rfc2108.mib and some corrections in others.

CR_0000124375 A switch configured to send syslog messages to a server also sends incorrect SNMP traps, causing `unknown trap` messages in the syslog server.

CR_0000125513 The value stored in MIB object ospfNbrState (OID 1.3.6.1.2.1.14.10.1.6) is incorrect.

SSH

PR_0000072707, CR_0000077550 The switch allows unlimited SSH connection attempts. With this fix, the switch's SSH server goes into a 60-second timeout period after three consecutive unsuccessful login attempts.

Web Management

CR_0000125239 After logging into the switch Web user interface, closing the tab on some Web browsers does not log the user out of the Web session.

Upgrade information

Upgrading restrictions and guidelines

K.15.12.0016 uses BootROM K.15.30. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

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

IMPORTANT: During the software update, the switch automatically boots twice. The switch updates the primary BootROM, then reboots, and then updates the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. Do not interrupt power to the switch during this important update.

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 "show flash" command)	Update directly into software version K.15.12.0015 (BootROM K.15.30)

Contacting HP

For additional information or assistance, contact HP Networking Support:

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.
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

Related information

Documents

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

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.15.12*
- *HP Switch Software Advanced Traffic Management Guide K/KA.15.12*
- *HP Switch Software Basic Operation Guide*
- *HP Switch Software IPv6 Configuration Guide K/KA.15.12*
- *HP Switch Software Management and Configuration Guide K/KA.15.12*
- *HP Switch Software Multicast and Routing Guide K/KA.15.12*
- *HP Switch Software Feature Index — Extended*

Websites

- Official HP Home page: www.hp.com
- HP Networking: www.hp.com/go/networking
- HP product manuals: www.hp.com/support/manuals
- HP download drivers and software: www.hp.com/networking/software
- HP software depot: www.software.hp.com
- HP education services: 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). Include the document title and part number, version number, or the URL when submitting your feedback.