K.15.12.0014 Software Fix List

Contents

Description
Product Models
Enhancements
    Version K.15.12.0006 Enhancements
Prerequisites
Fixes
    Version K.15.12.0006 Fix List
    Version K.15.12.0007 Fix List
    Version K.15.12.0008 Fix List
    Version K.15.12.0009 Fix List
    Version K.15.12.0010 Fix List
    Version K.15.12.0011 Fix List
    Version K.15.12.0012 Fix List
    Version K.15.12.0013 (Never Built)
    Version K.15.12.0014 Fix List

Description

This fix list covers software versions beginning with K.15.12.0006.

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 fix list (below).

Here is a visual depiction of the software sequence, showing how each Major version (for example K.15.12) is based on the previous Major version - and then additional fixes are added to Minor versions (for example K.15.12.0007). This depiction shows the three most recent Major versions and all the Minor versions that have been built at the time of this publication.

```
K.15.10.0003 --> K.15.10.0004 --> K.15.10.0005 --> K.15.10.0006 --> K.15.10.0007 --> K.15.10.0008 -->
        |        K.15.10.0009 --> K.15.10.0010 --> K.15.10.0011 --> K.15.10.0012 --> K.15.10.0013 -->
        |        K.15.10.0014 --> K.15.10.0015 --> K.15.10.0016 --> K.15.10.0017 --> K.15.10.0018 -->
        |        K.15.10.0019 --> K.15.10.0020 --> K.15.10.0021 --> K.15.10.0022 --> K.15.10.0023 -->
        |        K.15.10.0024 --> K.15.10.0025
        |
        v
K.15.11.0003 --> K.15.11.0004 --> K.15.11.0005 --> K.15.11.0007 --> K.15.11.0008 --> K.15.11.0009
        |        (K.15.11.0006 was never built)
        |
        v
K.15.12.0006 --> K.15.12.0007 --> K.15.12.0008 --> K.15.12.0009 --> K.15.12.0010 --> K.15.12.0011-->
                 K.15.12.0012 --> K.15.12.0014
                 (K.15.12.0013 was never built)
```

Included in the K.15.12.0014 "Release Notes Portfolio" pdf are these documents:

- Release Notes Basic Information Guide
- K.15.11.0003 Release Notes
- K.15.12.0014 Fix List

Product Models

HP 3500-24 Switch (J9470A)
HP 3500-24-PoE Switch (J9471A)
HP 3500-48 Switch (J9472A)
HP 3500-48-PoE Switch (J9473A)
HP 3500yl-24G-PWR Intelligent Edge Switch (J8692A)
HP 3500yl-48G-PWR Intelligent Edge Switch (J8693A)
HP 3500yl-24G-PoE+ Switch (J9310A)
HP 3500yl-48G-PoE+ Switch (J9311A)
HP 5406zl Intelligent Edge Switch (J8697A)
HP 5406zl Switch with Premium SW (J9642A)
HP 5412zl Intelligent Edge Switch (J8698A)
HP 5412 zl Switch with Premium SW (J9643A)
HP 5406zl-48G Intelligent Edge Switch (J8699A)
HP 5412zl-96G Intelligent Edge Switch (J8700A)
HP 5406zl-48G-PoE+ Switch (J9447A)
HP 5412zl-96G-PoE+ Switch (J9448A)
HP 5406-44G-PoE+/2XG-SFP+ v2 zl Switch (J9533A)
HP 5412-92G-PoE+/2XG-SFP+ v2 zl Switch (J9532A)
HP 5406-44G-PoE+/4G-SFP v2 zl Switch (J9539A)
HP 5412-92G-PoE+/4G-SFP v2 zl Switch (J9540A)
HP 5406 8p 10GBASE-T 8p 10GbE SFP+ v2 zl Switch with Premium Software (J9866A)
HP 6200yl-24G-mGBIC Switch (J8992A)
HP 6600-24G Switch (J9263A)
HP 6600-24G-4XG Switch (J9264A)
HP 6600-24XG Switch (J9265A)
HP 6600-48G Switch (J9451A)
HP 6600-48G-4XG Switch (J9452A)
HP 8206zl Switch (J9475A)
HP 8206 v2 zl Switch with Premium SW (J9640A)
HP 8212zl Switch (J8715A, J8715B)
HP 8212zl Switch with fan tray (J9091A)
HP 8212 v2 zl Switch with Premium SW (J9641A)
HP 8206-44G-PoE+/2XG v2 zl Switch with Premium SW (J9638A)
HP 8212-92G-PoE+/2XG v2 zl Switch with Premium SW (J9639A)

Enhancements

Version K.15.12.0006 Enhancements

Enhancement (PR_0000065038, CR_0000072256) - All Task Core Dump. The coredump file now includes all tasks that are operating when the switch crashes.

Enhancement (PR_0000072866, CR_0000077692) - RADIUS IPv6. This enhancement adds IPv6 capabilities for the RADIUS client. The Network Access Server will be 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.

Enhancement (CR_0000113486) - Readable Interface Names in Traps. 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.

Enhancement (CR_0000119734) - Event Log Severity Changes. 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.

Enhancement (CR_0000122671) - Strict Priority Queueing. 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.

Enhancement (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.

Prerequisites

BootROM Update Included!

IMPORTANT: If your switch is running a software version earlier than K.15, your BootROM will be updated when you upload K.15.12.xxxx 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. Please see details in the table below.

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.15.12.0014 (BootROM K.15.30)

Minimum Software Versions

Product Number	Product Name	Minimum Supported 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
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.14.31
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
J9263A	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 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

Fixes

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

Version K.15.12.0006 Fix List

Status: Released and fully supported, and posted on the web.

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`.

Crash (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 will 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).

Distributed Trunking (CR_0000125623) - After rebooting a switch participating in a distributed LACP trunk, a distributed trunk port that is disconnected will not link after it is connected.

Distributed Trunking (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.

Enhancement (PR_0000065038, CR_0000072256) - All Task Core Dump. The coredump file now includes all tasks that are operating when the switch crashes.

Enhancement (PR_0000072866, CR_0000077692) - RADIUS IPv6. This enhancement adds IPv6 capabilities for the RADIUS client. The Network Access Server will be 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.

Enhancement (CR_0000113486) - Readable Interface Names in Traps. 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.

Enhancement (CR_0000119734) - Event Log Severity Changes. 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.

Enhancement (CR_0000122671) - Strict Priority Queueing. 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.

Enhancement (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 (CR_0000127230) - Sucessful 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.

IGMP (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.

IGMP (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.

Power (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.

SNMP (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.

SNMP (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.

Version K.15.12.0007 Fix List

Status: Released and fully supported, but not posted on the web.

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.15.12.0008 Fix List

Status: Never released.

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 for only 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`.

Crash (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`.

Crash (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.

Distributed Trunking (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.

GVRP (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.

Passwords (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`.

PIM (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 **distributed-trunking 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 link. This has been observed with X2-SC SR Optics (J8436A) that have MYxxxxxxxx serial numbers.

Transceivers (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`.

Transceivers (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.15.12.0009 Fix List

Status: Released and fully supported, but not posted on the web.

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.15.12.0010 Fix List

Status: Released and fully supported, and posted on the web.

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.

Config (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) - 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`. This improves the original Crash fix (CR_0000120116).

Crash (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`.

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

Crash (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.

IGMP (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.

IGMP (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 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 were configured as 1000-full, the link will go 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 in order 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 area-scope 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.15.12.0011 Fix List

Status: Released and fully supported, but not posted on the web.

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.15.12.0012 Fix List

Status: Released and fully supported, and posted on the web.

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.

Config (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`.

Crash (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`.

Crash (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`.

Crash (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`.

Crash (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.

Crash (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.

Jumbo Frames (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 will temporarily drop.

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.

Web Management (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.15.12.0013

Status: Never built.

Version K.15.12.0014 Fix List

Status: Released and fully supported, and posted on the web.

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 will reboot unexpectedly with a message similar to `Software exception at block.c:1165 -- in 'SIGIO Task', task ID = 0xa989fc0 -> Routing Stack: Assert Failed`.

Crash (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`.

Crash (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`.

Crash (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` repeatedly.
. Pressing the "LED Mode" button has no effect (the mode selection does not change).

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`.

© Copyright 2014 Hewlett-Packard Company, L.P.
The information contained herein is subject to change without notice.

January 2014