WB.15.12.xxxx Software Fix List

Description

This fix list covers software versions beginning with WB.15.12. (WB.15.11.0003 was the first software version for the HP 2920 switches.)

Supersedes

WB.15.11.0003

Product Models

HP 2920-24G Switch (J9726A)
HP 2920-48G Switch (J9728A)
HP 2920-24G-PoE+ Switch (J9727A)
HP 2920-48G-PoE+ Switch (J9729A)
HP 2920-48G-PoE+ 740W Switch (J9836A)

Prerequisites

Minimum Software Versions

Product Number	Product Name	Minimum Supported Software Version
J9805A	HP 640 Redundant/External PS Shelf	WB.15.13.0003

Fixes

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

WB.15.11.0003 was the first software version for the HP 2920 switches.

Version WB.15.12.0006 Fix List

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

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_0000106140) - Flight Data Recorder Phase 2. The Flight Data Recorder provides a way to capture and preserve data that is related to a crash event. Phase 2 adds the capture and preservation of protocol and subsystem-specific information.

Enhancement (CR_0000107011) - CDPv2 Transmit Capability. When a Cisco VoIP phone boots up (or sometimes periodically), it queries the switch and advertises information about itself using CDPv2. The switch receives the VoIP VLAN Query TLV (type 0x0f) from the phone and then immediately sends the voice VLAN ID in a reply packet to the phone using the VLAN Reply TLV (type 0x0e). The phone then begins tagging all packets with the advertised voice VLAN ID.

Enhancement (CR_0000109154) - OpenFlow. OpenFlow is a programmable open-standard network protocol that uses flexible matching rules to classify and manage network traffic into flows. For more information, see the *OpenFlow Configuration Guide*.

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.

Loop Protection (CR_0000109506) - In some cases, loop protection fails to disable the port.

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.

Version WB.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`.

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 WB.15.12.0008 Fix List

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

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.
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.`

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.

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.

IGMP (CR_0000134412) - The switch sends an IGMP General Query with an incorrect layer 2 destination address.

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.

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.

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.

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 WB.15.12.0009 Fix List

Status: Never built.

Version WB.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`.

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.

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.)

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.

Web Management (CR_0000135883) - The "Rx Errors" column is missing from the Web user interface.

August 2013