

WB.15.13.xxxx Software Fix List

Description

This fix list covers software versions beginning with WB.15.13. For fixes in earlier software versions, please see the WB.15.12.0006 release notes that are included in the current software zip file.

Supersedes

WB.15.12.0006

Product Models

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

Prerequisites

BootROM Update Included!

BootROM updates are needed to be able to boot specified switch software versions. In most cases, selected software versions are used to automatically update the BootROM.

This software includes an update to BootROM WB.15.05. If your switch has an older version of BootROM, the BootROM will be updated with this WB.15.13.xxxx software. During the software update, the switch will automatically boot twice, first to update the BootROM to the proper version, and then to load the system software. 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.**

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.15.13.0003 Fix List

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

802.1X (CR_0000134257) - After 802.1X frame counters reach a maximum value of 2,147,483,647, the counters are displayed as negative values that become smaller until they reach zero. When the counters reach zero, they begin incrementing again.

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.

BootROM (CR_0000133411) - This software version includes a BootROM update to BootROM version WB.15.05.

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.

Crash (CR_0000118301) - With several trunks that contain a large number of VLANs (on the order of 1000), the switch might reboot unexpectedly with a message similar to Slot A subsystem went down: 07/17/12 18:19:11 K.15.09.0003 1571, Software exception at msgSys.c:552 -- in 'mNSR', task ID = 0xaa2bdc0, -> Can't get message buffer for msgSys_recv.

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_0000127335) - In some situations, issuing the **show tech all** command might cause the switch to reboot unexpectedly with a message similar to Length Corruption.

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.

DHCP (CR_0000128754) - If the switch is a DHCP client and the DHCP reply contains option 43 with sub-option codes that conflict with RFC 2132 options, the switch might use incorrect settings such as an incorrect subnet mask.

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.

Enhancement (PR_0000070948, CR_0000075993) - RPVST+. RPVST+ is a proprietary spanning tree implementation that extends RSTP (802.1w) to run a separate spanning tree for each VLAN on the switch, and ensures that only one active, loop-free path exists between any two nodes on a given VLAN. See "Rapid per-VLAN spanning tree (RPVST+) operation" in the *Advanced Traffic Management Guide* for your switch.

Enhancement (CR_0000109789) - Identification Field in Static Route Config. When there are a large number of static point-to-point routes, it is helpful to be able to identify the routes using a more meaningful designation than the IP Address. The **name** option allows you to name each configured static route, or to uniquely identify a set of static routes. See "Static Routing" in the *Multicast and Routing Guide* for your switch.

Enhancement (CR_0000111562) - Per-Interface Syslog Event Enable-Disable. This feature provides a per-port filter that can restrict the logging of events that are associated with a link status change. Unimportant linkup/linkdown events can be filtered out, avoiding unwanted messages in the event log and reducing troubleshooting time. See "Troubleshooting" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000112411) - Local Alarm Threshold. The CLI now supports the configuration of RMON alarm threshold settings. The settings can be saved in the configuration file. See "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000115448) - Disable Debug Without Stopping Syslog. When a syslog server is configured, the forwarding of events begins immediately. The commands **no debug event** or **no debug all** no longer have any effect. The only way to disable the forwarding of events to the Syslog server is by removing the server with the **no logging <ip-address>** command, or the **no logging** command, which removes all Syslog servers. See "Troubleshooting" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000123302) - Clear DHCP Snooping Counters via CLI. Clears all the statistics counters for DHCP snooping. The statistics are reset to zero. Syntax: **clear dhcp-snooping statistics**.

Enhancement (CR_0000125930) - Comware CLI Commands in ProVision Software. These commands allow a Comware CLI proficient user to use their Comware CLI knowledge to effectively manage and configure ProVision software switches. There are now 245 Comware display commands in the ProVision software CLI. In addition, a number of extended help messages have been added to the tab help system to provide guidance on the next action for those configuration items that may not be intuitive due to naming or concept differences between Comware and ProVision software. For details, see the *Comware CLI Commands in ProVision Software* manual.

Enhancement (CR_0000135055) - Adds support for the J9805A HP 640 Redundant/External PS Shelf.

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.

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

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.

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_0000122054) - When a large number of traps are generated in a short period of time, the switch buffers might be exhausted. With this fix, switch buffers are protected by several methods, including removing duplicate/identical traps and combining individual intra-switch messages.

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.

SNMP (CR_0000126364) - SNMP support for DHCP Relay Information (option 82) was inadvertently disabled.

SNMP (CR_0000129191) - When an SNMP trap destination is set for "no destinations", the log reports an entry of `unknown var type` when the event happens. Also, when the SNMP trap destination is set for "trap receivers only", traps are not sent.

SSL (CR_0000127972) - A self-signed certificate cannot use a common name (CNAME) longer than 40 characters. With this fix, the limit is 90 characters.

Stacking (CR_0000125606) - After issuing a **boot system flash** command, the Stack Commander erroneously reports that the member switches crashed.

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.

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.

