

# WB.15.14.0007 Software Fix List

## Contents

[Description](#)

[Product Models](#)

[Enhancements](#)

[Version WB.15.14.0002 Enhancements](#)

[Version WB.15.14.0007 Enhancement](#)

[Prerequisites](#)

[Fixes](#)

[Version WB.15.14.0002 Fix List](#)

[Version WB.15.14.0003 \(Never Built\)](#)

[Version WB.15.14.0004 \(Never Built\)](#)

[Version WB.15.14.0005 \(Never Built\)](#)

[Version WB.15.14.0006 Fix List](#)

[Version WB.15.14.0007 Fix List](#)

## Description

This fix list covers software versions beginning with WB.15.14.0002.

Version WB.15.14.0002 was the initial release of Major version WB.15.14 software. WB.15.14.0002 software was built from the same source as WB.15.13.0003. WB.15.14.0002 includes all enhancements and fixes in WB.15.13.0003 software, plus the additional enhancements and fixes in the WB.15.14.0002 fix list (below).

Here is a visual depiction of the software sequence, showing how each Major version (for example WB.15.13) is based on the previous Major version - and then additional fixes are added to Minor versions (for example WB.15.13.0004). This depiction shows the three most recent Major versions and all the Minor versions that have been built at the time of this publication.

```
WB.15.12.0006 --> WB.15.12.0007 --> WB.15.12.0008 --> WB.15.12.0010 --> WB.15.12.0011 -->
    |
    |   WB.15.12.0012 --> WB.15.12.0013 --> WB.15.12.0014 --> WB.15.12.0015
    |   (WB.15.12.0009 was never built)
    v
WB.15.13.0003 --> WB.15.13.0004 --> WB.15.13.0005 --> WB.15.13.0006 --> WB.15.13.0007
    |
    |   WB.15.13.0008
    v
WB.15.14.0002 --> WB.15.14.0006 --> WB.15.14.0007
                (WB.15.14.0003, .0004, and .0005 were never built)
```

These documents are included in the WB.15.14.0007 software zip file:

- Release Notes Basic Information Guide
- WB.15.12.0006 Release Notes
- WB.15.13.0003 Fix List
- WB.15.14.0007 Fix List

## 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)

## Enhancements

### Version WB.15.14.0002 Enhancements

**Enhancement (CR\_0000134999)** - Chassis Locate LED at Boot. The **chassislocate** command has an optional parameter that configures it to run in the future instead of immediately. See Appendix C "Troubleshooting" in the *Management and Configuration Guide* for your switch.

**Enhancement (CR\_0000129524)** - DHCPv4 Snooping Max Binding. DHCP snooping max-binding prevents binding entries from getting exhausted. This feature is on a per-port basis and restricts the maximum number of bindings allowed on a port/interface. The maximum bindings for a particular port includes both statically configured and dynamically learned. The number of bindings on a per port basis is incremented upon a lease offer and decremented upon a lease expiry or release. See "Port Security" in the *Access Security Guide* for your switch.

**Enhancement (CR\_0000127014)** - Filtering PVID Mismatch Log Messages. This enhancement filters out PVID mismatch log messages on a per-port basis. PVID mismatches are logged when there is a difference in the PVID advertised by a neighboring switch and the PVID of the switch port which receives the LLDP advertisement. However, if these events are logged too frequently, they can overwhelm the log buffer and push relevant logging data out of log memory, making it difficult to troubleshoot another issue. See "Troubleshooting" in the *Management and Configuration Guide* for your switch.

**Enhancement (CR\_0000140539)** - FIPS Mocana 5.7 Upgrade. The internal security/cryptography code has been improved to prevent circumvention. (This does not affect YB-software.)

**Enhancement (CR\_0000127160)** - Link Aggregation Control Protocol-Multi-Active Detection (LACP-MAD) is a detection mechanism deployed by switches to recover from a breakup of the Intelligent Resilient Framework (IRF) stack due to link or other failure. See "Port Trunking" in the *Management and Configuration Guide* for your switch.

**Enhancement (CR\_0000128955)** - Local MAC Authentication (LMA). LMA is a software feature that simplifies deployment for devices such as IP phones and security cameras. In general, it provides dynamic attribute assignment (e.g., VLAN and QoS) through the use of a locally configured authentication repository. The most common use model for LMA is to automatically assign a VLAN to IP phones. In some cases, it can also provide rudimentary access security for the network. See "Web and MAC Authentication" in the *Access Security Guide* for your switch.

**Enhancement (CR\_0000138355)** - OpenFlow 1.3 Support. OpenFlow controllers can securely connect to HP VAN SDN Controllers via a set of commands that establish and maintain the security certification. See the *OpenFlow Administrator's Guide* for your switch.

**Enhancement (CR\_0000131581)** - Smartlink is a switch feature that provides effective, simple and fast-converging link redundancy in network topology with dual uplink between different layers of the network. It requires an active (master) and a backup (slave) link. The active link carries the uplink traffic. Upon failure of the active link, a switchover is triggered and the traffic is directed to the backup link. See "Smartlink" in the *Advanced Traffic Management Guide* for your switch.

**Enhancement (CR\_0000135708)** - SNMP Trap When MAC Address Table Changes. This enhancement causes an SNMP trap to be generated once a laptop/PC is removed from the back of an IP phone and the laptop/PC MAC address ages out of the MAC table. See "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

## Version WB.15.14.0007 Enhancement

**Enhancement (CR\_0000132845)** - Additional Debug Capability. This enhancement adds tracking to identify possible switch hang situations during switch boot.

## 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 version WB.15.05. If your switch has an older version of BootROM, the BootROM will be updated with this WB.15.14.0007 software.

During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update 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.**

### 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 software version listed below includes all the software fixes and enhancements added in previous versions listed below.**

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

### Version WB.15.14.0002 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.

**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\_0000136428)** - CLI output for **show ip igmp vlan x conf** displays a plus sign under the Interconnect Trunk column heading, and nothing (blank) under the Port column heading.

**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.

**CLI (CR\_0000138493)** - The error message is not clear when the user attempts to create an overlapping network on a switch.

**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.

**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.

**Config (CR\_0000139251)** - When a configuration file is downloaded to the switch, a default SNMPv3 user named "initial" is created on the switch even though it is not in the config file.

**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\_0000127791)** - 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\_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.

**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 (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.

**Enhancement (CR\_0000134999)** - Chassis Locate LED at Boot. The **chassislocate** command has an optional parameter that configures it to run in the future instead of immediately. See Appendix C "Troubleshooting" in the *Management and Configuration Guide* for your switch.

**Enhancement (CR\_0000129524)** - DHCPv4 Snooping Max Binding. DHCP snooping max-binding prevents binding entries from getting exhausted. This feature is on a per-port basis and restricts the maximum number of bindings allowed on a port/interface. The maximum bindings for a particular port includes both statically configured and dynamically learned. The number of bindings on a per port basis is incremented upon a lease offer and decremented upon a lease expiry or release. See "Port Security" in the *Access Security Guide* for your switch.

**Enhancement (CR\_0000127014)** - Filtering PVID Mismatch Log Messages. This enhancement filters out PVID mismatch log messages on a per-port basis. PVID mismatches are logged when there is a difference in the PVID advertised by a neighboring switch and the PVID of the switch port which receives the LLDP advertisement. However, if these events are logged too frequently, they can overwhelm the log buffer and push relevant logging data out of log memory, making it difficult to troubleshoot another issue. See "Troubleshooting" in the *Management and Configuration Guide* for your switch.

**Enhancement (CR\_0000140539)** - FIPS Mocana 5.7 Upgrade. The internal security/cryptography code has been improved to prevent circumvention. (This does not affect YB-software.)

**Enhancement (CR\_0000127160)** - Link Aggregation Control Protocol-Multi-Active Detection (LACP-MAD) is a detection mechanism deployed by switches to recover from a breakup of the Intelligent Resilient Framework (IRF) stack due to link or other failure. See "Port Trunking" in the *Management and Configuration Guide* for your switch.

**Enhancement (CR\_0000128955)** - Local MAC Authentication (LMA). LMA is a software feature that simplifies deployment for devices such as IP phones and security cameras. In general, it provides dynamic attribute assignment (e.g., VLAN and QoS) through the use of a locally configured authentication repository. The most common use model for LMA is to automatically assign a VLAN to IP phones. In some cases, it can also provide rudimentary access security for the network. See "Web and MAC Authentication" in the *Access Security Guide* for your switch.

**Enhancement (CR\_0000138355)** - OpenFlow 1.3 Support. OpenFlow controllers can securely connect to HP VAN SDN Controllers via a set of commands that establish and maintain the security certification. See the *OpenFlow Administrator's Guide* for your switch.

**Enhancement (CR\_0000131581)** - Smartlink is a switch feature that provides effective, simple and fast-converging link redundancy in network topology with dual uplink between different layers of the network. It requires an active (master) and a backup (slave) link. The active link carries the uplink traffic. Upon failure of the active link, a switchover is triggered and the traffic is directed to the backup link. See "Smartlink" in the *Advanced Traffic Management Guide* for your switch.

**Enhancement (CR\_0000135708)** - SNMP Trap When MAC Address Table Changes. This enhancement causes an SNMP trap to be generated once a laptop/PC is removed from the back of an IP phone and the laptop/PC MAC address ages out of the MAC table. See "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

**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.

**GVRP (CR\_0000130090)** - After rebooting the switch, the configuration **unknown-vlans disable** does not work on trunks.

**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.

**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\_0000134412)** - The switch sends an IGMP General Query with an incorrect layer 2 destination 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.

**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.

**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.

**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.

**MAC Authentication (CR\_0000129991)** - MAC Authentication fails when the **peap-mschapv2** parameter is included in the **aaa authentication** CLI command.

**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 which password is changed.

**Policy Based Routing (CR\_0000134936)** - The **show statistics policy** counter is not reset by the **clear statistics policy** command.

**RADIUS Accounting (CR\_0000137793)** - An interim-update status request generates incorrect accounting information in the RADIUS server. This issue was introduced with CR\_0000123330.

**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.

**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.

**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\_0000135477)** - A trap from an undocumented OID can be triggered under certain conditions. With this fix, OID 1.3.6.1.4.1.11.2.3.7.11.107.0.2 has been added to the MIB.

**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.

**TFTP (CR\_0000123187)** - TFTP file transfers initiated via TELNET or SSH fail, if the **console inactivity-timer** setting causes the TELNET or SSH session to end during the transfer. This issue does not affect file transfers initiated via the console or via SFTP.

**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.

**Trunking (CR\_0000126473)** - The switch does not allow a static LACP trunk to be configured as active or passive. This fix adds a new interface command: **lACP static [active | passive]**.

**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.

**Web Management (CR\_0000135883)** - The "Rx Errors" column is missing from the Web user interface.

**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 WB.15.14.0003

Status: Never built.

## Version WB.15.14.0004

Status: Never built.

## Version WB.15.14.0005

Status: Never built.

## Version WB.15.14.0006 Fix List

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

**CLI (CR\_0000141831)** - The output of **show system temperature** gives incorrect and extra information. With this fix, the switch output displays `Chassis` instead of `Sys-1`, the correct threshold is displayed, and extra lines (for example, `Sys-2`) are removed.

**CLI (CR\_0000143576)** - The switch does not allow users to configure a port with the setting **speed-duplex auto-10-100**.

**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).

**Config (CR\_0000142393)** - Upgrading software from WB.15.11.xxxx to a newer version changes the **console inactivity-timer** from the configured value in minutes to that same value in seconds. Also, if the **console idle-timeout** value is set, after reboot the configured value is used for a console connection but not a TELNET connection.

**Config (CR\_0000145562)** - A switch with an active radio port and configured with the command **lldp auto-provision radio-ports auto-vlan 2100** will move the radio ports into VLAN 2101 after a reboot. Similar errors occur for other **auto-vlan** numbers; after reboot the switch creates and uses a new VLAN instead of using the configured VLAN for radio ports.

**Console (CR\_0000140941)** - The **console inactivity-timer** setting is applied even if the user is typing on the console, when the console physical connection is to a stack member instead of the commander.

**Counters (CR\_0000141119)** - The output of **show ip counters** is incorrect when routing is enabled for IP, IPv6, or multicasts.

**Counters (CR\_0000142198)** - When a trunk configured for sFlow polling is simultaneously queried via SNMP, all counter values for the trunk are zero.

**Counters (CR\_0000143860)** - On a switch configured with rapid PVST and BPDU protection, the output of the command **show spanning-tree bpduprotection** 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\_0000142238)** - From the menu, after selecting "Status and Counters" and "Port Address Table" for an active port, the switch might reboot unexpectedly with a message similar to Read Error Restr Mem Access HW Addr=0x2020201c IP=0x4ee7ce8 Task='mSess1' Task ID=0xe087cc0 fp: 0x06cefc48 sp:0x06cefc20 cpsr: 0x2000001f dfsr: 0x00000005.

**Crash (CR\_0000143459)** - When a switch is added to a physical stack, if either the new switch or the stack (but not both) is running a version of software listed below, the stack might reboot unexpectedly with a message similar to Software exception at proStackUtil.c:137 -- in 'mStackingCtrl', task ID = 0x3c940dc0. The applicable software versions are KA.15.12.0012 (for 3800 switches), and WB.15.12.0012 and WB.15.12.0013 (for 2920 switches).

**Crash (CR\_0000144879)** - The switch might reboot unexpectedly in these 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 btLrn.c:2616 -- in 'mLpmgrCtrl', task ID = 0xa98a9c0 -> Mac Table Error.

**Crash (CR\_0000145024)** - With local MAC authentication enabled, issuing the **show run** command causes a small decrease in the switch's available memory. Over time if memory becomes depleted, the switch might reboot unexpectedly with a message similar to Software exception at cli\_show\_config.c:667 -- in 'mSess6', task ID = 0xa965540.

**Crash (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.

**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**.



**Fastboot (CR\_0000141043)** - If the fastboot setting is changed by the user, and the switch experiences a power interruption or reboot while the new setting is being written to flash, upon bootup the MAC address on a switch or stack member might be erased. Note that this fix has a side effect: If the fastboot setting is changed by the user and the switch software is downgraded (changed to an earlier version), upon bootup the fastboot setting might revert to what it was before the user-initiated change, even though the switch reports that it has been changed. Workaround: Change the fastboot setting twice - first change it back to what it was before the user-initiated change, then change fastboot to the desired setting.

**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.

**IGMP (CR\_0000140514)** - After disabling IGMP forwarding on a port, multicast traffic incorrectly continues to flow from that port.

**IP Phones (CR\_0000147849)** - Alcatel phones might reboot unexpectedly when connected to a switch configured for IP phones to use MAC authentication and for PCs to use 802.1X authentication.

**Logging (CR\_0000143781)** - When some events occur on a stack, if the event happens on the Standby switch, the switch fails to generate an event log entry, a syslog entry, or an SNMP trap. Examples are disconnecting the RPS cable, and removing a module from the back of the switch.

**Logging (CR\_0000144926)** - When some events occur on a stack, if the event happens on the Standby switch, the switch fails to generate an event log entry, a syslog entry, or an SNMP trap. This fix adds additional events to those included in the original Logging fix (CR\_0000143781), also in 15.15 software.

**Meshing (CR\_0000143068)** - Multicast traffic and unicast traffic with unknown destination addresses are not routed over the mesh.

**MSTP (CR\_0000134194)** - With Spanning Tree enabled, configuring a live port as an **admin-edge-port** causes the output of **show run** to display a fixed path-cost for that port in the IST (for example, `spanning-tree instance ist 5 path-cost 20000`). Note that this is a display issue only, the switch uses the automatic path-cost based on the link speed.

**Multicast (CR\_0000138817)** - When a multicast stream is sent to a reserved multicast address, a General Query might not be forwarded by the switch, causing clients to be dropped from the multicast stream.

**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.

**Transceivers (CR\_0000143444)** - 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`. This is the same fix as CR\_0000132781 in 15.13.0003, which was inadvertently removed by CR\_0000126473 in 15.13.0004 software.

## Version WB.15.14.0007 Fix List

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

**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\_0000142154)** - The output of **show tech** halts after displaying **show debug buffer**, with the message `=== The command has completed with errors. ===`.

**CLI (CR\_0000145812)** - A new command **tcp-push-preserve** is added. This command is enabled by default, and causes TCP packets with the "push" flag to be sent before other packets in the queue. Note that high concentrations of TCP packets with push flags under certain conditions can destabilize your network. Use the **no** form of this command to disable the feature.

**CLI (CR\_0000148661)** - When the output of **show power-over-ethernet brief** displays a Detection Status of either Searching or Delivering for a port, the **show tech all "poe\_status\_port all"** section displays Other Fault as the Detect Stat.

**CLI (CR\_0000149525)** - The switch incorrectly allows a user to enable stacking when more than four MSTP instances are configured.

**CLI (CR\_0000150144)** - The output of **show dhcp-relay bootp-gateway vlan <VLAN\_number>** gives an incorrect BOOTP Gateway address for VLANs that are not configured for DHCP relay.

**Console (CR\_0000148468)** - With a console cable connected to a stack member, if the user issues the **show tech all** command and then attempts to cancel the output by entering **<CTRL-C>**, the output pauses but then continues for a long time (up to 30 minutes for a five-member stack). Note that the fix has a small side-effect: Entering **<CTRL-C>** will cause a short delay before the console prompt returns.

**Crash (CR\_0000147367)** - After a PoE switch is removed from the stack, issuing the command **show power-over-ethernet brief** from the Commander might cause the Commander to reboot unexpectedly with a message similar to `Health Monitor: Read Error Restr Mem Access HW Addr=0x9f6a5cf8 IP=0x7d27d78 Task='mSess1' Task ID=0x13ac6900 fp: 0x0d8544d8 sp:0x0d8544cc cpsr: 0xa000001f`.

**Enhancement (CR\_0000132845)** - Additional Debug Capability. This enhancement adds tracking to identify possible switch hang situations during switch boot.

**IPv6 (CR\_0000148594)** - IPv6 Router Advertisements that indicate an off-link prefix are not set as "preferred" in the switch, which causes incorrect information in the output of **show ipv6**, and can affect connectivity to hosts that use IPv6 Stateless Address Autoconfiguration. This issue also causes the sFlow "Agent Address" to be listed as 0.0.0.0.

**Logging (CR\_0000146773)** - In an IPv4 plus IPv6 environment, upon switch bootup the event log displays the set of source IP policy ("srcip") messages twice. With this fix, IPv6 policy messages are distinguished from IPv4 policy messages.

**Logging (CR\_0000150244)** - Some RMON events are not correctly defined for fault-finder (FFI), SSL, and virus throttling, which causes the switch to report an error such as `system: Unknown Event ID 776` when those events occur.

**Management (CR\_0000149528)** - In some situations with multiple TELNET and/or SSH sessions established, the switch does not accept additional management sessions even if some of the existing ones are killed, responding with the message `Sorry, the maximum number of sessions are active. Try again later.`

**OpenFlow (CR\_0000142663)** - The switch sends an error message to the controller in response to a multipart flow statistics request.

**PoE (CR\_0000147518)** - After reboot, pre-standard detection of PoE devices does not function correctly on a 2920 or 3800 stack, if the stack commander is a non-PoE switch.

**PoE (CR\_0000148808)** - After disabling PoE on one or more ports, the output of `show cpu slot <slot-number>` shows an increase in CPU utilization of 15% or more.

**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.

**SNMP (CR\_0000149657)** - When using the "createAndWait" mode to set parameters via SNMP, multiple RADIUS servers cannot be configured.

**SNMP (CR\_0000151035)** - The switch incorrectly reports that MIB object `entPhysicalIsFRU = False` for removable fantrays and transceivers.

**Stacking (CR\_0000146890)** - When the stacking cable is removed from a two-switch stack, both switches show "Stack Status" of `Fragment Active`.

**Switch Hang (CR\_0000146247)** - With both authentication and accounting enabled, the switch might become unresponsive to management, requiring a reboot to recover.

**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.

**Web Management (CR\_0000149099)** - When Spanning Tree Protocol (STP) is enabled via the Web user interface, "mstp" is shown as the default STP mode, and "mstp" is displayed as the operational mode after the user enables STP and saves the change. However, the command line interface shows that the switch operates in "rpvst" mode. Workaround: From the Web user interface, use the dropdown menu to explicitly select "mstp" from the dropdown options, then save the change.

