

# WB.15.16.0005 Release Notes

## Abstract

This document contains supplemental information for the WB.15.16.0005 release.



© Copyright 2014 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

#### **Acknowledgments**

Microsoft®, Windows®, and Windows Server® are U.S. registered trademarks of the Microsoft group of companies.

---

# Contents

1	WB.15.16.0005 Release Notes.....	5
	Description.....	5
	Important information.....	5
	Version history.....	5
	Products supported.....	6
	Minimum supported software versions.....	6
	Compatibility/interoperability.....	6
	Enhancements.....	6
	Version WB.15.16.0005.....	7
	Version WB.15.16.0004.....	7
	BYOD redirect (CR_0000152339).....	7
	CPU Protection (CR_0000124429).....	7
	DHCPv4 (CR_0000128651).....	7
	DHCPv6 (CR_0000144107).....	7
	DHCPv6 Snooping (CR_0000137520).....	7
	Generic header ID (CR_0000144861).....	7
	MAC-based VLANs (CR_0000128831).....	7
	UDLD (CR_0000147189).....	7
	VLAN (CR_0000145339).....	7
	Fixes.....	8
	Version WB.15.16.0005.....	8
	Version WB.15.16.0004.....	8
	802.1X (CR_0000149780).....	8
	Authentication (CR_0000148832).....	8
	CLI (CR_0000145136).....	8
	CLI (CR_0000145812).....	8
	CLI (CR_0000148661).....	8
	CLI (CR_0000149525).....	8
	CLI (CR_0000150144).....	8
	CLI (CR_0000152440).....	8
	Configuration (CR_0000149526).....	9
	Configuration (CR_0000152757).....	9
	Console (CR_0000148468).....	9
	Counters (CR_0000149229).....	9
	Counters (CR_0000151412).....	9
	Counters (CR_0000151415).....	9
	CPU utilization (CR_0000151164).....	9
	Crash (CR_0000115372).....	9
	Crash (CR_0000146176).....	9
	Crash (CR_0000151102).....	9
	Crash (CR_0000153386).....	9
	Crash (CR_0000154053).....	10
	Crash (CR_0000154769).....	10
	Crash messaging (CR_0000150468).....	10
	File transfer (CR_0000145212).....	10
	File transfer (CR_0000148584).....	10
	ICMP (CR_0000155702).....	10
	IGMP (CR_0000128678).....	10
	IP phones (CR_0000137652).....	10
	IP phones (CR_0000147849).....	10
	IPv6 (CR_0000148594).....	10

Latency (CR_0000129743).....	10
Logging (CR_0000146773).....	11
Logging (CR_0000149891).....	11
Logging (CR_0000150244).....	11
Management (CR_0000149528).....	11
Management (CR_0000155717).....	11
PoE (CR_0000147518).....	11
PoE (CR_0000148808).....	11
sFlow (CR_0000147660).....	11
SNMP (CR_0000131055).....	11
SNMP (CR_0000149657).....	11
SNMP (CR_0000151035).....	12
SNMP (CR_0000154463).....	12
Stacking (CR_0000146890).....	12
Stacking (CR_0000154380).....	12
Switch hang (CR_0000154152).....	12
Web management (CR_0000149099).....	12
Web management (CR_0000149777).....	12
Upgrade information.....	12
Upgrading restrictions and guidelines.....	12
Contacting HP.....	12
HP security policy.....	13
Related information.....	13
Documents.....	13
Websites.....	14
Documentation feedback.....	14

## Description

This release note covers software versions for the WB.15.16 branch of the software.

Version WB.15.16.0004 was the initial release of Major version WB.15.16 software.

WB.15.16.0004 includes all enhancements and fixes in the WB.15.15.0006 software, plus the additional enhancements and fixes in the WB.15.16.0004 enhancements and fixes sections of this release note.

Product series supported by this software:

- HP 2920 Switch Series

## Important information

To avoid damage to your equipment, do not interrupt power to the switch during a software update.

## Version history

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

Version number	Based on	Release date	Remarks
WB.15.16.0005	WB.15.16.0004	2014-11-21	Released, fully supported, and posted on the web.
WB.15.16.0004	WB.15.15.0006	2014-10-30	Initial release of WB.15.16. Released, fully supported, and posted on the web.
WB.15.15.0009	WB.15.15.0008	2014-11-17	Please see the WB.15.15.0009 release note for detailed information on the WB.15.15 branch. Released, fully supported, and posted on the web.
WB.15.15.0008	WB.15.15.0007	2014-09-15	Released, fully supported, and posted on the web
WB.15.15.0007	WB.15.15.0006	2014-06-26	Released, fully supported, and posted on the web
WB.15.15.0006	WB.15.14.0002	2014-03-19	Initial release of WB.15.15. Released, fully supported, and posted on the web
WB.15.14.0010	WB.15.14.0009	2014-11-17	Please see the WB.15.14.0010 release note for detailed information on the WB.15.14 branch. Released, fully supported, and posted on the web
WB.15.14.0009	WB.15.14.0008	2014-09-15	Released, fully supported, and posted on the web
WB.15.14.0008	WB.15.14.0007	2014-07-16	Released, fully supported, and posted on the web
WB.15.14.0007	WB.15.14.0006	2014-07-01	Released, fully supported, and posted on the web,
WB.15.14.0006	WB.15.14.0002	2014-04-01	Released, fully supported, but not posted on the web
WB.15.14.0005		n/a	Never built
WB.15.14.0004		n/a	Never built

Version number	Based on	Release date	Remarks
WB.15.14.0003		n/a	Never built
WB.15.14.0002	First release	2013-10-18	Initial release of WB.15.14

## Products supported

This release applies to the following product models:

Product number	Description
J9726A	HP 2920-24G Switch
J9728A	HP 2920-48G Switch
J9727A	HP 2920-24G-PoE+ Switch
J9729A	HP 2920-48G-PoE+ Switch
J9836A	HP 2920-48G-PoE+ 740W Switch

## Minimum supported software versions

**NOTE:** If your switch or module is not listed in the below table, it runs on all versions of the software.

Product number	Product name	Minimum software version
J9805A	HP 640 Redundant/External PS Shelf	WB.15.13.0003

## Compatibility/interoperability

The switch web agent supports the following operating system and web browser combinations:

Operating System	Supported Web Browsers
Windows XP SP3	Internet Explorer 7, 8 Firefox 12
Windows 7	Internet Explorer 9, 10 Firefox 24 Chrome 30
Windows 8	Internet Explorer 9, 10 Firefox 24 Chrome 30
Windows Server 2008 SP2	Internet Explorer 8, 9 Firefox 24
Windows Server 2012	Internet Explorer 9, 10 Firefox 24
Macintosh OS	Firefox 24

## Enhancements

This section lists enhancements found in the WB.15.16 branch of the software. Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

**NOTE:** The number that follows the enhancement description is used for tracking purposes.

## Version WB.15.16.0005

No enhancements are included in version WB.15.16.0005.

## Version WB.15.16.0004

### BYOD redirect (CR\_0000152339)

BYOD redirect. The switch can now be configured for BYOD (Bring Your Own Device) redirect, which sends the device's credentials to a BYOD server such as IMC, that is configured to control network access.

### CPU Protection (CR\_0000124429)

A port can receive a high volume of spanning tree BPDUs when there is a loop in the connected network. This enhancement prevents the switch CPU from being overwhelmed by limiting the rate at which those BPDUs are sent to the CPU. For more information, see the *Advanced Traffic Management Guide* for your switch.

### DHCPv4 (CR\_0000128651)

DHCPv4 server. The switch can now be configured as a DHCPv4 server. For more information, see the *Management and Configuration Guide* for your switch.

### DHCPv6 (CR\_0000144107)

DHCPv6 hardware addresses. The switch can be configured with option 79 to instruct DHCPv6 relay agents to forward client link-layer addresses. For more information, see the *Management and Configuration Guide* for your switch.

### DHCPv6 Snooping (CR\_0000137520)

DHCPv6 snooping and Dynamic IP Lockdown for IPv6 (DIPLDv6) are now supported. For more information, see the *Access Security Guide* for your switch. These features are not yet supported for YB-software switches.

### Generic header ID (CR\_0000144861)

Generic header ID in configuration file. The switch now allows addition of a generic header ID to configuration files saved on a server. This is used for DHCP Option 67 download requests for configuration files. For more information, see the *Management and Configuration Guide* for your switch.

### MAC-based VLANs (CR\_0000128831)

MAC-Based VLANs (MBV) Enable/Disable. MBV enable/disable options are available using CLI and SNMP. For more information, see the "Web-based and MAC Authentication", and the "Port-Based and User-Based Access Control (802.1X)" chapters in the *Access Security Guide* for your switch.

### UDLD (CR\_0000147189)

UDLD Verify Before Forwarding. Unidirectional Link Detection (UDLD) has been enhanced to account for the situation when the link to the directly-connected device is up, but there is no link on one segment of the path to the remote device. For more information, see the *Management and Configuration Guide* for your switch.

### VLAN (CR\_0000145339)

VLAN Precedence. Beginning with 15.06 software, if a VLAN is added to a port while authenticated clients are connected to that port, the VLAN addition is delayed until all authenticated clients are disconnected. This enhancement allows a tagged VLAN to be applied immediately to a port that

has connected authenticated clients. For more information, see the *Advanced Traffic Management Guide* for your switch.

## Fixes

This section lists released builds that include fixes. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

---

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

---

### Version WB.15.16.0005

No fixes were included in version WB.15.16.0005.

### Version WB.15.16.0004

#### 802.1X (CR\_0000149780)

Already-authenticated clients that send an EAPOL-Start message are de-authenticated by the switch. This situation happens if the client runs Windows Vista and later operating systems that are set to "include learning".

#### 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.

#### CLI (CR\_0000145136)

When the switch is configured with the `console event critical` setting, the event log output of `show tech all` lists only the critical events. With this fix, `show tech all` lists all event log entries.

#### 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.

#### CLI (CR\_0000152440)

The output of `show tech all` halts while displaying `lmaDbUtiltraverseLmaProfTbl`, with the message `=== The command has completed with errors. ===`.



## Configuration (CR\_0000149526)

Enabling stacking on a switch that has a trunk configured creates an invalid entry for the trunk in the configuration file. The resulting configuration file cannot be downloaded to the switch.

## Configuration (CR\_0000152757)

After configuring `snmp-server host` on the Commander, stack member configuration files include two lines with SNMPv3 configuration.

## 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.

## Counters (CR\_0000149229)

The "Route changes" counter in the output of `show ip rip` increments with every RIP update the router receives, even if there are no route changes.

## Counters (CR\_0000151412)

The output of a query for meter statistics gives an incorrect value for OpenFlow meter duration.

## Counters (CR\_0000151415)

The output of a query for port statistics gives an incorrect value for OpenFlow statistics duration.

## CPU utilization (CR\_0000151164)

The switch occasionally reports CPU utilization of 99%. This is a false reading and does not reflect switch performance.

## 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\_0000146176)

After receiving multiple route changes or route flaps in a short period of time, the switch might reboot unexpectedly with a message similar to `Software exception at krt.c:2134 -- in 'eRouteCtrl', task ID = 0xa9bc400 -> Routing Stack: Assert Failed`.

## Crash (CR\_0000151102)

In a rare situation, after a failover to the Standby Management Module (SMM) or the stack's Standby switch, the switch might reboot unexpectedly with a message similar to `Software exception at asicMgrSlaveFilters.c:185 -- in 'mNSA', task ID = 0x1b1fea80 -> Internal Name Server Error`.

## Crash (CR\_0000153386)

When a large number of 802.1X clients are being authenticated, reconfiguring port security modes such as "learn-mode" might cause the switch to reboot unexpectedly with a message similar to `Software exception at multMgmtUtil.c:88 -- in 'mPpmgrCtrl', task ID =0x13b1f940 -> Internal error`.

## Crash (CR\_0000154053)

When the switch has 802.1X-authenticated clients on a VLAN and the user deletes that VLAN, the switch might reboot unexpectedly with a message similar to `Software exception at multMgmtUtil.c:151 -- in 'eChassMgr', task ID = 0x3c945800 -> Internal error.`

## Crash (CR\_0000154769)

With a static IGMP group configured, after issuing the `show run` command, changing the sFlow configuration might cause the switch to reboot unexpectedly with a message similar to `Health Monitor: Restr Mem Access HW Addr=0x60630015 IP=0x1045630 Task='mSnmprCtrl' Task ID=0xa98b4c0 sp:0x47ecc50 lr:0x104a0ac msr: 0x02029200 xer: 0x20000000 cr: 0x48000400.`

## Crash messaging (CR\_0000150468)

The crash message includes extraneous text about filing a CR (Change Request).

## File transfer (CR\_0000145212)

Software downloads via SSL fail with certain browsers, including Internet Explorer versions 7, 8, and 10.

## File transfer (CR\_0000148584)

A configuration file with a blank community name in the `snmp-server host` entry cannot be downloaded to the switch. Although the switch does not allow the `snmp-server host` entry to be configured with a blank community name, earlier software bugs might cause this condition.

## ICMP (CR\_0000155702)

The switch sends a ping request to a random IP address every 20 minutes.

## IGMP (CR\_0000128678)

In certain topologies the IGMPv2 "Leave Group" from one host can cause the multicast stream to be dropped, even though there are other hosts receiving that stream.

## IP phones (CR\_0000137652)

An IP phone that uses the "Automatic Port Synchronization" feature loses its IP address and possibly drops the current call. This has been observed when the switch is configured with the command `cdp mode pre-standard-voice`, and the PC to which the phone is connected goes into hibernation. In that situation the "Automatic Port Synchronization" feature causes the phone to drop and then re-establish link with the switch.

## IP phones (CR\_0000147849)

Alcatel phones might reboot unexpectedly when connected to a switch configured to use MAC authentication for IP phones and to use 802.1X authentication for PCs.

## 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.

## Latency (CR\_0000129743)

When the switch receives a high volume of traffic for unknown destinations, the resulting ARPs sent by the switch in combination with other incoming traffic the switch must process can cause latency

and dropped packets. In this situation, the event log might report `IpAddrMgr: IPAM Control task delayed due to slave message queues too full.`

### 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\_0000149891)

When a user disables layer 3 on a VLAN, the event log message might state that layer 3 was disabled for the wrong VLAN.

### 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.`

### Management (CR\_0000155717)

After disabling the Out of Band Management (OOBM) interface, saving the configuration and rebooting the switch, the OOBM interface does not come up even after it is re-enabled.

### 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\_0000131055)

The MIB object `hpicfDownloadTftpConfig(1.3.6.1.4.1.11.2.14.11.1.3.5)` in switch software has a value of 1 for enabled and 2 for disabled, but the reverse is actually correct. With this fix the MIB object to enable and disable the TFTP client on the switch is changed to `hpicfDownloadTftpClientConfig(1.3.6.1.4.1.11.2.14.11.1.3.12)`. Also, the integer values are corrected so 1 is disabled and 2 is enabled.

### 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, power supplies, and transceivers.

## SNMP (CR\_0000154463)

The switch incorrectly reports that MIB object `entPhysicalIsFRU = False` for transceivers for some switches. This improves the original SNMP fix (CR\_0000151035).

## Stacking (CR\_0000146890)

When the stacking cable is removed from a two-switch stack, both switches show "Stack Status" of `Fragment Active`.

## Stacking (CR\_0000154380)

A failover from Commander to Standby with multiple MSTP instances in operation might cause the stack members and connected devices to be unreachable.

## Switch hang (CR\_0000154152)

If the switch is sending output to the console at the time the switch is rebooted, the switch might hang and not boot properly.

## 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.

## Web management (CR\_0000149777)

After a failover to the Standby Management Module (SMM) or the stack's standby switch, the Web user interface is not accessible via the Out of Band Management (OOBM) port.

# Upgrade information

## Upgrading restrictions and guidelines

A BootROM update is included in this release.

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. The 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.15.16.0005 software.

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

- 
- ❗ **IMPORTANT:** 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.
- 

## Contacting HP

For additional information or assistance, contact HP Networking Support:

[www.hp.com/networking/support](http://www.hp.com/networking/support)

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

## HP security policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

To find security bulletins:

1. Go to the HP Support Center website at [www.hp.com/go/hpsc](http://www.hp.com/go/hpsc).
2. Enter your product name or number and click **Go**.
3. Select your product from the list of results.
4. Click the **Top issues & solutions** tab.
5. Click the **Advisories, bulletins & notices** link.

To initiate a subscription to receive future HP Security Bulletin alerts via email, sign up at:

[www4.hp.com/signup\\_alerts](http://www4.hp.com/signup_alerts)

## Related information

### Documents

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

[www.hp.com/support/manuals](http://www.hp.com/support/manuals)

- Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

### Related documents

The following documents provide related information:

- *HP Switch Software Access Security Guide WB.15.16*
- *HP Switch Software Advanced Traffic Management Guide WB.15.16*
- *HP Switch Software Basic Operation Guide*
- *HP Switch Software IPv6 Configuration Guide WB.15.16*
- *HP Switch Software Management and Configuration Guide WB.15.16*
- *HP Switch Software Multicast and Routing Guide WB.15.16*

## Websites

- Official HP Home page: [www.hp.com](http://www.hp.com)
- HP Networking: [www.hp.com/go/networking](http://www.hp.com/go/networking)
- HP product manuals: [www.hp.com/support/manuals](http://www.hp.com/support/manuals)
- HP download drivers and software: [www.hp.com/support/downloads](http://www.hp.com/support/downloads)
- HP software depot: [www.software.hp.com](http://www.software.hp.com)
- HP education services: [www.hp.com/learn](http://www.hp.com/learn)

## Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback ([docsfeedback@hp.com](mailto:docsfeedback@hp.com)). Include the document title and part number, version number, or the URL when submitting your feedback.