

# WB.15.15.0010 Release Notes

## Abstract

This document contains supplemental information for the WB.15.15.0010 release.

HP Part Number: 5998-7703  
Published: March 2015  
Edition: 1



© Copyright 2015 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 trademarks of the Microsoft group of companies.

---

# Contents

1	WB.15.15.0010 Release Notes.....	6
	Description.....	6
	Important information.....	6
	Version history.....	6
	Products supported.....	7
	Compatibility/interoperability.....	7
	Minimum supported software versions.....	7
	Enhancements.....	8
	Version WB.15.15.0010.....	8
	Configurable TLS.....	8
	Rate Limiting.....	8
	Version WB.15.15.0009.....	9
	Version WB.15.15.0008.....	9
	Version WB.15.15.0007.....	9
	Version WB.15.15.0006 .....	9
	Audit Logging .....	9
	Broadcast Storm .....	9
	Core Dump .....	9
	Debug Capability .....	9
	Inactivity Timer .....	9
	Interface Authentication .....	10
	Password Length .....	10
	Reporting .....	10
	Service Insertion .....	10
	Syslog Messages .....	10
	TLS .....	10
	Fixes.....	10
	Version WB.15.15.0010.....	10
	Accounting.....	10
	Certificate Manager.....	11
	CLI.....	11
	Config.....	11
	Crash.....	11
	LLDP.....	12
	Memory.....	12
	OOBM.....	12
	Rate Limiting.....	12
	Redundant Management.....	13
	Self Test.....	13
	SNMP.....	13
	SSH.....	13
	TFTP.....	13
	Web Management.....	13
	Version WB.15.15.0009.....	13
	APR .....	13
	CLI .....	14
	CPU Utilization .....	14
	Config .....	14
	Counters .....	14
	Crash .....	14
	File Transfer .....	15

ICMP .....	15
IP Communication.....	15
IP Phones.....	15
LLDP/PoE.....	15
Memory.....	15
Meshing.....	16
Redundant Management.....	16
Routing.....	16
Smart Link.....	16
Stacking.....	16
Switch Hang.....	16
TACACS.....	16
Web Management.....	16
Version WB.15.15.0008.....	16
802.1X .....	16
CLI .....	16
Config .....	17
Console .....	17
Logging .....	17
Management .....	17
PoE .....	17
sFlow .....	17
SNMP .....	17
Stacking .....	18
Switch Hang .....	18
Web Management .....	18
Version WB.15.15.0007.....	18
Authentication .....	18
IP Phones .....	18
IPv6 .....	18
Logging .....	18
sFlow .....	18
Version WB.15.15.0006 .....	19
BPDU Protection .....	19
CLI .....	19
Config .....	19
Console .....	19
Counters .....	19
Crash .....	19
Display Issue .....	20
Event Log .....	20
Fastboot .....	20
IGMP .....	20
IPv6 .....	20
LLDP .....	21
Logging .....	21
Meshing .....	21
Mirroring .....	21
MSTP .....	21
Multicast .....	21
OpenFlow .....	21
RADIUS .....	21
SNMP .....	21
Spanning Tree .....	21
Stacking .....	22

Switch Hang .....	22
TELNET .....	22
Web Management .....	22
Upgrade information.....	22
Upgrading restrictions and guidelines.....	22
Contacting HP.....	22
HP security policy.....	23
Related information.....	23
Documents.....	23
Websites.....	23
Documentation feedback.....	23

# 1 WB.15.15.0010 Release Notes

## Description

This release note covers software versions beginning with WB.15.15.0006.

Version WB.15.15.0006 was the initial release of Major version WB.15.15 software.

WB.15.15.0006 software was built from the same source as WB.15.14.0002. WB.15.15.0006 includes all enhancements and fixes in WB.15.14.0002 software, plus the additional enhancements and fixes in the WB.15.15.0006 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 the software update.

## Version history

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

Version number	Release date	Based on	Remarks
WB.15.15.0010	2015-02-06	WB.15.15.0009	Released, fully supported, and posted on the web.
WB.15.15.0009	2015-01-07	WB.15.15.0008	Released, fully supported, and posted on the web.
WB.15.15.0008	2014-09-15	WB.15.15.0007	Released, fully supported, and posted on the web.
WB.15.15.0007	2014-06-26	WB.15.15.0006	Released, fully supported, but not posted on the web.
WB.15.15.0006	2014-03-18	WB.15.14.0002	Initial release of WB.15.15. Released, fully supported, and posted on the web for early availability.
WB.15.14.0011	2015-02-06	WB.15.14.0010	Please see the WB.15.14.0011 release note for detailed information on the WB.15.14 branch. Released, fully supported, and posted on the web.
WB.15.14.0010	2015-01-07	WB.15.14.0009	Released, fully supported, and posted on the web.
WB.15.14.0009	2014-09-15	WB.15.14.0008	Released, fully supported, and posted on the web.
WB.15.14.0008	2014-07-16	WB.15.14.0007	Released, fully supported, but not posted on the web.
WB.15.14.0007	2014-07-01	WB.15.14.0006	Released, fully supported, and posted on the web.
WB.15.14.0006	2014-03-27	WB.15.14.0002	Released, fully supported, but not posted on the web.
WB.15.14.0005	n/a		Never built.
WB.15.14.0004	2014-01-07	WB.15.14.0002	Released, fully supported, but not posted on the web.

Version number	Release date	Based on	Remarks
WB.15.14.0003	n/a		Never built.
WB.15.14.0002	2013-10-18	WB.15.13.0003	Initial release of WB.15.14, fully supported, and posted on the web for early availability.
WB.15.13.0014	2014-11-17	WB.15.13.0013	Please see the WB.15.13.0014 release note for detailed information on the WB.15.13 branch.
WB.15.13.0013	2014-09-15	WB.15.13.0012	Released, fully supported, and posted on the web.
WB.15.13.0012	2014-07-31	WB.15.13.0011	Released, fully supported, but not posted on the web.
WB.15.13.0011	n/a	WB.15.13.0010	Never released.
WB.15.13.0010	n/a	WB.15.13.0009	Never released.
WB.15.13.0009	n/a	WB.15.13.0008	Never released.
WB.15.13.0008	2014-05-29	WB.15.13.0006	Released, fully supported, and posted on the web.
WB.15.13.0007	2014-03-31	WB.15.13.0006	Released, fully supported, but not posted on the web.
WB.15.13.0006	2014-03-21	WB.15.13.0005	Released, fully supported, but not posted on the web.
WB.15.13.0005	2013-12-20	WB.15.13.0004	Released, fully supported, and posted on the web.
WB.15.13.0004	2013-08-28	WB.15.13.0003	Released, fully supported, but not posted on the web.
WB.15.13.0003	2013-07-02	First release	Initial release of WB.15.13, fully supported, and posted on the web for early availability.

## 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

## Compatibility/interoperability

### Minimum supported software versions

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

## Enhancements

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

---

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

---

### Version WB.15.15.0010

#### Configurable TLS

**CR\_0000160085** Configurable TLS version and enforcing the use of a specific cipher suite.

The National Institute of Standard and Technology (NIST) has provided requirements for the use of TLS in Special Publication 800-52. These requirements state that a minimum version of TLS must be enforced, as well as the use of specific cipher suites. In order to meet these requirements, the software has been modified to support enforcing minimum versions of TLS and specify which cipher suites are to be used.

As a TLS client, the switch will advertise the configured preferences for the TLS version and cipher suite to the server. If the server does not support the cipher suite or negotiates a lower TLS version, the connection between client and server will be terminated. As an HTTPS server, the switch will check the TLS version and cipher suite advertised by the client. Should it detect a mismatch with the configured TS version or cipher suite for the application, the connection will be terminated.

The following new CLI command has been implemented in order to configure the minimum TS version and cipher suite:

```
[no] tls application { web-ssl | openflow | syslog | tr69 | all }
lowest-version { tls1.0 | tls 1.1 | tls 1.2 | default } cipher {
aes256-sha256 | aes256-sha | aes128-sha256 | aes128-sha | des3-cbc-sha
| ecdh-rsa-aes128-gcm-sha256 }
```

The MIB HP-ICF-TLS-MIN-MIB (OID string: 1.3.6.1.4.1.11.2.14.11.5.1.112) has been implemented to provide support for the feature via SNMP.

#### Rate Limiting

**CR\_0000158994** Two new features have been implemented:

**1.** Guaranteed Minimum Bandwidth (GMB) on trunk interfaces

Up to now, it was not possible to configure GMB on aggregated interfaces (trunks). This has now been changed.

GMB allows a user to assign bandwidth percentages to a port's queues. The port queues will be serviced in descending order, up to the configured bandwidth percentage. When the configured limit has been reached, the software will service the next highest priority queue. When the queue has been fully serviced, but the limit has not yet been reached, remaining bandwidth will be offered to the next queue to be serviced. Any leftover bandwidth within a servicing window is then made available to the top priority queue.

It is also possible to configure 'strict priority queuing', which means that the highest priority queue might consume as much bandwidth as necessary, even if that will starve lower priority queues.

Note that even though GMB can now also be applied to a trunk, the actual GMB bandwidth percentages are applied to the physical ports that are a member of the trunk.



Configuring GMB on dynamic LACP trunks, Distributed Trunking interfaces, and Mesh ports will not be supported. The enhancement applies only to statically configured trunk ports.

## 2. Queue-based Rate Limiting for Egress Traffic

Rate Limiting percentages can now also be configured on a per-port queue basis and will be applied to the traffic exiting the port.

The following new CLI command has been implemented to configure the feature:

```
[no] interface <port | trunk > rate-limit queues out percent [<queue %> <queue %> <queue %> <queue %> <queue %> <queue %> <queue %> ]
```

The following objects have been added to the HP-ICF-RATE-LIMIT-MIB in order to support the feature in SNMP:

```
hpEgressRateLimitPortQueueControlMode (.1.3.6.1.4.1.11.2.14.10.2.14.1.4.1.2.1.6)
hpEgressRateLimitPortQueueIndex (.1.3.6.1.4.1.11.2.14.10.2.14.1.4.1.5.1.1)
hpEgressRateLimitPortQueueMax (.1.3.6.1.4.1.11.2.14.10.2.14.1.4.1.5.1.2)
```

## Version WB15.15.0009

No enhancements were included in version WB.15.15.0009.

## Version WB.15.15.0008

No enhancements were included in version WB.15.15.0008.

## Version WB.15.15.0007

No enhancements were included in version WB.15.15.0007.

## Version WB.15.15.0006

### Audit Logging

**CR\_0000138477** Audit logging captures information including date, time, and outcome of an event, user identity, event start and stop timestamps, firmware versions, and begin and end of self tests, and includes that information in event log messages. For more information, see the *Management and Configuration Guide* for your switch.

### Broadcast Storm

**CR\_0000126535** Port Shutdown With Broadcast Storm. Adds the `fault-finder broadcast-storm` command, with the option to disable the port for a configurable interval when a broadcast storm is detected. See "Port Trunking" in the *Management and Configuration Guide* for your switch.

### Core Dump

**CR\_0000140258** All Task Core Dump. The core dump file now includes all tasks that are operating when the switch crashes.

### Debug Capability

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

### Inactivity Timer

**CR\_0000128427** Web User Interface Inactivity Timer. This new configuration command enables the administrator to set the idle timeout for the Web user interface, and provides a session timeout page to the user when the Web user interface session ends. See the *Management and Configuration Guide* for your switch.

## Interface Authentication

**CR\_0000142449** Disable Username Prompts For Management Interface Authentication. This option allows the user to provide only the Manager or Operator password when logging into the switch, without first being prompted for username. When set, this option applies only if the switch uses default usernames for both Manager and Operator logins. See "Secure Shell (SSH)" in the *Access Security Guide* for your switch.

## Password Length

**CR\_0000128426** Minimum Password Length. Adds a command to set the minimum password length for Manager, Operator, and Port-Access passwords. The minimum password length is enforced when passwords are added or updated. See the *Access Security Guide* for your switch.

## Reporting

**CR\_0000139639** Task Usage Reporting. The task usage reporting feature provides the ability to collect and display CPU usage data (with a refresh rate of 5 seconds) of running tasks on the switch. See "Task Usage Reporting" in the *Management and Configuration Guide* for your switch.

## Service Insertion

**CR\_0000145084** Service Insertion. This feature adds a programmatic interface (MIB) that allows SDN controllers to create a tunnel and direct traffic into the tunnel using OpenFlow rules. The tunneled packets can then be inspected and processed by external services, and might be returned to the switch via the tunnel for normal forwarding. See the *Service Insertion User's Guide*. (This enhancement was inadvertently omitted from the original WB.15.15.0006 list.)

## Syslog Messages

**CR\_0000141040** Hostname in Syslog Messages. The switch can be configured to include its hostname as the source or "origin" for messages sent to a syslog server. For more information, see "Troubleshooting" in the *Management and Configuration Guide* for your switch.

## TLS

**CR\_0000139306** Syslog Over TLS. This enhancement to the existing Syslog feature enables the use of the Transport Layer Security (TLS) protocol to deliver Syslog messages. See the *Management and Configuration Guide* for your switch.

## Fixes

This section lists released builds that include fixes. Software fixes are listed in reverse-chronological order, from newest to oldest. Unless otherwise noted, each software version listed includes all fixes added in previous versions listed below.

---

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

---

## Version WB.15.15.0010

### Accounting

**CR\_0000152920** When RADIUS or Syslog Accounting is configured, every time an Accounting Start or Stop message is sent to the Accounting Server, the switch generates an RMON event message that is logged in the Event Log and is sent as SNMP trap and Syslog message. The RMON messages are also logged for every Accounting user-level instead of only the service starting and stopping.

## Certificate Manager

**CR\_0000159204** When a self-signed certificate is generated in the CLI, the certificate does not contain a valid start and end-date. This causes the certificate to be invalid, which causes problems establishing HTTPS sessions or using syslog over TLS. When the self-signed certificate is generated in the web interface, this problem does not occur.

## CLI

**CR\_0000156237** When a user has enabled Spanning Tree in the CLI and configured a protocol version other than the default MSTP, the CLI Menu does not allow the user to modify Spanning Tree parameters. The menu indicates that the switch requires a reboot. When the switch is actually rebooted the same problem is present after the reboot.

**CR\_0000161668** After a user has changed the Spanning Tree Protocol Version to RPVST in the CLI Menu, the switch prompts the user to save the configuration and reboot the system to activate the changes. However, after saving and rebooting, those messages continue to be displayed.

## Config

**CR\_0000145221** When a user enables Meshing, the software prompts the user to save the configuration and reboot the system. However, after saving the configuration, issuing the command to reboot the system causes the software to print the following redundant message: Do you want to save current configuration [y/n/^C]?

## Crash

**CR\_0000149153** When an exceptionally large amount of IP Address Manager (IPAM) output is generated by the output of `show tech all` and captured using the `copy command-output CLI` command, the system might crash with the following message: NMI event  
SW:IP=0x00147168 MSR:0x02029200 LR:0x00120f7c cr: 0x44000400  
sp:0x04d60f30 xer:0x00000000 Task='mSess3' Task ID=0x4d59728.

**CR\_0000155066** The switch might reboot unexpectedly with a Software Exception message similar to: Software exception at `stackingFile.c:2224 -- in 'mStackDatWriter'`, task ID = `0x3c953b00 -> Internal Error ID: 6382d706`) when a lot of TFTP file transfers to an external TFTP server have occurred.

**CR\_0000156164** When a user disables or enables an OpenFlow instance and alters the switch's association with the OpenFlow controller, a switch might crash with a message similar to: Software exception at `hwBp.c:218 -- in 'fault_handler'`, task ID = `0x3f602380 -> MemWatch Trigger: Offending task 'mOFctrlTask'`

This problem can also occur when the switch is rebooted, in which case the crash message is: Software exception at `hwBp.c:218 -- in 'fault_handler'`, task ID = `0x3c402380 -> MemWatch Trigger: Offending task 'swInitTask'`.

The fix in this CR also addresses a problem with the values for `current_speed` and `max-speed` for 1 Gbps ports. The values can be incorrectly set to `'3567587328 kbps'`.

**CR\_0000159646** After enabling Control Plane Protection on a system that contains a module or stack member switch that has less than 24 ports, all modules in a chassis or all stack member switches crash repeatedly with the following message: Software exception at `aqTcamSlaveUtils.c:2056 -- in 'mAsicUpd'`, task ID = `0x1b1e6780 -> Policy Engine: Port instance not on this slot.`

**CR\_0000159764** Due to a semaphore deadlock with an unknown trigger, a switch might crash with a message similar to: NMI event HW:IP=0x0151dec4 MSR:0x02029200  
LR:0x0151e468 cr: 0x20000800 sp:0x02f01460 xer:0x20000000  
Task='tDevPollRx' Task ID=0xaa28000.

**CR\_0000162155** Configuring an OpenFlow instance using secure mode, enabling OpenFlow, and then configuring the lowest-version for OpenFlow might cause the switch to reboot unexpectedly.

Other triggers include updating the `tls lowest-version` for an app for which a cipher is already configured, and executing the `no tls app <app> lowest-version <ver> cipher` CLI command. The crash message references a `mem-watch` trigger.

**CR\_0000162400** When the switch continuously attempts to transfer a file to a destination that returns an error; for example, because it runs out of space to store the file, the switch might eventually crash with the message: `Software exception at hwBp.c:218 -- in 'fault_handler', task ID = 0x3c403380 -> MemWatch Trigger: Offending task 'mftTask'.`

## LLDP

**CR\_0000157298** When a PD sends an LLDP-MED TLV to a switch port in which the PD uses the invalid value of 0 Watts, the switch software actually applies the invalid 0 Watts. This causes the PD to reboot every time it transmits the 0 Watts in the TLV. The switch might log overcurrent warnings (`00562 ports: port <port ID> PD Overcurrent indication`) because the PD is already drawing power over the port when the software applies 0 Watts power. The value of 0 Watts in the TLV is henceforth rejected with the error `Invalid power value 0 deciWatts received from MED PD on port <port ID>.`

## Memory

**CR\_0000150414** After a Flare OpenFlow controller sends flow modification packets to a switch that contains invalid zero-length action headers, the switch becomes unresponsive and eventually crashes with the following message: `NMI event SW:IP=0x09f4e6ec MSR:0x02029200 LR:0x09f4efe4 cr: 0x88000800 sp:0x130ad738 xer:0x20000000 Task='eOFNetTask' Task ID=0x130add28.`

## OOBM

**CR\_0000160533** Packets of 1500 bytes or larger might be dropped when they are sent to a stack via a stack member's OOBM interface. This can result in various communication problems between an external host and the stack.

## Rate Limiting

**CR\_0000163326** The guaranteed minimum bandwidth (GMB) feature and new feature Egress queue rate-limit are concurrent features. According to the design, we should not be able to configure Queue rate-limit values less than the GMB for each queue. This behavior is by design, but a special case was added to the software to allow a 0% rate-limit queue value in order to disable the feature.

**CR\_0000163327** A warning message designed for trunks is seen even if the user misconfigures the Egress Queue Rate-limit feature.

**CR\_0000163336** A configured rate-limit of 100% per queue is shown in the running config for 4-queue and 2-queue scenarios, but not in an 8-queue configuration.

**CR\_0000163745** Redundancy switchover on a switch impacts the default Guaranteed Minimum Bandwidth (GMB) implementation in 2-queue and 4-queue configurations.

**CR\_0000163748** When a new Queue Rate-limit configuration is saved on the 5400R zl series switch, the new configuration does not take effect when a redundancy switchover occurs. It does take effect when the switch is booted.

**CR\_0000163828** Traffic flow on lower-priority queues does not match the rate-limit queues configuration.

**CR\_0000164829** There is inconsistent CLI output in response to the `show rate-limit queues <port>` and the `show rate-limit queues` CLI commands when rate-limit queues are configured on a port and then the port is added to a trunk interface.

**CR\_0000163861** When the rate-limit configuration is removed from a trunk port using the `no rate-limit queues out` CLI command, the change does not take effect until a system boot occurs. Edits to the rate-limit occur immediately.

**CR\_0000163864** Rate-limit queue configuration of 100% for Queue 1 and 0% for other queues does not work as intended.

**CR\_0000163995** The switch allows configuration of rate-limit queues that are less than Guaranteed Minimum Bandwidth (GMB) profile for the same queue in a strict queuing scenario. The switch should not allow the rate limit to be less than the minimum bandwidth setting for any queue.

## Redundant Management

**CR\_0000149253** When a switch stack or chassis with redundant management modules is rebooted, the system might not finish booting properly. The modules in the chassis or the stack member switches will appear to have completed the boot process, but all their ports remain down.

## Self Test

**CR\_0000161371** When the switch is booting, the Out-of-band-management (OOBM) port might fail to initialize during self-test, resulting in the following message: `Switch Chassis needs replacement at scheduled downtime`. This is a software error and not a genuine hardware failure.

## SNMP

**CR\_0000160352** The string value for the temperature sensor's instance of the object `entPhysicalName (.1.3.6.1.2.1.47.1.1.1.1.7)` is incorrectly set to **Chassis**. It should return **Chassis Temperature**.

## SSH

**CR\_0000153145** When a user copies a large file from the switch to a server using the SFTP client on the switch, the file transfer might be prematurely interrupted because the session disconnects before the file transfer has been completed. When this occurs, the following message is recorded in the system's Event Log: `03311 sftp: AM1: User: SFTP connection failure while connecting from <ip address>`.

## TFTP

**CR\_0000159058** When the switch is used as a TFTP server and configuration files are transferred from the switch to an external TFTP client, the software creates a temporary file in memory that is removed after the transfer has completed. However, the temporary file is not deleted when an error occurs during the file transfer. When repeated file transfers of configuration files fail, the temporary files accumulate and might deplete the available memory space. Once depleted, further file transfers fail and the switch might reboot unexpectedly (crash). Note that when the switch is rebooted, all temporary files are removed from memory.

## Web Management

**CR\_0000160654** When 51 or more VLANs are configured on the switch, the web interface does not display any VLAN under the **VLAN Management** and **Multicast IGMP** tabs.

## Version WB.15.15.0009

### APR

**CR\_0000152907** When a user changes the value of the ARP Cache Timer, the new value is applied to new ARP entries, but not to the ARP entries that already existed when the timer value was modified.

## 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.

## CPU Utilization

**CR\_0000153428** With high volumes of routed IPv6 traffic, switch CPU utilization might remain at high levels for long periods of time. This issue is most prevalent with v1 z1 modules.

**CR\_0000155359** Three-stack 3800 device CPU utilization went to 100% while configuring ARP protection for 4094 VLANs.

## Config

**CR\_0000152418** Routing must be enabled before the Local Proxy-ARP feature can be configured, but when routing is removed from the config, the Local Proxy-ARP configuration is not removed.

## Counters

**CR\_0000148671** The output of `show ip counters ipv6` gives incorrect values.

## 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`.

**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`.

**CR\_0000151340** Compressed core file is corrupted.

**CR\_0000152464** With a heavy volume of traffic through the Out of Band Management (OOBM) port, the switch might reboots unexpectedly with a message similar to `Software exception at alloc_free.c:790 -- in 'mOobmCtrl', task ID = 0x13b15d00 -> buf already freed by 0x13B15E80, op=0x00000000Buffer`.

**CR\_0000152930** After deleting the last of any configured Smart Link groups, the switch might reboot unexpectedly.

**CR\_0000153035** With MAC-based authentication and mixed-mode enabled on a port that has both authenticated and unauthenticated clients, a redundancy failover might cause the switch to reboot unexpectedly with a message similar to `Software exception at btthwSrcBasedVlan.c:263 -- in 'mAdMUpCtrl', task ID = 0x1fecc6c0 -> ASSERT: failed`.

**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`.

**CR\_0000154230** When copying a coredump from standby management module (SMM) or the stack's standby switch to a server via SCP, the switch might reboot unexpectedly with a message similar to `hwBp.c:218 -- in 'fault_handler', task ID = 0x3c402380 -> MemWatch Trigger: Offending task 'mRfsCtrl'. Offending IP=0xa9712f0`.

**CR\_0000154602** The switch experiences a loss of free memory for failed PEAP-MSCHAPv2 MAC-based authentication requests. When memory is no longer available, the switch will reboot

unexpectedly with a message similar to Software exception at wma\_peap.c:713 -- in 'mWebAuth', task ID = 0x1de85340 -> ASSERT: failed.

**CR\_0000155538** Disabling and re-enabling a port configured for Web or MAC-authentication during client authentication might cause the switch to reboot unexpectedly with a message similar to Health Monitor: Restr Mem Access HW Addr=0xb1ba0c1a IP=0x108682b8 Task='mWebAuth' Task ID=0x1de8c680 sp:0x12f98530 lr:0x10868664 msr: 0x0000b032 xer: 0x00000000 cr: 0x88000400.

**CR\_0000155604** When a CLI command is entered with a backslash as the last character and then the repeat command is issued, the switch might reboot unexpectedly with a message similar to Task mSess1 encountered an exception.

**CR\_0000155710** Sending an ICMPv6 echo request packet with multiple fragment headers to the switch causes an NMI crash.

**CR\_0000155750** When using MAC Authentication on the 2620, the following software exception might occur: wma\_client\_sm.c:1646 -- in 'mWebAuth', task ID = 0x1de85380.

**CR\_0000156908** A banner configured with more than 1048 characters causes the switch to go into a continuous "boot loop" when the switch is rebooted. The switch logs a message similar to Health Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x54202800 IP=0x54202800 Task='swInitTask' Task ID=0xaa1a840 sp:0x2e288a0 lr:0x54202800 msr: 0x02029200 xer: 0x20000000 cr: 0x44000400.

**CR\_0000159294** Software exception at arenal\_chassis\_slot\_sm.c:3374 -- in 'eChassMgr', task ID = 0x13b21a40.

## 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.

**CR\_0000153959** The core dump file cannot be transferred from the switch to an external device.

## ICMP

**CR\_0000155702** The switch sends a ping request to a random IP address every 20 minutes.

## IP Communication

**CR\_0000155717** Unresponsive OOBM interface after boot.

## IP Phones

**CR\_0000157298** If an IP phone sends the switch an invalid power value of zero watts in an LLDP-MED TLV, the switch log shows PD Over Current indication and the phone might continuously reboot. This has been observed with the Avaya 9641G IP phone.

## LLDP/PoE

**CR\_0000156145** 2920 Stack with non-PoE commander fails LLDP negotiation of power management for PoE.

## Memory

**CR\_0000152126** Issuing the terminal length or terminal width command causes a small loss of free memory.

## Meshing

**CR\_0000155857** When enabling meshing on the device and then configuring IGMP, we get error message: 08/12/14 10:56:52 02413 igmp: Internal api IgmppInterface\_getPortMode failed: bad port mode.

## Redundant Management

**CR\_0000155089** Issuing the `erase all` command on a switch configured for **redundancy management-module nonstop-switching** might cause the Standby Management Module (SMM) or the stack's standby switch to reboot continuously.

**CR\_0000156759** After redundancy switchover with boot command when modules have not finished booting, an internal buffer might become corrupted. This could possibly lead to a crash.

## Routing

**CR\_0000155524** After issuing the `clear arp` command, traffic that is destined for the default router is routed via software, which causes poor performance.

## Smart Link

**CR\_0000152346** Upstream switches do not flush the MAC and ARP entries after a Smart Link switchover.

**CR\_0000152422** After deleting the active Master port from a Smart Link group, the Slave port takes over but does not send flush packets.

**CR\_0000152432** When Spanning Tree is enabled after Smart Link is configured, the Smart Link ports incorrectly take part in Spanning Tree.

## 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\_0000154477** Attempting to apply a 32-character **local-mac profile** name to a 32-character **local-mac mac-group** name causes the switch to become unresponsive, requiring a reboot to recover.

## TACACS

**CR\_0000155541** TACACS authentication is not working with encrypted credentials in FIPS devices.

## Web Management

**CR\_0000148902** Web UI fails to load when using OOBM via Standby MM.

## Version WB.15.15.0008

### 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".

### 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.



**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".

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

**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.

**CR\_0000152440** The output of `show tech all` halts while displaying `lmaDbUtil traverseLmaProfTbl`, with the message `=== The command has completed with errors. ===`.

## Config

**CR\_0000149526** Enabling stacking on a switch that has a trunk configured creates an invalid entry for the trunk in the config file. The resulting configuration file cannot be downloaded to the switch.

## 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.

## 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.`

## 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.

**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.

## sFlow

**CR\_0000152330** sFlow samples of packets transmitted by the switch have an incorrect value (`0x3ffffff`) for the output port.

## SNMP

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

**CR\_0000151035** The switch incorrectly reports that `MIB object entPhysicalIsFRU = False` for removable fantrays, power supplies, and transceivers.

**CR\_0000152809** The switch accepts incorrect values in an SNMPv1 query, instead of generating an error message.

**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`.

## 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.

**CR\_0000154477** Attempting to apply a 32-character local-mac profile name to a 32-character local-mac mac-group name causes the switch to become unresponsive, requiring a reboot to recover.

## 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.

**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.

## Version WB.15.15.0007

### 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.

### 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.

**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.

### 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.

### sFlow

**CR\_0000147660** In an IPv6-only environment with Stateless Address Autoconfiguration, sFlow incorrectly uses the link-local address as the agent ID.

## Version WB.15.15.0006

### 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\_0000143576** The switch does not allow users to configure a port with the setting `speed-duplex auto-10-100`.

**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.

**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.

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

**CR\_0000143860** On a switch configured with rapid PVST and BPDU protection, the output of the command `show spanning-tree bpdu-protection` 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\_0000136407** Entering the command `show tech all` or `show log -a` might cause the switch to reboot unexpectedly with a message similar to `Software exception at multMgmtUtil.c:88 -- in 'mLoopPTx', task ID = 0x3c8efa00 -> Internal error`.

**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`.

**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 bttfLearn.c:2616 -- in 'mLpmgrCtrl', task ID = 0xa98a9c0 -> Mac Table Error`.

**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`.

**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`.

**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`.

## 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`.

## Event Log

**CR\_0000136882** Several different "chassis" events use the same event ID = 374. With this fix, a unique event ID is used for each type of "chassis" event.

## 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.

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

## IPv6

**CR\_0000140467** The switch does not generate an event log message when IPv6 Neighbor Discovery (ND) detects a duplicate address.

## LLDP

**CR\_0000140297** The `PortID` information is truncated at 25 characters, in the output of `show lldp info remote-device`.

## 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.

**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.

## Mirroring

**CR\_0000144479** After copying a config file from an external device to the switch and booting with that config, the output of `show monitor` does not display any of the configured Network Monitoring sessions.

## 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.

## OpenFlow

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

## 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.

## SNMP

**CR\_0000143599** The switch does not allow users to configure RMON alarms via SNMP. This issue was introduced with CR\_0000112411.

**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.

## 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.
```

## Stacking

**CR\_0000145211** The output of `show tech statistics` gives incorrect information for stack members.

## 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\_0000137933** When connecting to a switch via HTTPS across a slow link, after the user logs in the screen freezes and does not display the switch management page. This issue has been observed across a 512 kbps WAN link, using several different Web browsers.

## Upgrade information

### Upgrading restrictions and guidelines

WB.15.15.0010 uses BootROM WB.15.05. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

For more information about BootROM, see the *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 Manual Supplement for A.15.15, RA.15.15, WB.15.15, and YA/YB.15.15*
- *HP Switch Software Basic Operation Guide*
- *HP Switch Software Feature Index — Extended*

### 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/networking/software](http://www.hp.com/networking/software)
- 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.