WB.15.16.0008 Release Notes

Abstract

This document contains supplemental information for the WB.15.16.0008 release.

HP Part Number: 5998-8040
Published: May 2015
Edition: 1

Acknowledgments

Contents

1 WB.15.16.0008 Release Notes

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	Release date	Based on	Remarks
WB.15.16.0008	2015-04-17	WB.15.16.0007	Released, fully supported, and posted on the web.
WB.15.16.0007	n/a	WB.15.16.0006	Never released.
WB.15.16.0006	2015-02-06	WB.15.16.0005	Released, fully supported, and posted on the web.
WB.15.16.0005	2014-11-21	WB.15.16.0004	Released, fully supported, and posted on the web.
WB.15.16.0004	2014-10-30	WB.15.15.0006	Initial release of WB.15.16. Released, but never posted on the web.
WB.15.15.0012	2015-04-17	WB.15.15.0011	Please see the WB.15.15.0012 release note for detailed information on the WB.15.15 branch. Released, fully supported, and posted on the web.
WB.15.15.0011	n/a	WB.15.15.0010	Never released.
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.

Version number	Release date	Based on	Remarks
WB.15.14.0012	2015-04-17	WB.15.14.0011	Please see the WB.15.14.0012 release note for detailed information on the WB.15.14 branch. Released, fully supported, and posted on the web.
WB.15.14.0011	2015-02-06	WB.15.14.0010	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.
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.

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 precedes the enhancement description is used for tracking purposes.

Version WB.15.16.0008

No enhancements are included in version WB.15.16.0008.

Version WB.15.16.0007

Never released.

Version WB.15.16.0006

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 may 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 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.

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 precedes the fix description is used for tracking purposes.

Version WB.15.16.0008

802.1X

CR_0000164489 802.1X re-authentication period works if the client connects after the switch is booted. If, however, the switch reboots while clients are connected, it authenticates initially, but no re-authentication occurs.

Certificate Manager

CR_0000162594 When a TA certificate is present during boot up, the switch may hang/restart with the following error: `Software exception at certmgr_store.c:1921 -- in 'swInitTask`. Triggered when a corrupted certificate is present as TA certificate upon boot up. The system tries to double free and hangs.

CR_0000164093 When an IDEVID certificate is being used to establish TLS connections with a CNM server, the existing signature algorithm is updated from SHA-1 to DER, with new root certificate for the RA server.

CLI

CR_0000159808 When DHCPv6 Snooping is enabled and the switch has recorded a binding on a trunk, the output of the CLI command `show dhcpv6-snooping binding` displays the trunk ID as a + sign when the trunk ID exceeds four characters. For example, when a binding was learned on Trk11:

```
MAC Address IPv6-Address VLAN Port Time Left
------------ -------------- ---- ---- ---------
f0921c-2312c0 2001::82 1 + 5565
```

CR_0000163218 The output of the CLI command `show interface ethernet <interface>` becomes misaligned when the value of `Total Rx (bps)` reaches 100,000,000. When the 9th digit is added to the value of Total Rx, the adjacent line in the output (`Total Tx (bps)`) is shifted one column farther.

Command Authorization

CR_0000160066 The `listen-port help` command has changed:

Usage: `[no] listen-port <PORT-NUM>`

Description: Specify TCP the port on which the OpenFlow agent of the switch waits (listens) for incoming connections from a OpenFlow controller. The default port number is 6633.

The Description should be changed to read: Description: Specify the TCP port on which the OpenFlow agent of the switch listens for incoming connections from an OpenFlow controller. The default port number is 6633.

Crash

CR_0000170037 When a minimum TLS cipher suite version is enforced and a client negotiates a cipher suite, the switch may crash due to a watchdog timer expiry. The crash message may look similar to the following: `Software exception at bsp_interrupts.c:90 -- in 'fault_handler'`.

DHCP

CR_0000156469 Missing CLI command `ip dns dhcp` is now available.

Distributed Trunking

CR_0000165004 When Spanning Tree is enabled and the switch is rebooted, after the reboot the DT peer-keepalive port is set to a Spanning Tree 'blocking' state (alternate/discarding). This state prevents the transmission and reception of Distributed Trunking peer-keepalive packets. When the

peer-keepalive port is toggled, the port transitions to a correct Spanning Tree Designated/Forwarding state and the peer-keepalive packets is sent and received again.

OOBM

CR_0000157738 The `show oobm discovery` command sometimes indicates Active Stack Fragment(local only without Active Stack Fragment(discovered), even if show stacking indicates both commander and member correctly with normal stacking connection.

After a stack in chain topology is split, the least commander fragment and the equal split standby fragment stays active until it discovers the other fragment is active over OOBM. If there is no OOBM connected, there are multiple active fragments or active commanders on the network.

CR_0000168719 During a stack split condition, multiple fragments may become active even when all OOBM ports are connected, due to the device failing to receive an IP address via DHCP server.

OpenFlow

CR_0000162736 When adding a rule entry to OpenFlow, a `TABLE_FULL ECodeFlowModeFailed` error can occur, even when there is space for additional rules.

CR_0000163370 Violation of OpenFlow requirement that if the match field OXM_OF_IP_DSCP is used, the ETH TYPE must be 0x0800 or 0x86dd.

CR_0000164665 3500 OpenFlow does not forward NORMAL with HTTP when COPY and NORMAL are included in an Action Set Flow. HTTP GET requests might be lost once COPY and NORMAL are set in an Action Set Flow. HTTP GET requests are blocked once COPY and NORMAL are set in an Action Set Flow. 3500/6200

PoE

CR_0000146605 All the ports on a module fail to deliver power when a single controller fails.

Port Connectivity

CR_0000161856 If `ip igmp static-group <group-address>` is added to the switch configuration for any VLAN, then upon a warm or cold reboot of the switch, the switch does not establish a link on any Ethernet ports. This issue is also present on stand-alone 2920, with stacking disabled.

QoS

CR_0000162179 When attempting to remove a configuration line from a QoS policy, the switch returns `commit failed`. The customer cannot delete the line and has to reload the configuration to recover. Occurs when multiple policies are configured.

SSH

CR_0000159714 The output of the `display device` command over SSH displays incorrectly as a misaligned single line of output, due to no carriage returns between multiple lines. This occurs more frequently if the terminal width is set > 80 characters, when SSH senses the terminal settings on Login.

CR_0000165393 When the SSH client has a keepalive mechanism configured that requires a response from the SSH server on the switch, the SSH client terminates the session after the first keepalive packet is transmitted. This happens because the switch drops the client's keepalive packet due to an incorrect packet length calculation. This issue has been observed using an openSSH client with the ServerAliveInterval configured and the parameter 'want_reply' enabled.

Stacking

CR_0000167758 The active fragment reboots when the inactive member is merged in five-member stacking.

Version WB.15.16.0007

Never released.

Version WB.15.16.0006

Authentication

CR_0000156072 When generating a self-signed certificate or Certificate Sign Request (CSR) in the web interface, the software incorrectly allows the use of non-ASN1 characters. When the CLI is used, the action is not allowed and an error message is displayed.

Certificate Manager

CR_0000159204 When a self-signed certificate is generated on 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 on 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 issue the following redundant message: `Do you want to save current configuration [y/n/^C]?`

CPU Utilization

CR_0000158909 When the CLI command `show system chassislocate member <ID>` is issued on a stack of switches, the CPU utilization rises to 100%.

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 may 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_0000152463 When the syslog feature **logging notify running-config-change** is enabled, inserting a new module into the chassis or reloading a module can cause the system to run out of message buffers. Once the message buffer pool is depleted, the system crashes with the typical `no msg buffer or no resources available` crash messages. For example:

```
Software exception at alloc_free.c:533 -- in 'mChassCtrl', task ID = 0xa99f140
-> No msg buffer
Software exception in ISR at btmDmaApi.c:436
-> ASSERT: No resources available!
```

CR_0000155066 The switch may 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_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, a switch might crash with a message similar to the following: `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 may 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 ran out of space to store the file), the switch might eventually crash with the following 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 will henceforth be 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 sent flow modification packets to a switch that contained invalid zero-length action headers, the switch became unresponsive and eventually crashed with the following message:

```
NMI event SW:IP=0x09f4e6ec MSR:0x02029200 LR:0x09f4efe4
cr: 0x88000800 sp:0x130ad738 xer:0x20000000
Task='eOFNetTask' Task ID=0x130add28
```

CR_0000152126 Every time a user issues the command `terminal width` or `terminal length`, 40 bytes are allocated in memory that are never freed.

CR_0000153262 SNMP Informs that are not acknowledged by the inform receiver are not properly removed. Over time, the amount of SNMP Inform messages stored in memory increases to the extent that insufficient contiguous memory is available to other processes, which causes the system to crash.

OOBM

CR_0000160533 Packets of 1500 bytes or larger may 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.

Port Access

CR_0000158890 After disabling and re-enabling a port, the port may end up in a state where it has established link, but does not pass any traffic. This issue can occur only on systems that do not have MSTP enabled.

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_0000163829 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.

Routing

CR_0000155524 Data traffic that is forwarded by the default route is routed in software after the ARP cache has been cleared by the command `clear arp`. Software routing can cause an increased latency and CPU utilization level.

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`. Note that this is a software error and not a genuine hardware failure.

SNMP

CR_0000156209 When a configuration file is downloaded to the switch in which the SNMP community name string for unrestricted access is something other than `unrestricted`, the software resets the access-level to the default `restricted`. Although it is expected behavior to default to `restricted` when the string `unrestricted` is not precisely matched, the software has been

modified to allow the use of both lower and uppercase characters in the word `unrestricted` when parsing a downloaded configuration file.

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`.

TFTP

CR_0000159058 When the switch is used as 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 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.15.16.0005

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.

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 `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.

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.

CR_0000151412 The output of a query for meter statistics gives an incorrect value for OpenFlow meter duration.

CR_0000151415 The output of a query for port statistics gives an incorrect value for OpenFlow statistics duration.

CPU utilization

CR_0000151164 The switch occassionally 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.`

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_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_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.`

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='mSnmpCtrl' 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.

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.

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.

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.

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.

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.`

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.

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.

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_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`.

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.

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

WB.15.16.0008 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

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.
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

Related information

Documents

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

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
- HP Networking: www.hp.com/go/networking
- HP product manuals: www.hp.com/support/manuals
- HP download drivers and software: www.hp.com/networking/software
- HP software depot: www.software.hp.com
- HP education services: 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**). Include the document title and part number, version number, or the URL when submitting your feedback.