KB.15.16.0010 Release Notes

Abstract

This document contains supplemental information for the KB.15.16.0010 release.

HP Part Number: 5998-8543
Published: August 2015
Edition: 1

Acknowledgments

Contents

1 KB.15.16.0010 Release Notes

Description

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

Version KB.15.16.0004 was the initial release of Major version KB.15.16 software. KB.15.16.0004 includes all enhancements and fixes in the KB.15.15.0006 software, plus the additional enhancements and fixes in the KB.15.16.0004 enhancements and fixes sections of this release note.

Product series supported by this software:

- HP 5400R 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
KB.15.16.0010	2015-08-29	KB.15.16.0009	Released, fully supported, and posted on the web.
KB.15.16.0009	2015-06-16	KB.15.16.0008	Released, fully supported, and posted on the web.
KB.15.16.0008	2015-04-17	KB.15.16.0007	Released, fully supported, and posted on the web.
KB.15.16.0007	n/a	KB.15.16.0006	Never released.
KB.15.16.0006	2015-02-06	KB.15.16.0005	Released, fully supported, and posted on the web.
KB.15.16.0005	2014-11-21	KB.15.16.0004	Released, fully supported, and posted on the web.
KB.15.16.0004	2014-10-30	KB.15.15.0006	Initial release of KB.15.16. Released, but never posted on the web.
KB.15.15.0014	2015-08-29	KB.15.15.0013	Please see the KB.15.15.0014 release note for detailed information on the KB.15.15 branch. Released, fully supported, and posted on the web.
KB.15.15.0013	2015-06-16	KB.15.15.0012	Released, fully supported, and posted on the web.
KB.15.15.0012	2015-04-17	KB.15.15.0011	Released, fully supported, and posted on the web.
KB.15.15.0011	n/a	KB.15.15.0010	Never released.
KB.15.15.0010	2015-02-06	KB.15.15.0009	Released, fully supported, and posted on the web.
KB.15.15.0009	2015-01-07	KB.15.15.0008	Released, fully supported, and posted on the web.

Version number	Release date	Based on	Remarks
KB.15.15.0008	2014-09-15	KB.15.15.0007	Released, fully supported, and posted on the web
KB.15.15.0007	2014-06-26	KB.15.15.0006	Released, fully supported, and posted on the web
KB.15.15.0006	2014-03-19	First release	Initial release of KB.15.15. Released, fully supported, but not posted to the web

Products supported

This release applies to the following product models:

Product number	Description
J9821A	HP 5406R zl2 Switch
J9824A	HP 5406R-44G-PoE+/4SFP (No PSU) v2 zl2 Switch
J9823A	HP 5406R-44G-PoE+/2SFP+ (No PSU) v2 zl2 Switch
J9868A	HP 5406R-8XGT/8SFP+ (No PSU) v2 zl2 Switch
J9822A	HP 5412R zl2 Switch
J9826A	HP 5412R-92G-PoE+/4SFP (No PSU) v2 zl2 Switch
J9825A	HP 5412R-92G-PoE+/2SFP+ (No PSU) v2 zl2 Switch

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 KB.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 preceding the enhancement description is used for tracking purposes.

Version KB.15.16.00010

CLI

CR_0000171261 New CLI is introduced to enable resetting the PoE controller and restore functionality on the affected port(s): `power-over-ethernet poe-reset port <port name>`

QoS

CR_0000172606 The Web UI can now display a port range when setting QoS, instead of displaying only the first port in the range.

Version KB.15.16.0009

Memory

Enhancements were made to optimize memory usage.

Version KB.15.16.0008

No enhancements are included in version KB.15.16.0008.

Version KB.15.16.0007

Version KB.15.16.0007 was never released.

Version KB.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.

Version KB.15.16.0005

No enhancements are included in version KB.15.16.0005.

Version KB.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

CR_0000124429 CPU protection during BPDU flooding. 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 DIPLDv6. 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.

OSPFv3

CR_0000154691 OSPFv3 trap enable/disable. The switch can be configured via CLI or SNMP to enable or disable sending of OSFPv3 traps. For more information, see the *IPv6 Configuration 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 KB.15.16.0010

Crash

CR_0000170286 Inserting or removing a module results in reloading the configuration, which can lead to a switch crash with a message similar to `Software exception in ISR at btmDmaApi.c:440`.

CR_0000171328 When entering Fail Standalone Mode in a dual SDN controller configuration (for example, the active controller disconnected) and all the controllers are disabled, the switch might crash with a message similar to `Software exception at ovsUtil.c:4761 -- in 'mOFCtrlTask'`.

CR_0000174081 In some cases, a switch module may fail when a corrupted packet is detected. Messaging may be similar to `Software exception in ISR at interrupts_ahs.c:3790 -> RULES FB 8100f9f9`.

Display Issue

CR_0000161014 Traffic counters that exceed the 32-bit value result in negative values in the output of CLI command `display interface PORT-NUM`.

IPv6

CR_0000172573 Configuring a port for IPv6 ra-guard and adding the port to a new or existing trunk results in the generic error message `Operation failed on Port X##: General error`.

OpenFlow

CR_0000172370 When a controller sends a `flow-stats` request, the switch sends a `flow stats` reply, the last header of this reply should have the flag value for `OFPMPF_REPLY_MORE` of `0`, not `1`.

CR_0000174751 If an OpenFlow rule containing an invalid VLAN (for example, a VLAN that has been deleted) is processed, it can result in the switch or module rebooting unexpectedly (crashing).

OpenFlow Crash

CR_0000163321 When an invalid meter ID is configured for an aggregate OpenFlow instance in the switch, an unexpected reboot might occur, logging a message similar to the following: `Software exception at inlines.h:83 -- in 'mSnmpCtrl', task ID = 0x13b11840`.

CR_0000163347 The switch might reboot unexpectedly (crash) while disabling and enabling a link that connects multiple Openflow controllers.

CR_0000169768 The switch might reboot unexpectedly (crash) while enabling OpenFlow, due to a problem computing the TCAM resources that would allow OpenFlow lookups. Crash messaging is similar to the following: `Software exception at hwBp.c:218 -- in 'fault_handler', task ID = 0x3f602380`.

CR_0000172055 Enabling aggregate OpenFlow instance when the controller-interface is configured to OOBM may lead to a switch crash with a message similar to `Software exception at aqTcamInterface.c:1865 -- in 'eOFNetTask'`.

CR_0000172595 Adding an unsupported chained group to the switch using VAN SDN controller might lead to a switch crash with a message similar to `Software exception at hwBp.c:218 -- in 'fault_handler'`.

CR_0000173380 When Network Optimizer is programming QOS Rules followed by an equal or higher priority rule, the switch mightcrash with a message similar to `Software exception at arenal_chassis_slot_sm.c:3597`.

OSPF

CR_0000162013 When using CLI command `show ipv6 route` during OSPF states transition with OSPFv3 virtual link configuration, a switch crash might be encountered with a message similar to `Software exception at hwBp.c:218 -- in 'fault_handler'`.

Packet Buffers

CR_0000170693 Packet buffer depletion in the switch might eventually trigger a PIM-related switch reboot (crash) similar to the following: `Software exception at PimApp.h:608 -- in 'mPim', task ID = 0xa953500 -> ASSERT0: failed`.

PIM-SM

CR_0000170522 Adding a lower-numbered IPv4 subnet to an existing C-BSR VLAN makes that IP address the primary. This can cause PIM to enter an incorrect state with multicast traffic loss and generate an error message (for example, `The Candidate-BSR is already using IP address of VLAN 0`) when C-BSR configuration changes are attempted.

PoE

CR_0000169265 After an electrical surge or ESD charge on a PoE port, the switch might exhibit BAD FET messages, which indicate a failure to deliver PoE on those ports. Event log messages appear similar to the following: `W 04/02/15 07:58:49 02562 ports: Port 1/1: Possible bad FET/PSE supplying PoE`

`power - suggest configuring other end of link with "no power"`

`W 04/02/15 07:58:49 00567 ports: port 1/1 PD Other Fault indication`.

Routing

CR_0000174012 Applying BPG route-map with set weight while there is more than one path could result in switch crash with a message similar to `Software exception at bgp_med.c:597 -- in 'eRouteCtrl'`. **Workaround:** The failure may be avoided by applying BPG route-map with set local-pref instead of using set weight.

VLAN

CR_0000172434 VLAN table is not displayed in Web UI when the switch is configured with 51 or more VLANs and 60 or more active ports.

Web GUI

CR_0000172729 When a VLAN is created with a name containing an apostrophe, the Web GUI troubleshooting pages appear to be blank.

Version KB.15.16.0009

BPDU Protection

CR_0000153533 If the switch receives BDPU config information with missing 'Forwarding' or 'Version' details, it incorrectly treats the message as a valid BDPU, resulting in spanning tree instability.

CLI

CR_0000157943 When the CLI command `copy command-output 'show tech all'` is executed, it is possible for the switch to run out of free memory and trigger an unexpected reboot (crash) when memory allocation fails. Conditions that increase the risk of this problem are the production of a file larger than 70 MB, or execution of the command when other switch tasks have consumed a large portion of free memory. Note that the first task or process to fail to allocate memory will be the one that is displayed in the crash message, so the event log and crash messaging may vary. One example message is as follows: `Software exception at svc_misc.c:858 -- in 'mCnfTrMgr', task ID = 0xa9f7c40 -> Failed to malloc 3032 bytes.` When insufficient resources are available to copy the requested output to a file, the process is terminated automatically. When this happens, the following message is displayed to the CLI and logged: `The command was terminated prematurely because the output exceeded the maximum memory limit.`

CR_0000159271 In some configuration contexts (for example, ip-access list, vlan), the IPv4 CLI commands (such as IP source-lockdown) are actually configuring the feature for IPv6.

CR_0000161010 When the `display` command is executed with pim-dense mode enabled, the command output/configuration is not displayed correctly.

CR_0000172046 The commands `show lldp info local-device` and `show lldp info remote-device` sometimes fail to display the correct information when the switch is not connected to any remote device.

Config

CR_0000170324 When a change is made from the CLI in the **Switch Configuration – Port/Trunk Settings** menu, the change is not saved, resulting in an `Unable to save field` error.

Crash

CR_0000164064 When a free radius authenticated user attempts to HTTPS to the switch web management GUI of the 2530-24G, the switch crashes with `Health Monitor: Read Error Restr Mem Access Task='tHttpd'.`

CR_0000165111 When OSPFv3 is enabled with traps, the SWS TA stack crashes the commander with a message similar to `Software exception at hwBp.c:218 -- in 'fault_handler', task ID = 0x3c402380.`

CR_0000166340 An SNMP crash occurs during PCM discovery on 2620 and 2650, if an Avaya phone is connected to the switch that advertises an organizational OUI value 00-00-00 (all zeros), or any neighbor entry contains an all zero OUI type TLV, during `walkmib` on the switch. Workaround: Change the **lldp admin** status to **`txOnly`** on the link that is connected to the specific Avaya phone.

CR_0000168119 Switch may crash in an unknown state over a very long period when a rare set of Web operations occur.

CR_0000168194 The switch might restart with an error message similar to the following during a session logout, kill, or timeout: `Software exception crash at multMgmtUtil.c:151 -- in 'mOobmCtrl', task ID = 0x13b15e00-> Internal error.`

DHCP Snooping

CR_0000160884 When DHCP-snooping is enabled, if any ports are configured as untrusted, DHCP packets are sent to those ports.

Display Issue

CR_0000167906 When the alert log is sorted by date/time, items are sorted (erroneously) alphabetically by day of the week, rather than day of the month.

Distributed Trunking

CR_0000168368 When the Distributed Trunk link is lost between the DTS primary switch and a distributed trunk device (DTD), the communication between the DTS primary and a distributed trunk device (DTD) or any hosts of DTD are also lost. This issue also causes loss of communication between DTD local hosts and any destinations whose path is the DTS-primary. Communication issues remain until the DT link is back online, AND, the other DT-link is disabled/re-enabled.

Event Log

CR_0000171023 During incorrect login attempts, a message is only logged to the event log after 3 attempts. A change has been made to log incorrect username/password attempt after *each* occurrence.

IPv6

CR_0000167682 The security feature "IP Source Lockdown" is not operating correctly and disrupts IPv6 traffic. This same feature can't be consistently and reliably disabled as expected. This CR includes two issues:

1. IPv4 ip source-lockdown on a port blocks IPv6 traffic in VLANs that do not have IPv4 DSNOOP enabled.
2. When removing the configuration by disabling 'no ip source-lockdown' globally and then removing the feature from the ports 'no ip source-lockdown 11.13', the feature does not seem to be removed correctly and keeps blocking IPv6 traffic.

This issue occurs when both DIPLD and DIPLDv6 are enabled.

Link

CR_0000169819 When the switch is configured for Rapid-PVST (RPVST), any changes to port path cost takes effect properly. However, when the port is disabled and then re-enabled, the port path cost applied and also advertised to neighbors changes to the default path cost.

Logging

CR_0000155070 The Alert-Log filter criteria does not work as expected when a substring is used as a filter.

CR_0000171737 After logging in to the switch using Operator credentials, and the enable command is then executed with incorrect Manager credentials, the event log erroneously shows the session belonged to Manager username.

CR_0000172072 Event log `show log -r` does not show an invalid key attempt during an SSH Public Key Login Failure.

OpenFlow

CR_0000170688 When enabling HP NetworkProtector on the VAN SDN Controller, the switch loses packet buffers until they are depleted and eventually the switch stops functioning and loses management access.

OSPF

CR_0000161636 When OSPF v3 is used, incorrect route calculations on the ABR by the switch result in symptoms such as multiple routes in RIB, and incorrect route selections based on preference settings (in the case of cost and distance, the lower value is preferred). Rebooting the ASBR may temporarily resolve the issue.

PIM

CR_0000169557 Under certain conditions, an IGMP stream freezes for all in the group. Two examples known to cause this are:

1. When a client directly attached to Core 1 sends a LEAVE for a Group that it is streaming, all other clients watching that Group freeze, until either a GQ is sent out for that Group, or another client sends a new Join for that group, after which all other clients resume streaming that group again.
2. When there are clients directly attached to Core 2, the LAST leave causes clients directly connected to Core 1 to freeze.

PoE

CR_0000155592 A PoE fault occurs after removing power supplies. The switch drops power across the board for about 30 seconds. This version contains a firmware fix to resolve this issue.

Power

CR_0000150101 The value for the Total Power displayed using the show system power-supply may be incorrect if one PSU in a multiple PSU system has its AC cord removed.

Routing

CR_0000160131 When more than 10,000 RIP routes are distributed by a neighbor, this RIP peer does not learn all of the routes – learning "stops" after about 10,000 neighbor RIP routes are installed.

Security Vulnerability

CR_0000162428 If the CLI command `verify signature flash [primary]` or `[secondary]` is issued more than once, it shows inconsistent results though the signature has already been verified.

CR_0000166717 Login is permitted with the default username Manager, even when the Manager username has been changed to a custom username.

sFlow

CR_0000168606 Switch 5400R continues to send incorrect sFlow datagrams for non-existent ports after removing the module associated with these ports.

SFTP

CR_0000162987 Management modules go out of synchronization and fail to recover when large SFTP copies or a large number of SFTP copies are performed.

SNMP

CR_0000158713 When reading the MIB data for a PSU Product ID J number, the number displayed is truncated by one character.

SSH

CR_0000171834 When logging in using Operator credentials for SSH and then executing the enable command with Manager credentials, the user name in the event log does not show the Manager username; it shows Operator mode.

Stacking

CR_0000170433 In a stacked configuration, if the MAC Authentication password is set to a password of exactly 16 characters (max length) and configuration is saved, when the stack reboots, the member switch hangs during reboot.

Switch Hang

CR_0000167470 A software exception occurs similar to: `Software exception at _chassis_slot_sm.c:3810 -- in 'eChassMgr', task ID = 0x3c93f100^J-> Member halting - non-conduit slave (Ports 1/1-24,49-50) lost comm (4).^J Debug slave and master.^J"`. This occurs during an arp-age timeout when heartbeat packets are failing to the master. It can occur when a high priority packet is sent to router's mac address.

Transceivers

CR_0000163290 Some SR J9150A and LRM J9152A transceivers show as NON-HP with K.15.07 and W.15.07 software.

Version KB.15.16.0008

10-GbE

CR_0000153118 When a 10G port is reset or when the port speed switches from 10 Gbps to 1 Gbps, or vice versa, the port might start dropping packets, flood packets, or packets received on the port might be corrupted. The latter condition might eventually cause the module or stack member to crash with a message similar to the following: `Software exception in ISR at interrupts_ahs.c:4087 -> Too many HPP ints: 00040000`. This problem affects only 10G Ethernet ports on 3800 series switches and ports 1, 2, 4, 7, and 8 on the J9546A and J9546A version 2 modules.

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
```

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 might crash due to a watchdog timer expiry. The crash message may be similar to the following: `Software exception at bsp_interrupts.c:90 -- in 'fault_handler'.`

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.

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

OSPF

CR_0000160228 During display of the output from two CLI commands, `display ospf routing` or `display ospf lsdb`, when a lot of routes are configured, if you use CTRL + C to interrupt the output, the console can hang for up to three minutes.

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.

Routing

CR_0000164381 When multiple ECMP routes are used with BGP, MSTP and VRRP, issues resulted due to message queues becoming full.

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.

Switch Hang

CR_0000166649 A PIM router might hang when RPF Override is enabled or disabled and another PIM-related CLI command is entered that changes the PIM protocol configuration. This is caused by the 'rpf-override' code locking the PIM code, but not releasing it when it has finished.

Switch Initialization

CR_0000162540 Switch hangs when downgraded to a previous version when mac classes and policy are configured.

This is a release note for both KB.15.16 and KB.15.15. (cycle 4).

Version KB.15.16.0007

Version KB.15.16.0007 was never released.

Version KB.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_0000154706 When a user configures a blackhole route for an IPv4 or IPv6 address and then attempts to configure that same IP address as a VRRP virtual IP address, the invalid configuration is rejected with the error message `Cannot configure a reject/blackhole route as backup virtual-ip-address`. When the configuration order is reversed by first configuring the IP address as VRRP virtual IP address and then the blackhole route, the configuration is incorrectly permitted by the configuration parser.

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_0000159125 When a system has Distributed Trunking enabled, a crash might occur when a packet with an incorrect flag is received on the ISC port. Instead of dropping the packet, the software attempts to process the packet, which triggers a crash similar to the following: `Health Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x0065d2f8 IP=0x65d2f8 Task='tDevPollTx' Task ID=0xa9f9700 sp:0x2ecc828 lr:0x6081c0 msr: 0x02029200 xer: 0x20000000 cr: 0x48000800.`

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_0000159784 The device might hang when configuring an IPv6 static route and configuring the forwarding address as a virtual-IP-address.

CR_0000162148 When an OSPFv3 NSSA area is changed to a stub area, the switch might reboot unexpectedly with a message similar to the following: `ospf3_ls.c:3748 -- in 'eRouteCtrl', task ID = 0xa9e7080-> Routing Stack: Assert Failed.`

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'.`

Distributed Trunking

CR_0000157975 When VRRP is enabled on a DT switch that is in VRRP Master State for one or more VLANs, deleting the VLANs by issuing the command `no vlan <vlan ID>` does not clear a VRRP data structure correctly. This causes the DT switch to assume it is still the owner of the VRRP virtual MAC addresses and ignore any learn updates it receives from its DT peer switches for those MAC addresses. This, in turn, can cause the VRRP virtual MAC addresses to get stuck on the system's ISC port.

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.

OSPF

CR_0000155425 When a high volume of Link State Acknowledgements are flooded to an OSPFv2 neighbor the adjacency might go down because OSPF Hello packets are dropped.

CR_0000160538 When a redundancy failover is executed on an OSPFv2 router that has Graceful Restart enabled, one or more neighbors might crash with the following message: `Software exception at ospf2_ls.c:1839 -- in 'eRouteCtrl', task ID = 0xa91ff00 -> Routing Stack: Assert Failed.`

CR_0000160814 When a user reconfigures an OSPFv3 area from stub or normal to NSSA without rebooting the router or restarting the OSPFv3 protocol, the ASBR status is not updated on the OSPFv3 router when it becomes an NSSA ABR. Likewise, when the area is reconfigured from NSSA to stub or normal, the ASBR status is also not updated and the router continues to act as if it is still an ASBR. Due to the incorrect ASBR status, the route advertisements are not correct, which results in routes being installed on routers in an area when they should not be or routes not being advertised when they should be.

CR_0000161927 When the redistribution of static or connected routes on an NSSA OSPFv3 router is disabled, the ASBR flag is not correctly reset. This can cause the router to function as an ASBR router when it should not.

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.

QoS

CR_0000159713 The Queue Monitor feature was inadvertently not enabled on the 5400R switches. The Queue Monitor allows the user to monitor the different ports queues and display the amount of dropped packets in each queue. The following CLI command enables the feature: `[no] qos watch-queue <port>`. The command `show qos watch-queue [port]` displays the number of dropped packets per port queue.

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.

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 KB.15.16.0005

Loop Protection

CR_0000160268 When there is a downstream network loop, the switch can learn its own port MAC address and add it to the MAC table. Normally the switch does not learn its own port MAC addresses, so this is incorrect behavior. However, this does not impact the Loop Protection feature as originally thought. Loop Protection works properly even with this incorrect MAC learning issue.

Version KB.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_0000136134 After issuing the command `no ip ssh cipher cipher_option`, the entry is listed twice in the output of `show run`.

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_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_0000152757 After configuring `snmp-server host` on the Commander, stack member configuration files include two lines with SNMPv3 configuration.

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.

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_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_0000153700 Three commands are removed from the `show tech all` and `show tech route` commands (which invoke many sub-commands): `show ipv6 ospf3 link-state link-scope detail`, `show ipv6 ospf3 link-state area-scope detail`, and `show ipv6 ospf3 link-state as-scope detail`. In certain situations, issuing those commands will cause the switch to reboot unexpectedly with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x017cb590 IP=0x17cb590`

```
Task='eRouteCtrl' Task ID=0xa96de00 sp:0x48cea20 lr:0x10086d4 msr:
0x02029200 xer: 0x20000000 cr: 0x44000400.
```

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.`

Distributed Trunking

CR_0000148165 When VRRP routers have distributed trunking enabled, VRRP failovers might cause the VRRP virtual MAC addresses (and therefore remote subnets) to become unreachable.

CR_0000148170 A MAC address that is learned by a distributed trunking switch and then moved to another port might be listed on the wrong port by the peer distributed trunking switch, causing that MAC address to be unreachable from the peer switch.

CR_0000149160 After removing the Inter-Switch Connection (ISC) and reconfiguring it, some traffic might be dropped or switched to the wrong port.

CR_0000151202 After receiving a join on an Inter-Switch Connection (ISC) port, the switch does not forward joins from other ports onto the ISC.

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.

IGMP

CR_0000128678 In certain topologies the IGMPv2 "Leave Group" from one host can cause the multicast stream to be dropped, even though there are other hosts receiving that stream.

IP phones

CR_0000137652 An IP phone that uses the "Automatic Port Synchronization" feature loses its IP address and possibly drops the current call. This has been observed when the switch is configured with the command `cdp mode pre-standard-voice`, and the PC to which the phone is connected goes into hibernation. In that situation the "Automatic Port Synchronization" feature causes the phone to drop and then re-establish link with the switch.

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_0000147833 Some RMON events are not correctly defined for VRRP, which causes the switch to report an error such as `system: Unknown Event ID 776` when those events occur.

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 config and rebooting the switch, the OOBM interface does not come up even after it is re-enabled.

OSPF

CR_0000147711 Link State Advertisements (LSAs) are retransmitted by the router before the retransmit timer expires. This improves the original OSPF fix (CR_0000134463).

CR_0000149413 The SPF counter for OSPFv3 increments for link-state updates even if there is no topology change.

CR_0000155308 When a large number of routes (on the order of 9000) are updated with a better path, the better paths are not always put into the routing table, which can cause unreachable subnets.

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_0000155619 Some Unify IP phones exhibit a PoE incompatibility with some HP switches, which might result in a hard failure of the phone. For more information see the customer advisory at http://h20564.www2.hp.com/portal/site/hpsc/public/kb/docDisplay/?docId=c04438506.

Policy based routing

CR_0000147703 In some situations, the switch does not allow a `service-policy` to be removed from a VLAN, responding with the error commit failed. Workaround: Reboot the switch, then issue the `no service-policy` command.

Rate limiting

CR_0000147093 If rate limiting is applied on the port that connects adjacent OSPF routers, the adjacency is lost after a switch reboot. This issue affects v2 zl modules and 3800 switches.

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_0000146616 OSPFv3 traps are not sent by the switch.

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_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_0000153460 Issuing the `boot system` command while VRRP traffic is being received by the switch might cause the switch to hang and not boot completely.

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.

Switch initialization

CR_0000149065 When the switch is rebooted, one module takes about 10 seconds longer to come online than the other modules.

Transceivers

CR_0000146528 After rebooting the switch, the configuration parameter `speed-duplex auto-100` (for a J8177C gigabit-copper transceiver slot) is removed from the config file.

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.

Issues and workarounds

CLI

CR_0000174064 There is a discrepancy between the Management and Configuration Guides and implemented CLI. Management and Configuration Guides: `lldp config PORT-LIST dot3TlvEnable poeplus_config` CLI command implementation: `lldp config PORT-LIST dot3TlvEnable poe_config`.
Workaround: Use the `lldp config PORT-LIST dot3TlvEnable poe_config` command syntax.

Switch Initialization

CR_0000169998 A port becomes an untagged member in more than one VLAN when the changes to the port's tagged/untagged VLAN membership are made in the CLI Menu.
Workaround: Reset the switch, reset the module, or power cycle the switch.

Upgrade information

Upgrading restrictions and guidelines

KB.15.16.0010 uses BootROM KB.15.01.0001. 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 K/KA/KB.15.16*
- *HP Switch Software Advanced Traffic Management Guide K/KA/KB.15.16*
- *HP Switch Software Basic Operation Guide*
- *HP Switch Software IPv6 Configuration Guide K/KA/KB.15.16*
- *HP Switch Software Management and Configuration Guide K/KA/KB.15.16*
- *HP Switch Software Multicast and Routing Guide K/KA/KB.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.