KA.15.13.0013 Software Fix List

Contents

Description

This fix list covers software versions beginning with KA.15.13.0003.

Version KA.15.13.0003 was the initial release of Major version KA.15.13 software. KA.15.13.0003 software was built from the same source as KA.15.12.0006. KA.15.13.0003 includes all enhancements and fixes in KA.15.12.0006 software, plus the additional enhancements and fixes in the KA.15.13.0003 fix list (below).

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

```
KA.15.11.0003 --> KA.15.11.0004 --> KA.15.11.0005 --> KA.15.11.0007 --> KA.15.11.0008 --> KA.15.11.0009
         |              (KA.15.11.0006 was never built)
         v
KA.15.12.0006 --> KA.15.12.0007 --> KA.15.12.0008 --> KA.15.12.0009 --> KA.15.12.0010 --> KA.15.12.0011
         |          --> KA.15.12.0012 --> KA.15.12.0014 --> KA.15.12.0015
         |              (KA.15.12.0013 was never built)
         v
KA.15.13.0003 --> KA.15.13.0004 --> KA.15.13.0005 --> KA.15.13.0006 --> KA.15.13.0008 --> KA.15.13.0009
                    --> KA.15.13.0010 --> KA.15.13.0011 --> KA.15.13.0012 --> KA.15.13.0013
                        (KA.15.13.0007 was never built)
```

These documents are included in the KA.15.13.0013 software zip file:

- Release Notes Basic Information Guide
- KA.15.12.0006 Release Notes
- KA.15.13.0013 Fix List

Product Models

HP 3800-24G-2SFP+ Switch	(J9575A)
HP 3800-48G-4SFP+ Switch	(J9576A)
HP 3800-24G-PoE+-2SFP+ Switch	(J9573A)
HP 3800-48G-PoE+-4SFP+ Switch	(J9574A)
HP 3800-24SFP-2SFP+ Switch	(J9584A)
HP 3800-24G-2XG Switch	(J9585A)
HP 3800-48G-4XG Switch	(J9586A)
HP 3800-24G-PoE+-2XG Switch	(J9587A)
HP 3800-48G-PoE+-4XG Switch	(J9588A)

Enhancements

Version KA.15.13.0003 Enhancements

Enhancement (CR_0000123302) - Clear DHCP Snooping Counters via CLI. Clears all the statistics counters for DHCP snooping. The statistics are reset to zero. Syntax: **clear dhcp-snooping statistics**.

Enhancement (CR_0000115448) - Disable Debug Without Stopping Syslog. When a syslog server is configured, the forwarding of events begins immediately. The commands **no debug event** or **no debug all** no longer have any effect. The only way to disable the forwarding of events to the Syslog server is by removing the server with the **no logging <ip-address>** command, or the **no logging** command, which removes all Syslog servers. See "Troubleshooting" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000109789) - Identification Field in Static Route Config. When there are a large number of static point-to-point routes, it is helpful to be able to identify the routes using a more meaningful designation than the IP Address. The **name** option allows you to name each configured static route, or to uniquely identify a set of static routes. See "Static Routing" in the *Multicast and Routing Guide* for your switch.

Enhancement (CR_0000112411) - Local Alarm Threshold. The CLI now supports the configuration of RMON alarm threshold settings. The settings can be saved in the configuration file. See "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000111562) - Per-Interface Syslog Event Enable-Disable. This feature provides a per-port filter that can restrict the logging of events that are associated with a link status change. Unimportant linkup/linkdown events can be filtered out, avoiding unwanted messages in the event log and reducing troubleshooting time. See "Troubleshooting" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000111663) - RADIUS Set Port Speed to 10 Mbps. A new RADIUS Vendor Specific Attribute (VSA) - HP-Port-Speed - permits the automated configuration of port speed to 10 Mbps. The port comes up at the auto-negotiated speed during initial authentication, and then the VSA overrides this auto-negotiated speed and configures it to the port speed set in the VSA. A new option, **port-speed-vsa**, is added to the **aaa port-access** command. See "Port-Based and User-Based Access Control (802.1X)" in the *Access Security Guide* for your switch.

Enhancement (CR_0000111892) - sFlow Data Over OOBM. This enhancement provides a configurable option for sending sFlow packets to a destination through the OOBM port on the switch. The sFlow collector collects sample packets through the OOBM port, allowing the monitoring of network traffic. Both IPv4 and IPv6 addresses are supported. See "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000130536) - VRRPv3. Virtual router redundancy protocol (VRRP) provides redundancy in routed networks without requiring configuration of dynamic routing or router discovery protocols. This enhancement adds IPv6 support to VRRP. VRRPv3 supports both IPv4 and IPv6 VRs. VRRPv2 mode is supported for backward compatibility. The maximum number of virtual routers supported stays at 2048, and the maximum number of VRs per VLAN stays at 32. See "Virtual Router Redundancy Protocol (VRRP)" in the *Multicast and Routing Guide* for your switch.

Version KA.15.13.0008 Enhancement

Enhancement (CR_0000132845) - Additional Debug Capability. This enhancement adds tracking to identify possible switch hang situations during switch boot.

Prerequisites

BootROM Update Included!

BootROM updates are needed to be able to boot specified switch software versions. In most cases, selected software versions are used to automatically update the BootROM.

This software includes an update to BootROM version KA.15.09. If your switch has an older version of BootROM, the BootROM will be updated with this KA.15.13.xxxx software.

During the software update, the switch will automatically boot twice. The switch will update the primary BootROM, then reboot, and then update the secondary BootROM. After the switch flash memory is updated and the final boot is initiated, no additional user intervention is needed. **Do not interrupt power to the switch during this important update.**

Fixes

Software fixes are listed in chronological order, from oldest to newest software version. Unless otherwise noted, each software version listed below includes all the software fixes and enhancements added in previous versions listed below.

KA.15.03.3004 was the first software version for the HP 3800 switches.

Version KA.15.13.0003 Fix List

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

Authentication (CR_0000134114) - With both 802.1X and MAC Authentication configured on a port, it is possible for an already-authenticated client to be erroneously moved to the unauthenticated VLAN.

CLI (CR_0000128124) - The output of **show monitor** and **show monitor <mirror_destination_number>** displays information for only mirror destination #1.

CLI (CR_0000131778) - The output of **show oobm** does not include the MAC address of the OOBM interface.

Config (CR_0000129797) - A config file that has the entry **ipv6 ospf3 passive** on a tunnel cannot be downloaded to the switch.

Config (CR_0000131054) - Setting an operator or manager password on the switch causes four features to be disabled: auto run, DHCP-based config file download from an external tftp server, DHCP-based software image download from an external tftp server, and tftp server functionality within the switch. With this fix, more accurate messages are sent regarding the specific features that are disabled by setting the operator or manager password.

Crash (CR_0000118301) - With several trunks that contain a large number of VLANs (on the order of 1000), the switch might reboot unexpectedly with a message similar to `Slot A subsystem went down: 07/17/12 18:19:11 K.15.09.0003 1571, Software exception at msgSys.c:552 -- in 'mNSR', task ID = 0xaa2bdc0, -> Can't get message buffer for msgSys_recv`.

Crash (CR_0000126777) - With a combination of interface state changes along with IPV6 address configuration changes, it is possible for the switch to reboot unexpectedly with a message similar to `SubSystem 0 went down:  01/24/13 13:31:29, Invalid Instr HW Addr=0x000004a8 IP=0x4a8, Task='mIpCtrl' Task ID=0xa9ca140 sp:0x470aab0 lr:0x723f4c, msr: 0x02029200 xer: 0x20000000 cr: 0x48000400`.

Crash (CR_0000127335) - In some situations, issuing the **show tech all** command might cause the switch to reboot unexpectedly with a message similar to `Length Corruption`.

Crash (CR_0000127791) - With OSPF configured, in a rare situation the switch might reboot unexpectedly with a message similar to `Software exception at rt_table.c:4453 -- in 'eRouteCtrl', task ID = 0xa9c4c00 -> Routing Stack: Assert Failed`. This improves the original Crash fix (CR_0000120116).

Crash (CR_0000130339) - In some situations, executing the command **show snmp-server traps** might cause the switch to reboot unexpectedly with a message similar to `Software exception at cli_snmpv2_action.c:9634 -- in mSess2', task ID = 0x13ab0 -> ASSERT: failed`.

Crash (CR_0000131604) - Configuring Mac Authentication with a 256-client limit might cause the switch or stack member to reboot unexpectedly.

DHCP (CR_0000128754) - If the switch is a DHCP client and the DHCP reply contains option 43 with sub-option codes that conflict with RFC 2132 options, the switch might use incorrect settings such as an incorrect subnet mask.

DHCP Snooping (CR_0000126311) - The CLI entry **dhcp-snooping option 82 untrusted-policy keep** is not included in the config file if **no dhcp-snooping option 82** is also configured. If the config file is saved to a TFTP server, it will not function properly when subsequently loaded on a switch.

Distributed Trunking (CR_0000132286) - When a MAC address moves from a Distributed Trunk port to a non-Distributed-Trunk port, the switch MAC tables sometimes show that MAC address on the wrong port.

Distributed Trunking (CR_0000132900) - With a switch configured for both Distributed Trunking and MSTP, a MAC address learned on a VLAN that is not part of the Inter-Switch Connection (ISC) might not appear in the MAC table, or might appear on the wrong port. This issue has been observed when all the Distributed Trunk ports are down on the switch that learns the MAC address.

Dynamic ARP Protection (CR_0000132073) - When a VLAN is configured for dynamic ARP protection and also DHCP snooping, ARP packets should be forwarded but are incorrectly dropped when the **arp-protect** configuration does not include the **validate ip** option.

Enhancement (CR_0000123302) - Clear DHCP Snooping Counters via CLI. Clears all the statistics counters for DHCP snooping. The statistics are reset to zero. Syntax: **clear dhcp-snooping statistics**.

Enhancement (CR_0000115448) - Disable Debug Without Stopping Syslog. When a syslog server is configured, the forwarding of events begins immediately. The commands **no debug event** or **no debug all** no longer have any effect. The only way to disable the forwarding of events to the Syslog server is by removing the server with the **no logging <ip-address>** command, or the **no logging** command, which removes all Syslog servers. See "Troubleshooting" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000109789) - Identification Field in Static Route Config. When there are a large number of static point-to-point routes, it is helpful to be able to identify the routes using a more meaningful designation than the IP Address. The **name** option allows you to name each configured static route, or to uniquely identify a set of static routes. See "Static Routing" in the *Multicast and Routing Guide* for your switch.

Enhancement (CR_0000112411) - Local Alarm Threshold. The CLI now supports the configuration of RMON alarm threshold settings. The settings can be saved in the configuration file. See "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000111562) - Per-Interface Syslog Event Enable-Disable. This feature provides a per-port filter that can restrict the logging of events that are associated with a link status change. Unimportant linkup/linkdown events can be filtered out, avoiding unwanted messages in the event log and reducing troubleshooting time. See "Troubleshooting" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000111663) - RADIUS Set Port Speed to 10 Mbps. A new RADIUS Vendor Specific Attribute (VSA) - HP-Port-Speed - permits the automated configuration of port speed to 10 Mbps. The port comes up at the auto-negotiated speed during initial authentication, and then the VSA overrides this auto-negotiated speed and configures it to the port speed set in the VSA. A new option, **port-speed-vsa**, is added to the **aaa port-access** command. See "Port-Based and User-Based Access Control (802.1X)" in the *Access Security Guide* for your switch.

Enhancement (CR_0000111892) - sFlow Data Over OOBM. This enhancement provides a configurable option for sending sFlow packets to a destination through the OOBM port on the switch. The sFlow collector collects sample packets through the OOBM port, allowing the monitoring of network traffic. Both IPv4 and IPv6 addresses are supported. See "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000130536) - VRRPv3. Virtual router redundancy protocol (VRRP) provides redundancy in routed networks without requiring configuration of dynamic routing or router discovery protocols. This enhancement adds IPv6 support to VRRP. VRRPv3 supports both IPv4 and IPv6 VRs. VRRPv2 mode is supported for backward compatibility. The maximum number of virtual routers supported stays at 2048, and the maximum number of VRs per VLAN stays at 32. See "Virtual Router Redundancy Protocol (VRRP)" in the *Multicast and Routing Guide* for your switch.

GVRP (CR_0000129917) - When the switch receives its own GVRP frames, it learns from them instead of dropping the frames.

Loop Protection (CR_0000127150) - Loop protection fails to detect a loop on a port configured for 802.1X authentication, if 802.1X is not enabled globally.

Management (CR_0000134091) - Disabling write access to an SNMP community via the Web user interface might cause the switch to become unresponsive to command input. The switch must be rebooted to regain management access.

OpenFlow (CR_0000134471) - OpenFlow flows are not programmed correctly when RPVST+ is disabled on the OpenFlow member VLAN.

Passwords (CR_0000130921) - If the switch is configured with a username and password, changing the password causes the username to also change. The username is changed to the default "manager" or "operator", depending on which password is changed.

PIM (CR_0000128681) - After a large number of multicast streams are added and old streams time out, the switch might get into a state where it is unable to add new multicast streams, responding with a message similar to `IpAddrMgr: Failed to allocate new SW IP multicast group, table full FIB entry`.

PIM (CR_0000130353) - The switch might send duplicate multicast packets when sFlow is enabled and the multicast packets are routed by software.

Routing (CR_0000123230) - The switch does not forward traffic to a host that has a static route configured with a 32-bit subnet mask. Traces show that the switch never sends an ARP request for that host.

SNMP (CR_0000122054) - When a large number of traps are generated in a short period of time, the switch buffers might be exhausted. With this fix, switch buffers are protected by several methods, including removing duplicate/identical traps and combining individual intra-switch messages.

SNMP (CR_0000122623) - After rebooting a switch configured for SNMP with the parameters **operator unrestricted**, the switch does not allow the user to set any read/write MIB objects.

SNMP (CR_0000123582) - Including the **detail** parameter in the command **show ipv6 ospf3 link-state area-scope detail** might cause infinite output. This affects the **show tech all** command, which includes the **detail** parameter.

SNMP (CR_0000126364) - SNMP support for DHCP Relay Information (option 82) was inadvertantly disabled.

SNMP (CR_0000129191) - When an SNMP trap destination is set for "no destinations", the log reports an entry of `unknown var type` when the event happens. Also, when the SNMP trap destination is set for "trap receivers only", traps are not sent.

SSL (CR_0000127972) - A self-signed certificate cannot use a common name (CNAME) longer than 40 characters. With this fix, the limit is 90 characters.

Stacking (CR_0000121075) - When stacking is enabled, the switch is accessible via the Web even after disabling the Web server, and via TELNET even after disabling TELNET.

Stacking (CR_0000125606) - After issuing a **boot system flash** command, the Stack Commander erroneously reports that the member switches crashed.

TFTP (CR_0000129475) - A switch config that has certain lines in the config file cannot be downloaded to the switch via TFTP. For example, attempting to download a config file with the valid statement **distributed-trunking peer-keepalive udp-port 6400** results in the error message `UDP port 6400 is already in use`.

Transceivers (CR_0000132781) - Software does not allow the dual-speed J8177C Gigabit-copper transceiver to be configured for 100 Mbps operation, responding with a message such as `Value auto-100 is not applicable to port A21`.

Uplink Failure Detection (CR_0000127868) - On a switch that is configured for uplink failure detection where the link to monitor (LtM) or link to disable (LtD) is an LACP trunk, after reboot the link to monitor is listed as `down` in the output of **show uplink-failure-detection**, and the link to disable is taken down by the switch.

Version KA.15.13.0004 Fix List

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

Accounting (CR_0000133762) - If a Windows system is configured for both computer authentication and user authentication, accounting might not function properly.

CLI (CR_0000137287) - The output of **show run vlan <VLAN_ID>** omits the **no** in the configuration entry **no ip igmp fastleave**. Note that the output of **show run** gives correct information.

Config (CR_0000135481) - After boot, a config file that has a trap destination community name with an open parenthesis "(" or a close parenthesis ")" cannot be downloaded to the switch.

Distributed Trunking (CR_0000135353) - With Distributed Trunking and VRRP enabled, when both the VRRP master and backup routers reboot together, the VRRP master might not be reachable by the Distributed Trunking switches.

Event Log (CR_0000127436) - After the switch uptime reaches 497 days, the timestamp entries in the event log become erratic with gaps of several hours or days. In some cases the timestamps revert to previous months and years, even though SNTP updates with those wrong timestamps report the correct date and time.

Guaranteed Minimum Bandwidth (CR_0000136039) - When the switch is configured to use fewer than the default of 8 queues, packets in lower-priority queues might be unintentionally dropped.

IGMP (CR_0000132149) - Although the RFC requires that the switch with the lowest IP address becomes querier, a switch that is acting as querier stops being querier when it receives a query from a switch with a higher IP address.

IGMP (CR_0000135527) - A non-querier switch that receives a Join from the querier fails to send further Joins to the querier, resulting in loss of multicast traffic.

IGMP (CR_0000136013) - After the switch becomes querier, it does not update the table that defines the querier port, and continues to forward IGMP packets out the port that previously led to the querier.

Link (CR_0000137549) - Gigabit fiber transceivers operate in auto-negotiation mode even if the port is configured for 1000 Mbps full-duplex operation (**speed-duplex 1000-full**). If both sides of the link were configured as 1000-full, the link will go down after the switch at one side of the link is updated with affected software. This issue was introduced in software version 15.12.0006.

MAC Authentication (CR_0000129991) - MAC Authentication fails when the **peap-mschapv2** parameter is included in the **aaa authentication** CLI command.

OSPF (CR_0000135171) - Using the Menu interface, if the user navigates to Switch Configuration -> IP Configuration and selects Save without changing anything on that screen, any OSPF configuration will be removed from every VLAN.

PIM (CR_0000134883) - High CPU utilization from PIM message exchanges causes dropped multicast streams.

RADIUS Accounting (CR_0000137793) - An interim-update status request generates incorrect accounting information in the RADIUS server. This issue was introduced with CR_0000123330.

TFTP (CR_0000123187) - TFTP file transfers initiated via TELNET or SSH fail, if the **console inactivity-timer** setting causes the TELNET or SSH session to end during the transfer. This issue does not affect file transfers initiated from the console or from SFTP.

Trunking (CR_0000126473) - The switch does not allow a static LACP trunk to be configured as active or passive. This fix adds a new interface command: **lacp static [active | passive]**.

Web Management (CR_0000135883) - The "Rx Errors" column is missing from the Web user interface.

Web Management (CR_0000137792) - A self-signed SSL certificate generated via the Web interface cannot use a common name (CNAME) longer than 40 characters. With this fix, the limit is 90 characters.

Version KA.15.13.0005 Fix List

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

BGP (CR_0000138230) - When BGP has equal cost routes but one route is preferred due to a higher configured weight, the outputs of **show ip bgp** and **show ip route** show that the router uses the wrong route.

CLI (CR_0000137695) - The **console terminal <vt100 | none | ansi>** command is only available in config mode. With this fix, the command can be entered directly from the Manager and Operator prompts.

CLI (CR_0000138041) - The command **show ipv6 ospf3 link-state area-scope** does not display any output when more than 25 VLANs are configured on the switch.

Config (CR_0000138447) - After a switch software update, SNMP community access privileges are incorrectly changed by the switch. The output of **show snmp-server** and the output of a "walkmib" command give different results, and neither output represents how the switch actually behaves for Manager or Operator access. This issue was introduced with CR_0000122623; if the access settings were configured on a switch without the CR_0000122623 fix, after updating to software with the CR_0000122623 fix the settings are changed.

Crash (CR_0000115372) - The switch might reboot unexpectedly with a message similar to `NMI event SW:IP=0x00000000 MSR:0x00000000 LR:0x00000000 cr: 0x00000000 sp:0x00000000 xer:0x00000000  Task='InetServer' Task ID=0xaad3000`.

Crash (CR_0000118056) - The switch experiences a loss of free memory each time the **show ip ospf link-state detail** or **display ospf lsdb network** or **display ospf lsdb router** command is issued. When memory is no longer available, the switch will reboot unexpectedly with a message similar to `Software exception at block.c:1165 -- in 'SIGIO Task', task ID = 0xa989fc0 -> Routing Stack: Assert Failed`.

Crash (CR_0000135900) - In some situations it is possible for the switch to reboot unexpectedly with a message similar to `Software exception at alloc_free.c:646 -- in 'eDrvPoll', task ID = 0xa9a7a80 -> buf already freed by 0x0A9A7D40, op=0x0006003E`.

Crash (CR_0000137288) - With SNTP configured, in a rare situation after a time update the switch might reboot unexpectedly with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x31352e30 IP=0x31352e30 Task='mDebugCtrl' Task ID=0x3c9558c0 sp:0x11f92cd0 lr:0x31352e31 msr: 0x02029200 xer: 0x00000000 cr: 0x28000800`.

Crash (CR_0000138879) - After boot, a switch that has a syslog server and an IPv6 address configured might become unresponsive to management, and after a period of time the switch might reboot repeatedly with a message similar to `NMI event SW:IP=0x001517d4 MSR:0x02029200 LR:0x0015178c cr: 0x28000400 sp:0x03aae0e0 xer:0x00000000 Task='mDebugCtrl' Task ID=0xa9f8000`.

Crash (CR_0000141095) - When a switch port is configured for MAC authentication with the **addr-moves** parameter, if a client on that port moves to a different port the switch might reboot unexpectedly with a message similar to `Software exception at hwBp.c:218 -- in 'fault_handler', task ID = 0xa5df1c0 -> MemWatch Trigger: Offending task 'mWebAuth'. Offending IP=0xb35494`.

Crash (CR_0000142271) - The v2 zl modules in a switch might reboot unexpectedly, or the switch itself might reboot unexpectedly, after repeated link toggling of v2 zl module ports or 3800 ports.

Crash (CR_0000142755) - The switch might reboot unexpectedly after repeated link toggling of fiber ports.

DHCP (CR_0000137877) - A switch acting as a DHCP relay agent sends two DHCP packets, one of which incorrectly has the source MAC address of the client instead of the switch.

Display Issue (CR_0000140830) - When **terminal length** is changed from the default of 24, the config file display is truncated, and the outputs of **show logging** and **show interfaces** might be interleaved in the output of **show tech all**.

Guaranteed Minimum Bandwidth (CR_0000138064) - When a 10-Gigabit port on a 3800 switch or v2 zl module is operating at 1-Gigabit, low priority queues might become "starved" and drop traffic.

ICMP (CR_0000134682) - The switch does not log an unsolicited ICMP reply unless it has first pinged some (any) IP address. Also, unsolicited ICMP reply log messages are sometimes associated with the DEFAULT_VLAN instead of the VLAN of the incoming unsolicited ICMP reply.

IGMP (CR_0000138408) - Joins sent by clients in response to a Group Specific Query are not forwarded by the Querier, causing the clients to lose the stream.

IGMP (CR_0000140514) - After disabling IGMP forwarding on a port, multicast traffic incorrectly continues to flow from that port.

Jumbo Frames (CR_0000137961) - When jumbo frames are enabled on any VLAN, OSPF fails to establish an adjacency after a switch reboot, and RIP updates might not be accepted by the router.

Meshing (CR_0000143068) - Multicast traffic and unicast traffic with unknown destination addresses are not routed over the mesh.

Mirroring (CR_0000134191) - IP connectivity to the mirror endpoint switch might be intermittent when remote mirroring is configured on the management VLAN, and mirroring is configured for traffic in **both** directions.

MSTP (CR_0000134194) - With Spanning Tree enabled, configuring a live port as an **admin-edge-port** causes the output of **show run** to display a fixed path-cost for that port in the ist (for example, `spanning-tree instance ist 5 path-cost 20000`). Note that this is a display issue only, the switch uses the automatic path-cost based on the link speed.

Multicast (CR_0000138817) - When a multicast stream is sent to a reserved multicast address, a General Query might not be not forwarded by the switch, causing clients to be dropped from the multicast stream.

OSPF (CR_0000137616) - When the switch is configured as an OSPF neighbor, and the neighbor changes time, OSPF adjacency will temporarily drop.

PIM-SM (CR_0000135871) - In some cases, a "join" from a remote host is not properly processed by the switch and the multicast traffic is not forwarded. This has been observed after a host on the same subnet as the multicast source has joined the stream, and a remote host leaves the multicast stream.

Policy Based Routing (CR_0000134936) - The **show statistics policy** counter is not reset by the **clear statistics policy** command.

sFlow (CR_0000134427) - sFlow sampling of multicast packets sometimes results in duplicate packets that can cause pixelation of video or other degradation of the multicast stream.

TFTP (CR_0000132721) - Certain lines in the configuration file are sometimes incorrectly changed when imported via TFTP. For example, the configuration entry **snmp-server community public unrestricted** might have the **unrestricted** parameter removed when the config file is downloaded via TFTP.

Web Management (CR_0000139666) - Customers using a browser that does not support the X-Frame-Options tag, and who have an open Web management session and then initiate another browser session, could be vulnerable to cross-frame scripting.

Web Management (CR_0000140379) - A self-signed SSL certificate and a CA-generated certificate cannot use an organizationName, organizationalUnitName, localityName, stateOrProvinceName longer than 40 characters. With this fix, the limit is 64 characters.

Version KA.15.13.0006 Fix List

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

Config (CR_0000145562) - A switch with an active radio port and configured with the command **lldp auto-provision radio-ports auto-vlan 2100** will move the radio ports into VLAN 2101 after a reboot. Similar errors occur for other **auto-vlan** numbers; after reboot the switch creates and uses a new VLAN instead of using the configured VLAN for radio ports.

Console (CR_0000140941) - The **console inactivity-timer** setting is applied even if the user is typing on the console, when the console physical connection is to a stack member instead of the commander.

Counters (CR_0000141119) - The output of **show ip counters** is incorrect when routing is enabled for IP, IPv6, or multicasts.

Counters (CR_0000142198) - When a trunk configured for sFlow polling is simultaneously queried via SNMP, all counter values for the trunk are zero.

Counters (CR_0000143860) - On a switch configured with rapid PVST and BPDU protection, the output of the command **show spanning-tree bpdu-protection** shows zero `errant BPDUs` received, even when the switch has disabled a port due to receiving a BPDU. This is a display issue only, both rapid PVST and BPDU protection function properly.

Crash (CR_0000137552) - With OSPF enabled, if one switch has jumbo frames enabled but the link partner does not, the switch might reboot unexpectedly with a message similar to `Software exception at block.c:1158 -- in 'SIGIO Task', task ID = 0xa94f800 -> Routing Stack: Assert Failed`.

Crash (CR_0000139042) - With a physical stack in operation, issuing a command such as **show tech statistics** when one of the stack members is rebooting or otherwise not communicating might cause the switch to reboot unexpectedly with a message similar to `Software exception at ppmgr_globals.c:270 -- in 'mSess3', task ID = 0x3c8ae780 -> Port record out of bounds`.

Crash (CR_0000141877) - With MSTP enabled, when the event log receives a large number of entries in a very short time, the switch might reboot unexpectedly with a message similar to `Software exception at svc_misc.c:865 -- in 'mMstpCtrl', task ID = 0xa953140 -> Failed to calloc 700 bytes`.

Crash (CR_0000143067) - Under extremely heavy traffic loads, repeated port toggling might cause the switch to reboot unexpectedly with a message similar to `Software exception at bgp_tsi.c:361 -- in 'eRouteCtrl', task ID = 0xa95fcc0 -> Routing Stack: Assert Failed`.

Crash (CR_0000144879) - The switch might reboot unexpectedly in these situations:
1) The switch is running 15.08 or earlier software, is configured to drop frames that have a destination address of 01:00:0c:cc:cc:cd, and has PVST filtering or PVST protection enabled. Then the switch is updated to 15.09 or later software.
2) The switch is running 15.09 or later software, is configured to drop frames that have a destination address of 01:00:0c:cc:cc:cd, and then PVST filtering or PVST protection is enabled.
The switch reboots unexpectedly with a message similar to `Software exception at bttfLearn.c:2616 -- in 'mLpmgrCtrl', task ID = 0xa98a9c0 -> Mac Table Error`.

Crash (CR_0000146306) - The switch uses TCP connections internally for inter-process communication. In a situation where an internal loopback TCP socket pair receives stimulus after an extended period of idle time, the switch might reboot unexpectedly with a message similar to `NMI event SW:IP=0x00e20c1c MSR:0x02029200 LR:0x00e077d0 cr: 0x44000400 sp:0x02b03c58 xer:0x00000000 Task='InetServer' Task ID=0xab31000`.

Distributed Trunking (CR_0000144697) - Distributed Trunking LACP links do not come up when connected to non-HP devices such as Solaris Unix systems.

Mirroring (CR_0000145818) - With more than one remote mirroring session configured on a VLAN, if the user deletes a VLAN with a lower number than the VLAN being mirrored, all mirrors except the lowest-numbered mirror session are removed from the mirrored VLAN.

OSPF (CR_0000134463) - When the router receives multiple duplicate LSAs in a short time period, the router does not acknowledge them all in time, which causes OSPF adjacencies to be lost and then re-formed.

RADIUS (CR_0000138258) - In some situations, the switch response to "Change of Authorization" and "Disconnect Messages" from the RADIUS server is sent from an incorrect source IP address, which the RADIUS server therefore ignores.

Spanning Tree (CR_0000143817) - With a switch configured for MSTP, if the spanning tree mode is changed to **force-version rstp-operation** and then a second management module (or stack member) is inserted, the switch might reboot unexpectedly with a message similar to `Health Monitor: Read Error Restr Mem Access HW Addr=0xe59ff10c IP=0x779004c Task='mMstpCtrl' Task ID=0x13af9740 fp: 0x0d372620 sp:0x0d372604 cpsr: 0x6000001f`.

Switch Hang (CR_0000142411) - On a switch configured for Web or MAC authentication plus MSTP plus Distributed Trunking with keepalive, with high levels of reauthentication occurring on multiple ports, the switch might appear to hang and be unreachable for remote management. The console is initially accessible, but issuing a **show** command might cause the console to also hang. This affects LACP and LLDP protocols, as seen by neighboring switches.

Transceivers (CR_0000143444) - Software does not allow the dual-speed J8177C Gigabit-copper transceiver to be configured for 100 Mbps operation, responding with a message such as `Value auto-100 is not applicable to port A21`. This is the same fix as CR_0000132781 in 15.13.0003, which was inadvertently removed by CR_0000126473 in 15.13.0004 software.

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.

Version KA.15.13.0007

Status: Never built.

Version KA.15.13.0008 Fix List

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

Authentication (CR_0000148832) - A switch configured with RADIUS authentication for primary login, and local authentication for secondary login fails to use local authentication when RADIUS servers do not respond. In that situation, the switch console is not accessible to valid users.

BPDU Protection (CR_0000144148) - If VLAN 1 is not enabled on the link between a switch running rapid PVST and a switch running any Spanning Tree version, a rapid PVST switch configured for BPDU protection does not shut down the port when it receives a BPDU from the neighboring switch. However, the BPDUs are correctly dropped.

CLI (CR_0000136134) - After issuing the command **no ip ssh cipher <cipher_option>**, the entry is listed twice in the output of **show run**.

CLI (CR_0000143652) - The switch does not allow the **lockout-mac** command to be configured for a MAC address that is all zeros (000000-000000).

Config (CR_0000145221) - The switch prompts users to save the configuration when no changes have been made. This has been observed after configuring meshing, saving the config, and rebooting the switch.

Console (CR_0000148468) - With a console cable connected to a stack member, if the user issues the **show tech all** command and then attempts to cancel the output by entering **<CTRL-C>**, the output pauses but then continues for a long time (up to 30 minutes for a five-member stack). Note that the fix has a small side-effect: Entering **<CTRL-C>** will cause a short delay before the console prompt returns.

Crash (CR_0000139181) - After configuring a RADIUS server for both IPv4 and IPv6, if the software is downgraded to a version that does not support RADIUS on IPv6, and then upgraded to a software version that supports RADIUS on IPV6, the switch might reboot unexpectedly with a message similar to `Software exception at ip_util.c:1171 -- in 'swInitTask', task ID = 0x3c971540 -> ASSERT:  failed`.

Distributed Trunking (CR_0000148165) - When VRRP routers have Distributed Trunking enabled, VRRP failovers might result in the VRRP virtual MAC addresses (and therefore remote subnets) to become unreachable.

Distributed Trunking (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.

Enhancement (CR_0000132845) - Additional Debug Capability. This enhancement adds tracking to identify possible switch hang situations during switch boot.

IPv6 (CR_0000148594) - IPv6 Router Advertisements that indicate an off-link prefix are not set as "preferred" in the switch, which causes incorrect information in the output of **show ipv6**, and can affect connectivity to hosts that use IPv6 Stateless Address Autoconfiguration. This issue also causes the sFlow "Agent Address" to be listed as 0.0.0.0.

Logging (CR_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.

Logging (CR_0000150244) - Some RMON events are not correctly defined for fault-finder (FFI), SSL, and virus throttling, which causes the switch to report an error such as `system: Unknown Event ID 776` when those events occur.

PoE (CR_0000142629) - When the switch experiences an AC power glitch, the switch reports a power supply failure and incorrectly drops PoE power to all connected powered devices (PDs).

PoE (CR_0000147518) - After reboot, pre-standard detection of PoE devices does not function correctly on a 2920 or 3800 stack, if the stack commander is a non-PoE switch.

PoE (CR_0000148808) - After disabling PoE on one or more ports, the output of **show cpu slot <slot-number>** shows an increase in CPU utilization of 15% or more.

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 auto-configuration, sFlow incorrectly uses the link-local address as the agent ID.

SNMP (CR_0000147370) - After using SNMP to configure a RADIUS server on the switch, the switch does not allow a login until the switch is rebooted.

SNMP (CR_0000149657) - When using the "createAndWait" mode to set parameters via SNMP, multiple RADIUS servers cannot be configured.

Switch Hang (CR_0000146247) - With both authentication and accounting enabled, the switch might become unresponsive to management, requiring a reboot to recover.

TELNET (CR_0000142571) - While a user is being authenticated by a RADIUS server, issuing the **show access-list radius all** command from a TELNET session might cause the TELNET session to hang.

Web Management (CR_0000149099) - When Spanning Tree Protocol (STP) is enabled via the Web user interface, "mstp" is shown as the default STP mode, and "mstp" is displayed as the operational mode after the user enables STP and saves the change. However, the command line interface shows that the switch operates in "rpvst" mode. Workaround: From the Web user interface, use the dropdown menu to explicitly select "mstp" from the dropdown options, then save the change.

Version KA.15.13.0009 Fix List

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

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).

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

Version KA.15.13.0010 Fix List

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

Crash (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`.

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

Version KA.15.13.0011 Fix List

Status: Never released.

Crash (CR_0000153524) - Entering the command **show ipv6 ospf3 link-state area-scope detail** might 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`, given one of the following conditions:
1) There are more than 64 OSPFv3-enabled VLANs
2) There are more than 64 neighbors on an OSPFv3-enabled broadcast link
3) There are more than 64 addresses advertised in a NAP LSA
4) There are more than 64 IPv6 addresses on an OSPFv3-enabled VLAN

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.

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.

Version KA.15.13.0012 (No Fixes)

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

Version KA.15.15.0013 Fix List

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

802.1X (CR_0000149780) - Already-authenticated clients that send an EAPOL-Start message are de-authenticated by the switch. This situation happens if the client runs Windows Vista and later operating systems that are set to "include learning".

CLI (CR_0000148661) - When the output of **show power-over-ethernet brief** displays a Detection Status of either `Searching` or `Delivering` for a port, the **show tech all** "poe_status_port all" section displays `Other Fault` as the "Detect Stat".

CLI (CR_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.

Config (CR_0000149526) - Enabling stacking on a switch that has a trunk configured creates an invalid entry for the trunk in the config file. The resulting configuration file cannot be downloaded to the switch.

Crash (CR_0000152222) - With multiple authentication protocols active in a high-stress environment, the switch might reboot unexpectedly with a message similar to `NMI event HW:IP=0x0103191c MSR:0x02029200 LR:0x00121208 cr: 0x20000800 sp:0x02d56220 xer:0x20000000 Task='tDevPollRx' Task ID=0x2d3fc78`.

Management (CR_0000149528) - In some situations with multiple TELNET and/or SSH sessions established, the switch does not accept additional management sessions even if some of the existing ones are killed, responding with the message `Sorry, the maximum number of sessions are active. Try again later`.

PoE (CR_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.

SNMP (CR_0000151035) - The switch incorrectly reports that MIB object entPhysicalIsFRU = False for removable fantrays, power supplies, and transceivers.

SNMP (CR_0000154463) - The switch incorrectly reports that MIB object entPhysicalIsFRU = False for transceivers for some switches. This improves the original SNMP fix (CR_0000151035).

September 2014