A.15.14.0007 Software Fix List

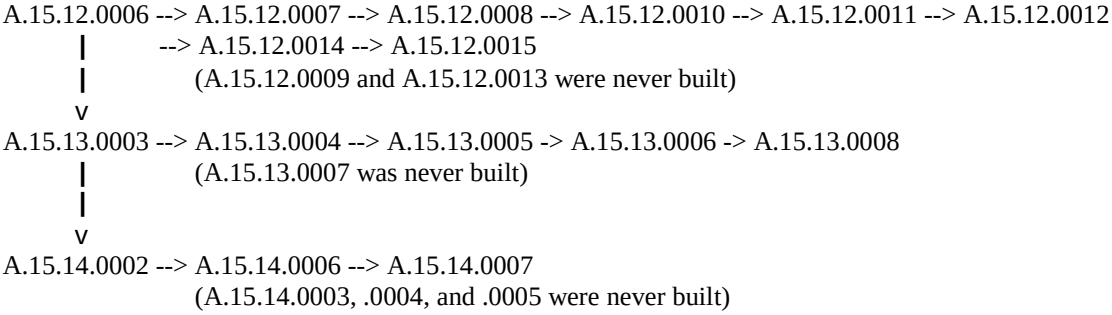
Contents

Description

This fix list covers software versions beginning with A.15.14.0002.

Version A.15.14.0002 was the initial release of Major version A.15.14 software. A.15.14.0002 software was built from the same source as A.15.13.0003. A.15.14.0002 includes all enhancements and fixes in A.15.13.0003 software, plus the additional enhancements and fixes in the A.15.14.0002 fix list (below).

Here is a visual depiction of the software sequence, showing how each Major version (for example A.15.13) is based on the previous Major version - and then additional fixes are added to Minor versions (for example A.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.



These documents are included in the A.15.14.0007 software zip file:

- Release Notes Basic Information Guide
- A.15.12.0006 Release Notes
- A.15.13.0003 Fix List
- A.15.14.0007 Fix List

Product Models

HP 2615-8-PoE Switch (J9565A)
HP 2915-8G-PoE Switch (J9562A)

Enhancements

Version A.15.14.0002 Enhancements

Enhancement (CR_0000115812) - Certificate Manager. Certificate Manager enables Public Key Infrastructure (PKI) capability on the switch providing authentication of network entities. See "Certificate Manager" in the *Access Security Guide* for your switch.

Enhancement (CR_0000134999) - Chassis Locate LED at Boot. The **chassislocate** command has an optional parameter that configures it to run in the future instead of immediately. See Appendix C "Troubleshooting" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000129524) - DHCPv4 Snooping Max Binding. DHCP snooping max-binding prevents binding entries from getting exhausted. This feature is on a per-port basis and restricts the maximum number of bindings allowed on a port/interface. The maximum bindings for a particular port includes both statically configured and dynamically learned. The number of bindings on a per port basis is incremented upon a lease offer and decremented upon a lease expiry or release. See "Port Security" in the *Access Security Guide* for your switch.

Enhancement (CR_0000126020) - Differentiated Services Code Point (DSCP)-Based Rate Limiting. This enhancement implements access-method for authorized managers and QoS rate limiting for the HP 2615 and 2915 switches. It is implemented on a per-port basis and has no performance impact on the data-plane of in-profile (metered) or out-of-profile (not metered) traffic. Each code point can be configured to be rate-limited on a given port or ports. See "Port Traffic Controls" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000129156) - Download Software via DHCP. Adds the option to specify the location of switch software via DHCP.

Enhancement (CR_0000127014) - Filtering PVID Mismatch Log Messages. This enhancement filters out PVID mismatch log messages on a per-port basis. PVID mismatches are logged when there is a difference in the PVID advertised by a neighboring switch and the PVID of the switch port which receives the LLDP advertisement. However, if these events are logged too frequently, they can overwhelm the log buffer and push relevant logging data out of log memory, making it difficult to troubleshoot another issue. See "Troubleshooting" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000140539) - FIPS Mocana 5.7 Upgrade. The internal security/cryptography code has been improved to prevent circumvention. (This does not affect YB-software.)

Enhancement (CR_0000127640) - IPv6 QoS. Enables the switch to mark matching TCP or UDP packets with an 802.1p priority. See "Quality of Service: Managing Bandwidth Effectively" in the *Advanced Traffic Management Guide* for your switch.

Enhancement (CR_0000127665) - IPv6 QoS Setting. Adds IPv6 as an option for the **qos device-priority** command. See the *Advanced Traffic Management Guide* for your switch. (This does not affect YB-software.)

Enhancement (CR_0000127933) - IPv6 VLAN ACLs. IPv6 VLAN ACLs filter traffic entering the switch on a VLAN configured with the VLAN ACL option. See "IPv6 Access Control Lists (ACLs)" in the *IPv6 Configuration Guide* for your switch.

Enhancement (CR_0000127160) - Link Aggregation Control Protocol-Multi-Active Detection (LACP-MAD) is a detection mechanism deployed by switches to recover from a breakup of the Intelligent Resilient Framework (IRF) stack due to link or other failure. See "Port Trunking" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000130301) - MAC-Based VLANs (MBVs). MBVs allow multiple clients on a single switch port to receive different untagged VLAN assignments. VLAN assignment of untagged traffic is based on the source MAC address rather than the port. See "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide* for your switch. (This does not affect YA-software.)

Enhancement (CR_0000132219) - Multiple Features Added - This enhancement adds many new features:
1) Support for the hop count field in DHCP packets. See the *Basic Operation Guide* for your switch.
2) Enables the **ip dns dhcp** command for IPv6.
3) Extended Ping Traceroute. Enhances the **traceroute** command used for network troubleshooting.
4) Enables the **fault-finder link-flap** command to detect unstable links that are constantly going up and down. See Appendix C "Troubleshooting" in the *Management and Configuration Guide* for your switch.
5) Enables the **fault-finder** option to disable ports on fault. See Appendix C "Troubleshooting" in the *Management and Configuration Guide* for your switch.
6) Enables the **qos watch-queue** and **show interface queue** commands for monitoring drops per queue, used to analyze traffic prioritization and tune QoS policies appropriately. See "Quality of Service: Managing Bandwidth Effectively" in the *Advanced Traffic Management Guide* for your switch.
7) Enables the **trunk-load-balance** command for configuring the trunk load balancing algorithm so both ends can be configured for the same algorithm and trunk traffic is load-balanced the same way on both ends. See "Port Trunking" in the *Management and Configuration Guide* for your switch.
8) Adds throttling for LLDP messages to avoid filling the event log.
9) Adds support for the VLAN TLV and VLAN name TLV for LLDP.
10) Provides a better tuned **lockout-mac** command limit. See "Port Security" in the *Access Security Guide* for your switch.
11) Enables the **session** command. See "Using the Command Line Interface (CLI)" in the *Basic Operation Guide* for your switch.

Enhancement (CR_0000126775) - Router Advertisement (RA) Guard. The RA Guard feature restricts the ports (or trunks) that can accept IPv6 Router Advertisements (RAs). Additionally, ICMPv6 router redirects are blocked on the configured ports. See "IPv6 Router Advertisements" in the *IPv6 Configuration Guide* for your switch. (This does not affect YA-software.)

Enhancement (CR_0000131581) - Smartlink is a switch feature that provides effective, simple and fast-converging link redundancy in network topology with dual uplink between different layers of the network. It requires an active (master) and a backup (slave) link. The active link carries the uplink traffic. Upon failure of the active link, a switchover is triggered and the traffic is directed to the backup link. See "Smartlink" in the *Advanced Traffic Management Guide* for your switch.

Enhancement (CR_0000135708) - SNMP Trap When MAC Address Table Changes. This enhancement causes an SNMP trap to be generated once a laptop/PC is removed from the back of an IP phone and the laptop/PC MAC address ages out of the MAC table. See "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000127927) - Updated IGMP Type Numbers and Keywords. For an updated list of IGMP type numbers and keywords, see "RADIUS Server Support for Switch Services" in the *Access Security Guide* for your switch.

Enhancement (CR_0000128607) - VLAN-Based Loop Protection. VLANs can now be configured for loop protection. See "Multiple Instance Spanning Tree Operation" in the *Advanced Traffic Management Guide* for your switch.

Enhancement (CR_0000135776) - VLAN-Based Rate Limiting. This enhancement provides specific bandwidth for a specific VLAN for the ingress traffic on this VLAN. The specified VLAN drops all traffic that exceeds the configured rate. See "Port Traffic Controls" in the *Management and Configuration Guide* for your switch.

Version A.15.14.0007 Enhancement

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

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.

Version A.15.14.0002 Fix List

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

802.1X (CR_0000134257) - After 802.1X frame counters reach a maximum value of 2,147,483,647, the counters are displayed as negative values that become smaller until they reach zero. When the counters reach zero, they begin incrementing again.

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

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_0000136428) - CLI output for **show ip igmp vlan x conf** displays a plus sign under the Interconnect Trunk column heading, and nothing (blank) under the Port column heading.

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.

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.

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.

Config (CR_0000139251) - When a configuration file is downloaded to the switch, a default SNMPv3 user named "initial" is created on the switch even though it is not in the config file.

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_0000127791) - 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_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`.

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 (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.

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_0000115812) - Certificate Manager. Certificate Manager enables Public Key Infrastructure (PKI) capability on the switch providing authentication of network entities. See "Certificate Manager" in the *Access Security Guide* for your switch.

Enhancement (CR_0000134999) - Chassis Locate LED at Boot. The **chassislocate** command has an optional parameter that configures it to run in the future instead of immediately. See Appendix C "Troubleshooting" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000129524) - DHCPv4 Snooping Max Binding. DHCP snooping max-binding prevents binding entries from getting exhausted. This feature is on a per-port basis and restricts the maximum number of bindings allowed on a port/interface. The maximum bindings for a particular port includes both statically configured and dynamically learned. The number of bindings on a per port basis is incremented upon a lease offer and decremented upon a lease expiry or release. See "Port Security" in the *Access Security Guide* for your switch.

Enhancement (CR_0000126020) - Differentiated Services Code Point (DSCP)-Based Rate Limiting. This enhancement implements access-method for authorized managers and QoS rate limiting for the HP 2615 and 2915 switches. It is implemented on a per-port basis and has no performance impact on the data-plane of in-profile (metered) or out-of-profile (not metered) traffic. Each code point can be configured to be rate-limited on a given port or ports. See "Port Traffic Controls" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000129156) - Download Software via DHCP. Adds the option to specify the location of switch software via DHCP.

Enhancement (CR_0000127014) - Filtering PVID Mismatch Log Messages. This enhancement filters out PVID mismatch log messages on a per-port basis. PVID mismatches are logged when there is a difference in the PVID advertised by a neighboring switch and the PVID of the switch port which receives the LLDP advertisement. However, if these events are logged too frequently, they can overwhelm the log buffer and push relevant logging data out of log memory, making it difficult to troubleshoot another issue. See "Troubleshooting" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000140539) - FIPS Mocana 5.7 Upgrade. The internal security/cryptography code has been improved to prevent circumvention. (This does not affect YB-software.)

Enhancement (CR_0000127640) - IPv6 QoS. Enables the switch to mark matching TCP or UDP packets with an 802.1p priority. See "Quality of Service: Managing Bandwidth Effectively" in the *Advanced Traffic Management Guide* for your switch.

Enhancement (CR_0000127665) - IPv6 QoS Setting. Adds IPv6 as an option for the **qos device-priority** command. See the *Advanced Traffic Management Guide* for your switch. (This does not affect YB-software.)

Enhancement (CR_0000127933) - IPv6 VLAN ACLs. IPv6 VLAN ACLs filter traffic entering the switch on a VLAN configured with the VLAN ACL option. See "IPv6 Access Control Lists (ACLs)" in the *IPv6 Configuration Guide* for your switch.

Enhancement (CR_0000127160) - Link Aggregation Control Protocol-Multi-Active Detection (LACP-MAD) is a detection mechanism deployed by switches to recover from a breakup of the Intelligent Resilient Framework (IRF) stack due to link or other failure. See "Port Trunking" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000130301) - MAC-Based VLANs (MBVs). MBVs allow multiple clients on a single switch port to receive different untagged VLAN assignments. VLAN assignment of untagged traffic is based on the source MAC address rather than the port. See "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide* for your switch. (This does not affect YA-software.)

Enhancement (CR_0000132219) - Multiple Features Added - This enhancement adds many new features:
1) Support for the hop count field in DHCP packets. See the *Basic Operation Guide* for your switch.
2) Enables the **ip dns dhcp** command for IPv6.
3) Extended Ping Traceroute. Enhances the **traceroute** command used for network troubleshooting.
4) Enables the **fault-finder link-flap** command to detect unstable links that are constantly going up and down. See Appendix C "Troubleshooting" in the *Management and Configuration Guide* for your switch.
5) Enables the **fault-finder** option to disable ports on fault. See Appendix C "Troubleshooting" in the *Management and Configuration Guide* for your switch.
6) Enables the **qos watch-queue** and **show interface queue** commands for monitoring drops per queue, used to analyze traffic prioritization and tune QoS policies appropriately. See "Quality of Service: Managing Bandwidth Effectively" in the *Advanced Traffic Management Guide* for your switch.
7) Enables the **trunk-load-balance** command for configuring the trunk load balancing algorithm so both ends can be configured for the same algorithm and trunk traffic is load-balanced the same way on both ends. See "Port Trunking" in the *Management and Configuration Guide* for your switch.
8) Adds throttling for LLDP messages to avoid filling the event log.
9) Adds support for the VLAN TLV and VLAN name TLV for LLDP.
10) Provides a better tuned **lockout-mac** command limit. See "Port Security" in the *Access Security Guide* for your switch.
11) Enables the **session** command. See "Using the Command Line Interface (CLI)" in the *Basic Operation Guide* for your switch.

Enhancement (CR_0000126775) - Router Advertisement (RA) Guard. The RA Guard feature restricts the ports (or trunks) that can accept IPv6 Router Advertisements (RAs). Additionally, ICMPv6 router redirects are blocked on the configured ports. See "IPv6 Router Advertisements" in the *IPv6 Configuration Guide* for your switch. (This does not affect YA-software.)

Enhancement (CR_0000131581) - Smartlink is a switch feature that provides effective, simple and fast-converging link redundancy in network topology with dual uplink between different layers of the network. It requires an active (master) and a backup (slave) link. The active link carries the uplink traffic. Upon failure of the active link, a switchover is triggered and the traffic is directed to the backup link. See "Smartlink" in the *Advanced Traffic Management Guide* for your switch.

Enhancement (CR_0000135708) - SNMP Trap When MAC Address Table Changes. This enhancement causes an SNMP trap to be generated once a laptop/PC is removed from the back of an IP phone and the laptop/PC MAC address ages out of the MAC table. See "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

Enhancement (CR_0000127927) - Updated IGMP Type Numbers and Keywords. For an updated list of IGMP type numbers and keywords, see "RADIUS Server Support for Switch Services" in the *Access Security Guide* for your switch.

Enhancement (CR_0000128607) - VLAN-Based Loop Protection. VLANs can now be configured for loop protection. See "Multiple Instance Spanning Tree Operation" in the *Advanced Traffic Management Guide* for your switch.

Enhancement (CR_0000135776) - VLAN-Based Rate Limiting. This enhancement provides specific bandwidth for a specific VLAN for the ingress traffic on this VLAN. The specified VLAN drops all traffic that exceeds the configured rate. See "Port Traffic Controls" in the *Management and Configuration Guide* for your switch.

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.

GVRP (CR_0000130090) - After rebooting the switch, the configuration **unknown-vlans disable** does not work on trunks.

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_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.

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.

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.

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.

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

MSTP (CR_0000132175) - In a complicated sequence of events with multiple MSTP instances and UDLD configured on only one path between switches, after link failure and link restoration it is possible for MSTP to begin forwarding on a port that should be blocked, causing a network topology loop.

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 which password is changed.

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

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.

sFlow (CR_0000128439) - When an sFlow-sampled inbound packet is to be routed, the sFlow data gives the wrong output port on the switch.

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_0000134672) - The entStateOper OID from the Entity State MIB gives an incorrect value of 1 (unknown) instead of 3 (enabled), for some switches.

SNMP (CR_0000135477) - A trap from an undocumented OID can be triggered under certain conditions. With this fix, OID 1.3.6.1.4.1.11.2.3.7.11.107.0.2 has been added to the MIB.

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.

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 via the console or via SFTP.

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`.

Transceivers (CR_0000136125) - The switch allows the user to configure the 1000BASE-T transceiver (J8177B/C) for 100-Megabit operation, but that setting is not supported. The transceiver operates at Gigabit speed despite the 100-Megabit setting.

Transceivers (CR_0000140560) - The port shows link, but no traffic passes through a J4858C Gigabit-SX transceiver when the port is configured for **1000-full** operation.

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 A.15.14.0003

Status: Never built.

Version A.15.14.0004

Status: Never built.

Version A.15.14.0005

Status: Never built.

Version A.15.14.0006 Fix List

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

CLI (CR_0000143577) - The switch allows users to configure a 1000BASE-T port with the setting **speed-duplex 1000-full**, which is not a valid setting for 1000BASE-T ports according to the IEEE spec.

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_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`.

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**.

Fastboot (CR_0000141043) - If the fastboot setting is changed by the user, and the switch experiences a power interruption or reboot while the new setting is being written to flash, upon bootup the MAC address on a switch or stack member might be erased. Note that this fix has a side effect: If the fastboot setting is changed by the user and the switch software is downgraded (changed to an earlier version), upon bootup the fastboot setting might revert to what it was before the user-initiated change, even though the switch reports that it has been changed. Workaround: Change the fastboot setting twice - first change it back to what it was before the user-initiated change, then change fastboot to the desired setting.

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

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

IP Phones (CR_0000147849) - Alcatel phones might reboot unexpectedly when connected to a switch configured for IP phones to use MAC authentication and for PCs to use 802.1X authentication.

MAC Table (CR_0000143371) - A MAC table entry does not age out while there is traffic destined to the MAC address, even if no traffic is received from that MAC address.

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.

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.

sFlow (CR_0000143703) - sFlow samples for a trunk include the interface index of one of the trunk ports instead of the interface index of the trunk.

Stacking (CR_0000135643) - With the default terminal size of 80x24, connecting to the stack commander via TELNET or SSH results in the list of stack member switches displayed below the command prompt, with each additional member overwriting the previous one, leaving only the last stack member visible to the user.

TFTP (CR_0000143546) - With sFlow sampling enabled on the uplink port, in some situations a TFTP transfer from the switch fails with the message `Error in sending file. Exceeded max number of retransmits`.

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.

Version A.15.14.0007 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_0000142154) - The output of **show tech** halts after displaying **show debug buffer**, with the message `=== The command has completed with errors. ===`.

Crash (CR_0000150015) - With DHCP snooping enabled, the switch might go into a continual boot cycle, with messages similar to `Health Monitor:  Misaligned Mem Access HW Addr=0x0fc7ae2e IP=0x465ecf4 Task='eDrvPoll' Task ID=0xe0e2380 fp: 0x0685b4d4 sp:0x0685b4a0 cpsr: 0x6000001f dfsr: 0x00000001`.

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_0000146773) - In an IPv4 plus IPv6 environment, upon switch bootup the event log displays the set of source IP policy ("srcip") messages twice. With this fix, IPv6 policy messages are distinguished from IPv4 policy messages.

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

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

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

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

sFlow (CR_0000142777) - When sFlow is enabled, 802.1X authentication might fail, causing users to be randomly locked out of the network for 20 minutes.

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_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.

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

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.

July 2014

Return to Contents