Hewlett Packard Enterprise

J.15.09.0028 Release Notes

Abstract

This document contains supplemental information for the J.15.09.0028 release.

Part Number: 5200-2169
Published: September 2016
Edition: 1

Acknowledgments

Microsoft®, Windows®, and Windows Server® are U.S. registered trademarks of the Microsoft group of companies.

Contents

1 J.15.09.0028 Release Notes

Description

This release note covers software versions for the J.15.09 branch of the software.

This document covers software versions beginning with J.15.09.0023.

Product series supported by this software:

- HPE 2520G Switch Series

Important information

To avoid damage to your equipment, do not interrupt power to the switch during a software update.

Products supported

This release applies to the following product models:

Product number	Description
J9298A	HPE 2520 8G PoE Switch
J9299A	HPE 2520 24G PoE 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 only the software versions that contain enhancements found in the J.15.09 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. The last release that introduced enhancements was J.15.09.0012.

NOTE: The number that precedes the enhancement description is used for tracking purposes.

Version J.15.09.0012

Traffic Templates

CR_0000123968 The HP 2520G switches currently implement priority-to-queue mapping as defined in the IEEE 802.1D-2004 Annex G standard. Another standard, IEEE 802.1Q-2005, defines a slightly different mapping where the ordering of priorities 0-2 is changed. This enhancement allows you to configure the switch to follow either standard. The HP 2520G switch supports two or four outbound queues. When only two queues are configured, the priority-to-queue mapping is the same as that based on the IEEE 802.1Q-2005 standard. When four outbound queues are configured, the mappings are different. For more information on queues, see "Quality of Service: Managing Bandwidth more Effectively" in the *Advanced Traffic Management Guide* for your switch.

Version J.15.09.0003

CDPv2 Transmit Capability

CR_0000107011 When a Cisco VoIP phone boots up (or sometimes periodically), it queries the switch and advertises information about itself using CDPv2. The switch receives the VoIP VLAN Query TLV (type 0x0f) from the phone and then immediately sends the voice VLAN ID in a reply packet to the phone using the VLAN Reply TLV (type 0x0e). The phone then begins tagging all packets with the advertised voice VLAN ID.

Terminal Line Width and Length

CR_0000074537 For console/serial link and inbound Telnet sessions, the switch output:

- Uses whatever width is set by the terminal program. If the width is not specified, 80 characters is the default.
- Automatically wraps on word boundaries (such as spaces) for non-columnar output.
- Automatically wraps on column boundaries for columnar output.

Hewlett Packard Enterprise recommends that you do not set your terminal width (**`terminal width <y>`**) above 150 columns.

Version J.15

MAC Limit Notify

PR_0000073085, CR_0000077875 The MAC Address Count feature provides a way to notify the switch management system when the number of MAC addresses learned on a switch port exceeds the permitted configurable number.

Reporting Config Changes

PR_0000069196, CR_0000074531 This feature provides the ability to track and report information about switch management processes on a per-user, per-session basis. Syslog or RADIUS is used for logging the information.

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 preceding the fix description is used for tracking purposes.

Version J.15.09.0028

File Transfer

CR_0000211619 Symptom: The switch is administratively rebooted/reloaded before finalizing writing OS image files to the flash file system.

Scenario: When OS image files are put into the switch via SCP/SFTP, the switch allows execution of the CLI command `boot system flash [primary|secondary]` before finalizing writing OS image files to the flash file system. This can lead to a corrupted OS image on the flash and the inability of the switch to boot from that OS. The switch will failback to the uncorrupted primary/secondary OS image, if available.

Workaround: Reboot/reload the switch after confirming the OS image files are completely written to the flash file system. Verify the switch event log system for a message similar to `Update: Primary Image updated` or `Update: Secondary Image updated.`

Online Help

CR_0000201063 Symptom: Web management help file is not accessible.

Scenario: The web management interface online help file URL changed to accommodate domain change for host files.

Spanning Tree

CR_0000202511 Symptom: Incorrect spanning tree hello time is reported as a MIB value.

Scenario: In a spanning tree topology, the switch reports the value of OID dot1dStpHelloTime on a root switch in seconds instead of centiseconds as reported in non-root switches.

Workaround: There is no impact on spanning tree functionality as this is merely a value conversion from seconds to centiseconds.

Version J.15.09.0027

TFTP

CR_0000180230 Symptom: TFTP transfer does not work with packet sizes other than 1416 bytes.

Workaround: Configure TFTP client to use a packet size of 1416 bytes.

Version J.15.09.0026

Config

CR_0000175001 When the value of any event's `eventtype` is set to a non-default value, after the switch is rebooted, the new value that has been set does not take effect. The issue lies with reading of the value from the file after reload.

Version J.15.09.0025

Crash

CR_0000158589 When GVRP is configured and active, entering the command `no gvrp` might cause the switch to reboot unexpectedly with a message similar to `Health Monitor: Restr Mem Access, HW Addr=0x7c7342ae IP=0x3cd640 Task='mGarpCtrl' Task ID=0x5dbf400sp:0x1dc2618 lr:0x3c4bd8 msr: 0x00009032 xer: 0x20000000 cr: 0x48000400`.

Version J.15.09.0024

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`.

File Transfer

CR_0000148584 A configuration file with a blank community name in the `snmp-server host` entry cannot be downloaded to the switch. Although the switch does not allow the `snmp-server host` entry to be configured with a blank community name, earlier software bugs might cause this condition.

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 configuration file is downloaded via TFTP.

Web Management

CR_0000151179 After clicking **Save** without making changes, the Web user interface incorrectly changes VLAN members to be untagged. This happens after selecting **VLAN Mgmt**, clicking **Change**, and then clicking **Save** without making any changes. Also, the VLAN port membership is not correctly displayed in the Web user interface, which is a display issue; the correct VLAN port membership can be seen with the command line interface (CLI).

Version J.15.09.0023

ARP

CR_0000145065 ARP packets sent to a broadcast destination address are forwarded twice by 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.

Version J.15.09.0022

File Transfer

CR_0000113260 Attempts to upgrade software via PCM (ProCurve Manager) fail. Also, actions taken via the Web user interface might experience delayed responses or timeouts.

SSH

CR_0000114000 After rebooting the switch many times, the Operator public key might erroneously be removed from the config file.

CR_0000137266b This removes the CR_0000137266 fix: After rebooting the switch many times, the Operator public key might erroneously be removed from the config file. Instead, this issue is fixed with CR_0000114000.

Version J.15.09.0021

Crash

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

CR_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`.

SSH

CR_0000137266 After rebooting the switch many times, the Operator public key might erroneously be removed from the config file.

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.

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.

Version J.15.09.0020

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.

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.

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.

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.

MAC Authentication

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

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.

CR_0000134672 The `entStateOper` OID from the Entity State MIB gives an incorrect value of `1` (unknown) instead of `3` (enabled), for some switches.

Version J.15.09.0019

Version J.15.09.0019 was never built.

Version J.15.09.0018

Passwords

CR_0000134675 The switch does not automatically create a default username of `manager` or `operator` when a password is configured for those levels of access.

Version J.15.09.0017

LLDP

CR_0000132891 When an IP phone is connected directly to the switch, the output of the command `show lldp info remote-device` gives an incorrect value for the phone's IP address.

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.

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.

Version J.15.09.0016

Version J.15.09.0016 was never built.

Version J.15.09.0015

CLI

CR_0000130897 Existing trap receiver entries might be overwritten by later entries.

GVRP

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

CR_0000130090 After rebooting the switch, the configuration `unknown-vlans disable` does not work on trunks.

Version J.15.09.0014

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`.

CR_0000122568 With SSL enabled, an attempt to download software via the Web interface might cause the switch to reboot unexpectedly with a message similar to: `NMI event SW:IP=0x006d1538 MSR:0x02029200 LR:0x006d19e4, cr: 0x28000800 sp:0x05197088 xer:0x20000000, Task=tHttpd Task ID=0xa955000`.

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.

IGMP

CR_0000127628) In a topology where the host connects to a querier, the querier connects to a non-querier switch, the non-querier switch connects to a router, and the multicast source is beyond the router, the host might not receive the multicast stream. This happens because a join from the host that is received by the querier is not forwarded by the non-querier switch.

CR_0000127974 If a switch receives a PIM packet while it is in the querier election state, the switch gives up the querier role and does not forward multicast traffic.

Multicast

CR_0000125558 Multicast streams sometimes stop after a few minutes. Disabling IGMP restores the multicast stream. Other qualifiers: IP Multicast Route table may still see the stream, and VLAN ingress port may show the stream exists while the same VLAN egress port might not.

Version J.15.09.0013

Crash

CR_0000126799 Under unusual stress conditions, the switch might reboot unexpectedly with a message similar to `Software exception at fileTransfer.c:1144 -- in 'tHttpd', task ID = 0xa9389c0 -> Could not open file`.

CR_0000127541 While providing output for some `show` commands, the switch experiences a gradual loss of free memory. When memory is depleted, the switch might reboot unexpectedly with a message similar to `Software exception at svc_misc.c:831 -- in 'mSess3', task ID = 0x5d9ff40 -> Failed to malloc 16472 bytes`.

Include Credentials

CR_0000127700 With include credentials enabled, a config file that is saved to a TFTP server does not contain the SNMPv3 credentials.

Multicast

CR_0000128222 Frames that use the special LLDP multicast destination address 01:80:c2:00:00:0e are sometimes forwarded. According to IEEE specs, this destination MAC address is reserved to indicate `Nearest Bridge Group` and should not be forwarded.

Web Management

CR_0000125239 After logging into the switch Web user interface, closing the tab on some Web browsers does not log the user out of the Web session.

Version J.15.09.0012

Authentication

CR_0000124607 Disconnecting an authenticated PC from an authenticated VoIP phone might cause the phone to lose its authentication. The phone must be disconnected from and then reconnected to the switch to recover.

MSTP

CR_0000123820 With MSTP enabled and multiple instances configured, LACP is incorrectly blocked on ports connected to MSTP-blocked ports. This issue was fixed on other platforms with CR_0000117473.

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.

Version J.15.09.0011

802.1X

CR_0000122837 Clients have issues with authentication when 802.1X and MAC Authentication are both configured on a port.

Display Issue

CR_0000121028 Some MAC addresses are displayed incorrectly in the output of CLI commands `show lldp info remote-device` and `display lldp neighbor-information list`.

IGMP

CR_0000105902 IGMPv2 LEAVE processing functionality no longer works for a multicast group after receipt of IGMPv1 group specific membership query (GSMQ) packet when operating in IGMPv2 mode, even when `ip igmp forcedfastleave 1-24"` is enabled.

Multicast

CR_0000110677 GMRP Frames should flood to the VLAN just as multicast traffic does, but are not flooding as expected.

SNMP

CR_0000124375 A switch configured to send syslog messages to a server also sends incorrect SNMP traps, causing `unknown trap` messages in the syslog server.

Spanning Tree

CR_0000110052 In a topology with multiple MSTP regions and multiple same-cost links connecting the regions, the CST root port might change to a CST alternate port, and MSTP instances might be blocked on region boundary ports.

SSH

CR_0000122795 SSH session disconnects when the SSH key re-exchange takes place.

TFTP

CR_0000124276 After multiple TFTP file transfers from the switch, additional file transfers might fail with the error message `Translator failed or RFS Error Reboot`.

Version J.15.09.0010

Version J.15.09.0010 was never built.

Version J.15.09.0009

Version J.15.09.0009 was never built.

Version J.15.09.0008

Version J.15.09.0008 was never built.

Version J.15.09.0007

Authentication

CR_0000109782 In some situations the switch stops sending RADIUS requests and client authentication fails.

SNMP

CR_0000119914 Adds the ability to configure port security via SNMP. This was not available in earlier J.15.09 software versions.

TFTP

CR_0000119184 The switch experiences a loss of free memory each time command output is copied to a TFTP server. When memory is no longer available, the TFTP fails with a message similar to `TFTP download in progress. Failed to allocate a new TFTP client. 00000K Request failed`.

Version J.15.09.0006

Version J.15.09.0006 was never built.

Version J.15.09.0005

Crash Messaging

CR_0000114843 The output of an NMI event crash wrongly shows pointer values to be all zeros.

Display Issue

CR_0000118422 A MAC address that begins with a non-zero value is displayed incorrectly in CLI and Web interface output.

MSTP

CR_0000117421 A trunk has the default MSTP port priority = 4. If the trunk is configured with a port priority = 8 (which is the default for non-trunk gigabit ports), after saving the configuration and rebooting the switch, that port priority is wrongly changed to 4.

Port Security

CR_0000114545 With port security enabled, the first packet received on the port is not forwarded by the switch. This can cause DHCP failures for clients who send only one DHCP Discover packet.

Transceivers

CR_0000119781 Mini-GBICs (SFPs) in slots 23 and 24 fail self-test and are incorrectly flagged as unsupported.

Version J.15.09.0004

CLI

CR_0000115515 The switch does not allow configuration changes via the CLI, responding with the error message `inconsistent value`. This has been observed when the configuration includes `snmpv3 targetaddress TARGETADDRESS` with a `TARGETADDRESS` string longer than 24 characters.

Config

CR_0000117518 A switch configured with a username and password and with include-credentials cannot be accessed after updating software, because the username is wrongly removed from the config file during the software update.

Crash

CR_0000115929 With very large key sizes, the command `show crypto host-cert` might cause the switch to reboot unexpectedly with a message similar to the following:

```
Invalid Instr
HW Addr=0x00000000 IP=0x0 Task='mSess2' Task ID=0xa97ad40
sp:0x4acecc8 lr:0x57e468
msr: 0x02029200 xer: 0x20000000 cr: 0x28000400
```

CR_0000116647 It is possible for the switch to reboot unexpectedly with a message similar to `Software exception in kernel context at ghsException.c:1101 -> Internal system error`.

Multicast

CR_0000107597 The switch floods GMRP (GARP Multicast Registration Protocol) packets that are received on Spanning Tree backup and alternate ports, instead of dropping the packets.

SSL

CR_0000115933 Under certain conditions, the **VLAN → VLAN Mgmt** page on the switch cannot be accessed via an SSL connection to the web user interface.

Web Management

CR_0000108339 The switch's web user interface cannot be accessed via the fully-qualified domain name in some situations.

Workaround: Use the IP address to access the switch's web user interface.

Upgrade information

Upgrading restrictions and guidelines

J.15.09.0028 uses BootROM J.14.05. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

Support and other resources

Accessing Hewlett Packard Enterprise Support

- For live assistance, go to the Contact Hewlett Packard Enterprise Worldwide website:

  www.hpe.com/assistance

- To access documentation and support services, go to the Hewlett Packard Enterprise Support Center website:

  www.hpe.com/support/hpesc

Information to collect

- Technical support registration number (if applicable)
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages
- Product-specific reports and logs
- Add-on products or components
- Third-party products or components

Accessing updates

- Some software products provide a mechanism for accessing software updates through the product interface. Review your product documentation to identify the recommended software update method.
- To download product updates, go to either of the following:
  - Hewlett Packard Enterprise Support Center **Get connected with updates** page:

    www.hpe.com/support/e-updates

  - HPE Networking Software:

    www.hpe.com/networking/software

  - To view and update your entitlements, and to link your contracts and warranties with your profile, go to the Hewlett Packard Enterprise Support Center **More Information on Access to Support Materials** page:

    www.hpe.com/support/AccessToSupportMaterials

ⓘ **IMPORTANT:** Access to some updates might require product entitlement when accessed through the Hewlett Packard Enterprise Support Center. You must have an HPE Passport set up with relevant entitlements.

Hewlett Packard Enterprise 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 HPE Support Center - Hewlett Packard Enterprise at **www.hpe.com/support/hpesc**.
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 Hewlett Packard Enterprise Security Bulletin alerts via email, sign up at:

www4.hpe.com/signup_alerts

Documents

To find related documents, see the Hewlett Packard Enterprise Support Center website: **www/hpe.com/support/hpesc**. Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.

Websites

Website	Link
Networking websites	
Hewlett Packard Enterprise Networking Information Library	**www.hpe.com/networking/resourcefinder**
Hewlett Packard Enterprise Networking website	**www.hpe.com/info/networking**
Hewlett Packard Enterprise Networking My Support	**www.hpe.com/networking/support**
General websites	
Hewlett Packard Enterprise Information Library	**www.hpe.com/info/enterprise/docs**
Hewlett Packard Enterprise Support Center	**www.hpe.com/support/hpesc**
Contact Hewlett Packard Enterprise Worldwide	**www.hpe.com/assistance**
Subscription Service/Support Alerts	**www.hpe.com/support/e-updates**
HPE Networking Software	**www.hpe.com/networking/software**
Customer Self Repair (not applicable to all devices)	**www.hpe.com/support/selfrepair**
Insight Remote Support (not applicable to all devices)	**www.hpe.com/info/insightremotesupport/docs**

Customer self repair

Hewlett Packard Enterprise customer self repair (CSR) programs allow you to repair your product. If a CSR part needs to be replaced, it will be shipped directly to you so that you can install it at your convenience. Some parts do not qualify for CSR. Your Hewlett Packard Enterprise authorized service provider will determine whether a repair can be accomplished by CSR.

For more information about CSR, contact your local service provider or go to the CSR website:

www.hpe.com/support/selfrepair

Remote support

Remote support is available with supported devices as part of your warranty or contractual support agreement. It provides intelligent event diagnosis, and automatic, secure submission of hardware event notifications to Hewlett Packard Enterprise, which will initiate a fast and accurate resolution based on your product's service level. Hewlett Packard Enterprise strongly recommends that you register your device for remote support.

For more information and device support details, go to the following website:

www.hpe.com/info/insightremotesupport/docs

Documentation feedback

Hewlett Packard Enterprise 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@hpe.com). When submitting your feedback, include the document title, part number, edition, and publication date located on the front cover of the document. For online help content, include the product name, product version, help edition, and publication date located on the legal notices page.