

K.15.17.0008 Release Notes

Abstract

This document contains supplemental information for the K.15.17.0008 release.



© Copyright 2015 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgments

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

Contents

| | |
|---|----|
| 1 K.15.17.0008 Release Notes..... | 6 |
| Description..... | 6 |
| Important information..... | 6 |
| Version history..... | 6 |
| Products supported..... | 7 |
| Compatibility/interoperability..... | 8 |
| Minimum supported software versions..... | 9 |
| Enhancements..... | 10 |
| Version K.15.17.0008..... | 10 |
| CLI..... | 10 |
| QoS..... | 10 |
| Version K.15.17.0007..... | 10 |
| Version K.15.17.0006..... | 10 |
| Version K.15.17.0005..... | 10 |
| Version K.15.17.0004..... | 10 |
| Configurable TLS..... | 10 |
| Memory..... | 11 |
| show interface command..... | 11 |
| Version K.15.17.0003..... | 11 |
| Concurrent PIM-DM and Distributed Trunking..... | 11 |
| Counters..... | 11 |
| MAC-based Classifier..... | 11 |
| OpenFlow..... | 11 |
| RADIUS..... | 11 |
| TACACS..... | 11 |
| Trust Anchor Certificates..... | 12 |
| v2-v3 module compatibility mode..... | 12 |
| Fixes..... | 12 |
| Version K.15.17.0008..... | 12 |
| Crash..... | 12 |
| Display Issue..... | 12 |
| IPv6..... | 12 |
| OpenFlow..... | 12 |
| OpenFlow Crash..... | 13 |
| OSPF..... | 13 |
| Packet Buffers..... | 13 |
| PIM-SM..... | 13 |
| PoE..... | 13 |
| Routing..... | 13 |
| Spanning Tree..... | 14 |
| TACACS..... | 14 |
| UDP Crash..... | 14 |
| VLAN..... | 14 |
| VRRP..... | 14 |
| Web GUI..... | 15 |
| Version K.15.17.0007..... | 15 |
| File Transfer..... | 15 |
| Version K.15.17.0006..... | 15 |
| CLI..... | 15 |
| Config..... | 15 |
| Crash..... | 15 |

| | |
|-----------------------------|----|
| Display Issue..... | 15 |
| Distributed Trunking..... | 16 |
| Event Log..... | 16 |
| IPv6..... | 16 |
| Link..... | 16 |
| Logging..... | 16 |
| OpenFlow..... | 16 |
| OSPF..... | 16 |
| PIM..... | 16 |
| Routing..... | 17 |
| Security Vulnerability..... | 17 |
| sFlow..... | 17 |
| Stacking..... | 17 |
| Transceivers..... | 17 |
| Version K.15.17.0005..... | 17 |
| SDN | 17 |
| Version K.15.17.0004..... | 17 |
| CLI..... | 17 |
| Counters..... | 17 |
| Crash..... | 18 |
| Logging..... | 18 |
| Module Fault..... | 18 |
| Power..... | 19 |
| TFTP..... | 19 |
| Version K.15.17.0003..... | 19 |
| 10-GbE..... | 19 |
| 802.1X..... | 19 |
| Authentication..... | 19 |
| BGP..... | 19 |
| CLI..... | 19 |
| Command Authorization..... | 20 |
| CPU Utilization..... | 20 |
| Crash..... | 20 |
| Display Issue..... | 21 |
| Distributed Trunking..... | 21 |
| File Transfer..... | 21 |
| ICMP..... | 22 |
| IPv6..... | 22 |
| LLDP..... | 22 |
| Logging..... | 22 |
| Module Fault..... | 22 |
| Multicast..... | 22 |
| Nonstop Switching..... | 22 |
| OpenFlow..... | 23 |
| OSPF..... | 23 |
| PoE..... | 23 |
| Port Connectivity..... | 23 |
| QinQ..... | 23 |
| QoS..... | 23 |
| RADIUS..... | 24 |
| Rate Limiting..... | 24 |
| Routing..... | 24 |
| SNMP..... | 24 |
| SSH..... | 24 |
| SSL..... | 24 |

| | |
|--|----|
| Stacking..... | 25 |
| Switch Hang..... | 25 |
| Switch Initialization..... | 25 |
| Trunking..... | 25 |
| Web Management..... | 25 |
| Issues and workarounds..... | 25 |
| CLI..... | 25 |
| Switch Initialization..... | 25 |
| Upgrade information..... | 26 |
| Upgrading restrictions and guidelines..... | 26 |
| Contacting HP..... | 26 |
| HP security policy..... | 26 |
| Related information..... | 27 |
| Documents..... | 27 |
| Websites..... | 27 |
| Documentation feedback..... | 27 |

1 K.15.17.0008 Release Notes

Description

This release note covers software versions for the K.15.17 branch of the software.

Version K.15.17.0003 was the initial build of Major version K.15.17 software. K.15.17.0003 includes all enhancements and fixes in the K.15.16.0004 software, plus the additional enhancements and fixes in the K.15.17.0003 enhancements and fixes sections of this release note.

Product series supported by this software:

- HP 3500 & 3500 yl Switch Series
- HP 5400 zl & 8200 zl Switch Series
- HP 6200yl Switch Series
- HP 6600 Switch Series

Important information

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

Version history

All released versions are fully supported by HP, unless noted in the table.

| Version number | Release date | Based on | Remarks |
|----------------|--------------|--------------|--|
| K.15.17.0008 | 2015-08-29 | K.15.17.0007 | Released, fully supported, and posted on the web. |
| K.15.17.0007 | 2015-06-22 | K.15.17.0006 | Released, fully supported, and posted on the web. |
| K.15.17.0006 | n/a | K.15.17.0005 | Never released. |
| K.15.17.0005 | 2015-05-11 | K.15.17.0004 | Released, fully supported, but not posted on the web. |
| K.15.17.0004 | 2015-04-23 | K.15.17.0003 | Released, fully supported, but not posted on the web. |
| K.15.17.0003 | n/a | K.15.16.0004 | Never released. |
| K.15.16.0010 | 2015-08-29 | K.15.16.0009 | Please see the K.15.16.0010 release note for detailed information on the K.15.16 branch. Released, fully supported, and posted on the web. |
| K.15.16.0009 | 2015-06-16 | K.15.16.0008 | Released, fully supported, and posted on the web. |
| K.15.16.0008 | 2015-04-17 | K.15.16.0007 | Released, fully supported, and posted on the web. |
| K.15.16.0007 | n/a | K.15.16.0006 | Never released. |
| K.15.16.0006 | 2015-02-06 | K.15.16.0005 | Released, fully supported, and posted on the web. |
| K.15.16.0005 | 2014-11-21 | K.15.16.0004 | Released, fully supported, and posted on the web. |

| Version number | Release date | Based on | Remarks |
|----------------|--------------|--------------|--|
| K.15.16.0004 | 2014-10-30 | K.15.15.0006 | Initial release of K.15.16. Released, but not posted on the web. |
| K.15.15.0014 | 2015-08-29 | K.15.15.0013 | Please see the K.15.15.0014 release note for detailed information on the K.15.15 branch. Released, fully supported, and posted on the web. |
| K.15.15.0013 | 2015-06-16 | K.15.15.0012 | Released, fully supported, and posted on the web. |
| K.15.15.0012 | 2015-04-17 | K.15.15.0011 | Released, fully supported, and posted on the web. |
| K.15.15.0011 | n/a | K.15.15.0010 | Never released. |
| K.15.15.0010 | 2015-02-06 | K.15.15.0009 | Released, fully supported, and posted on the web. |
| K.15.15.0009 | 2015-01-07 | K.15.15.0008 | Released, fully supported, and posted on the web. |
| K.15.15.0008 | 2014-09-15 | K.15.15.0007 | Released, fully supported, and posted on the web. |
| K.15.15.0007 | 2014-06-26 | K.15.15.0006 | Released, fully supported, but not posted on the web. |
| K.15.15.0006 | 2014-03-19 | K.15.14.0002 | Initial release of K.15.15. Released, fully supported, and posted on the web for early availability. |

Products supported

This release applies to the following product models:

| Product number | Description |
|----------------|---|
| J9470A | HP 3500-24 Switch |
| J9471A | HP 3500-24-PoE Switch |
| J9472A | HP 3500-48 Switch |
| J9473A | HP 3500-48-PoE Switch |
| J8692A | HP 3500yl-24G-PWR Intelligent Edge Switch |
| J8693A | HP 3500yl-48G-PWR Intelligent Edge Switch |
| J9310A | HP 3500yl-24G-PoE+ Switch |
| J9311A | HP 3500yl-48G-PoE+ Switch |
| J8697A | HP 5406zl Intelligent Edge Switch |
| J9642A | HP 5406zl Switch with Premium SW |
| J8698A | HP 5412zl Intelligent Edge Switch |
| J9643A | HP 5412 zl Switch with Premium Software |
| J8699A | HP 5406zl-48G Intelligent Edge Switch |
| J8700A | HP 5412zl-96G Intelligent Edge Switch |

| Product number | Description |
|----------------|---|
| J9447A | HP 5406zl-48G-PoE+ Switch |
| J9448A | HP 5412zl-96G-PoE+ Switch |
| J9533A | HP 5406-44G-PoE+/2XG-SFP+ v2 zl Switch |
| J9532A | HP 5412-92G-PoE+/2XG-SFP+ v2 zl Switch |
| J9539A | HP 5406-44G-PoE+/4G-SFP v2 zl Switch |
| J9540A | HP 5412-92G-PoE+/4G-SFP v2 zl Switch |
| J9866A | HP 5406 8p 10GBASE-T 8p 10GbE SFP+ v2 zl Switch with Premium Software |
| J8992A | HP 6200yl-24G-mGBIC Switch |
| J9263A | HP 6600-24G Switch |
| J9264A | HP 6600-24G-4XG Switch |
| J9265A | HP 6600-24XG Switch |
| J9451A | HP 6600-48G Switch |
| J9452A | HP 6600-48G-4XG Switch |
| J9475A | HP 8206zl Switch |
| J9640A | HP 8206 v2 zl Switch with Premium Software |
| J8715A, J8715B | HP 8212zl Switch |
| J9091A | HP 8212zl Switch with fan tray |
| J9641A | HP 8212 v2 zl Switch with Premium Software |
| J9638A | HP 8206-44G-PoE+/2XG v2 zl Switch with Premium Software |
| J9639A | HP 8212-92G-PoE+/2XG v2 zl Switch with Premium Software |

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 |

Minimum supported software versions

NOTE: If your switch or module is not listed in the below table, it runs on all versions of the software.

| Product number | Product name | Minimum software version |
|----------------|--|--------------------------|
| J9546A | HP 8-port 10GBase-T v2 zl Module | K.15.04.0002 |
| J9310A | HP 3500yl-24G-PoE+ Switch | K.15.02.0004 |
| J9311A | HP 3500yl-48-PoE+ Switch | K.15.02.0004 |
| J9312A | HP 2-Port SFP+/2-Port CX4 10GbE yl Module | K.15.02.0004 |
| J9534A | HP 24-port 10/100/1000 PoE+ v2 zl Module | K.15.02.0004 |
| J9535A | HP 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module | K.15.02.0004 |
| J9536A | HP 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl | K.15.02.0004 |
| J9537A | HP 24-port SFP v2 zl Module | K.15.02.0004 |
| J9538A | HP 8-port 10-GbE SFP+ v2 zl Module | K.15.02.0004 |
| J9547A | HP 24-port 10/100 PoE+ v2 zl Module | K.15.02.0004 |
| J9548A | HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module | K.15.02.0004 |
| J9549A | HP 20-port Gig-T / 4-port SFP v2 zl Module | K.15.02.0004 |
| J9550A | HP 24-port Gig-T v2 zl Module | K.15.02.0004 |
| J9637A | HP 12-port Gig-T / 12-port SFP v2 zl Module | K.15.02.0004 |
| J9475A | HP 8206zl Switch Base System | K.14.34 |
| J9307A | HP 24-Port 10/100/1000 PoE+ zl Module | K.14.34 |
| J9308A | HP 20-Port 10/100/1000 PoE+/4-port MiniGBIC zl Module | K.14.34 |
| J9478A | HP 24-port 10/100 PoE+ zl Module | K.14.34 |
| J9447A | HP 5406zl-48G-PoE+ Switch | K.14.34 |
| J9448A | HP 5412zl-96G-PoE+ Switch | K.14.34 |
| J9470A | HP 3500-24 Switch | K.14.31 |
| J9471A | HP 3500-24-PoE Switch | K.14.31 |
| J9472A | HP 3500-48 Switch | K.14.31 |
| J9473A | HP 3500-48-PoE Switch | K.14.31 |
| J9451A | HP Switch 6600-48G | K.14.24 |
| J9452A | HP Switch 6600-48G-4XG | K.14.24 |
| J9263A | HP Switch 6600-24G | K.14.03 |
| J9264A | HP Switch 6600-24G-4XG | K.14.03 |
| J9265A | HP Switch 6600-24XG | K.14.03 |
| J9154A | HP ONE Services zl Module | K.13.51 |
| J9051A, J9052A | HP Wireless Edge Services zl Module, HP Redundant Wireless Services zl Module | K.12.43 |
| J8715A, J8715B | HP Switch 8212zl Base System | K.12.31 |

| Product number | Product name | Minimum software version |
|----------------|---|--------------------------|
| J8993A, J8994A | Premium Features on Series 3500yl and 5400zl Switches | K.11.33 |
| J8706A | HP Switch 5400zl 24p Mini-GBIC Module | K.11.33 |
| J8708A | HP Switch 5400zl 4p 10-GbE CX4 Module | K.11.33 |
| J8992A | HP Switch 6200yl-24G-mGBIC | K.11.33 |
| J8694A | HP Switch 3500yl 2p 10GbE X2 + 2p CX4 Module | K.11.17 |

Enhancements

This section lists enhancements found in the K.15.17 branch of the software. Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

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

Version K.15.17.0008

CLI

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

QoS

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

Version K.15.17.0007

No enhancements are included in version K.15.17.0007.

Version K.15.17.0006

No enhancements were included in version K.15.17.0006.

Version K.15.17.0005

No enhancements were included in version K.15.17.0005.

Version K.15.17.0004

Configurable TLS

CR_0000160085 Configurable TLS version and enforcing the use of a specific cipher suite.

The National Institute of Standard and Technology (NIST) has provided requirements for the use of TLS in Special Publication 800-52. These requirements state that a minimum version of TLS must be enforced, as well as the use of specific cipher suites. In order to meet these requirements, the software has been modified to support enforcing minimum versions of TLS and specify which cipher suites are to be used.

As a TLS client, the switch will advertise the configured preferences for the TLS version and cipher suite to the server. If the server does not support the cipher suite or negotiates a lower TLS version, the connection between client and server will be terminated. As an HTTPS server, the switch will check the TLS version and cipher suite advertised by the client. Should it detect a mismatch with the configured TS version or cipher suite for the application, the connection will be terminated.

The following new CLI command has been implemented in order to configure the minimum TS version and cipher suite:

```
[no] tls application { web-ssl | openflow | syslog | tr69 | all }  
lowest-version { tls1.0 | tls 1.1 | tls 1.2 | default }  
  
cipher { aes256-sha256 | aes256-sha | aes128-sha256 | aes128-sha |  
des3-cbc-sha | ecdh-rsa-aes128-gcm-sha256 }
```

The MIB HP-ICF-TLS-MIN-MIB (OID string: 1.3.6.1.4.1.11.2.14.11.5.1.112) has been implemented to provide support for the feature via SNMP.

Memory

Enhancements were made to optimize memory usage.

show interface command

CR_0000166947 The option `smartrate` was added to the `show interface [<PORT-LIST>]` command. This option is used to display port diagnostics on a Smart Rate port only. If the command is run on a non-Smart Rate port, a message similar to the following displays: Port A1: This command is only applicable to Smart Rate ports. Syntax: `show interface [<PORT-LIST>] smartrate`.

Version K.15.17.0003

Concurrent PIM-DM and Distributed Trunking

Allows a switch that is part of Distributed Trunking to support PIM Dense Mode concurrently. For more information, see the *Multicast and Routing Guide*.

Counters

Per queue counters provide visibility into the performance of the egress queue for diagnostics and monitoring of QoS implementation. For more information, see the *HP Switch Software Advanced Traffic Management Guide*.

MAC-based Classifier

This feature allows policies such as QoS and ACL to be based on MAC address in addition to the existing capability with IP address. For more information, please see the *HP Switch Software Advanced Traffic Management Guide*.

OpenFlow

Fully-flexible OpenFlow allows the switch to create resources such as matching tables, ACL, and so forth, to support requirements of SDN applications; only on v3 modules. For more information, see the *HP OpenFlow 1.3 Administrator Guide*.

Multi-VLAN per OpenFlow instance allows multiple VLANs to be supported in one OpenFlow instance. For more information, see the *HP OpenFlow 1.3 Administrator Guide*.

RADIUS

RADIUS filter-id allows RADIUS to better support IMC policy interoperability. For more information, see the *HP Switch Software Access Security Guide*.

TACACS

Addition of accounting to the existing TACACS+ authentication capability. For more information, see the *HP Switch Software Access Security Guide*.

Trust Anchor Certificates

CR_0000156165 Basic Constraint Extension `pathlenConstraint` support added to Certificate Manager. In software versions 15.14 and later, support was added for Trust Anchor (TA) certificates, which allow a user to sign intermediate Trust Anchor certificates or an end entity certificate. In section 4.2.1.9, RFC 5820 defines a Basic Constraint Extension named `pathlenConstraint` as the field that defines "...the maximum number of non-self-issued intermediate certificates that may follow this certificate in a valid certification path. ...A `pathlenConstraint` of zero indicates that no non-self-issued intermediate CA certificates may follow in a valid certification path. Where it appears, the `pathlenConstraint` field MUST be greater than or equal to zero. Where `pathlenConstraint` does not appear, no limit is imposed." Support for the `pathlenConstraint` has been added to the software. It can be set to the maximum value of 3 because the software supports up to 3 intermediate certificates. When it is set to 0, it can only sign an end entity certificate and not another intermediate certificate.

v2-v3 module compatibility mode

Allows a mix of v2 and v3 modules to function in the same 5400R chassis. Most of the features that are supported only in v3 modules do not work in compatibility mode. For more information, see the *Management and Configuration Guide*.

Fixes

This section lists released builds that include fixes. Software fixes are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all fixes added in earlier versions.

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

Version K.15.17.0008

Crash

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

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

Display Issue

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

IPv6

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

OpenFlow

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

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

OpenFlow Crash

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

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

OSPF

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

Packet Buffers

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

PIM-SM

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

PoE

CR_0000169265 After an electrical surge or ESD charge on a PoE port, the switch might exhibit BAD FET messages, which indicate a failure to deliver PoE on those ports. Event log messages appear similar to the following: .

`W 04/02/15 07:58:49 02562 ports: Port 1/1: Possible bad FET/PSE supplying PoE power - suggest configuring other end of link with "no power"`

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

Routing

CR_0000174012 Applying BPG route-map with `set weight` while there is more than one path could result in switch crash with a message similar to `Software exception at bgp_med.c:597 -- in 'eRouteCtrl'.`

Workaround: The failure may be avoided by applying BPG route-map with `set local-pref` instead of using `set weight`.

CR_0000174881, CR_0000176140 The switch does not initiate an ARP request to the next hop IPv4 address for routed IPv4 traffic entering a VLAN that has a Routed Access List (RACL) applied using the commands `vlan vid ip access-group identifier in` or `vlan vid ip access-group identifier out`. As a result, the IPv4 routed traffic does not reach its destination because the switch does not create an ARP entry in the switch ARP Table for the next hop IPv4 address, which is required to route the traffic. The issue may be intermittent because there could be other sources trying to reach the same next hop IPv4 address which will result in creating an ARP entry. Due to the ARP age-out time of 20 minutes, the issue may reoccur after 20 minutes. For example, if the routed IPv4 traffic also enters the switch via a VLAN that does not have RACL or if you ping it from the affected switch. Pinging from the switch to the unreachable IPv4 destination address temporarily resolves the reachability issue; however, the issue may reoccur after the APR

age-out expire or after invoking the CLI command `clear arp`. Example of an IPv4 inbound RACL configuration that could encounter this issue for packets routed through the switch:

```
ip access-list extended "102"
 10 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
 exit
ip routing
ip route 0.0.0.0 0.0.0.0 192.168.0.1 vlan 10
 name "VLAN10"
 untagged A1
 ip access-group "102" in
 ip address 10.0.0.1 255.255.255.0
 exit
vlan 20
 name "VLAN20"
 untagged A2
 ip address 192.168.0.100 255.255.255.0
 exit
```

Example of an IPv4 ourbound RACL configuration that could encounter this issue for packets routed through the switch:

```
ip access-list extended "102"
 10 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
 exit
ip routing
ip route 0.0.0.0 0.0.0.0 192.168.0.1
vlan 10
 name "VLAN10"
 untagged A1
 ip address 10.0.0.1 255.255.255.0
 exit
vlan 20
 name "VLAN20"
 untagged A2
 ip access-group "102" out
 ip address 192.168.0.100 255.255.255.0
 exit
```

Spanning Tree

CR_0000167601 In a spanning tree environment during BPDU storms, the switch may fail and require a manual reboot.

TACACS

CR_0000177904 If more than one TACACS servers are configured as authentication method and all TACACS servers become unreachable, failover to secondary authentication does not occur. When this event occurs, one will not be able to login to the switch using the same access method.

UDP Crash

CR_0000172405 When UDP broadcast traffic is sent to a switch with UDP forwarder configured, an unexpected reboot (crash) occurs with a message similar to Software exception at `alloc_free.c:825 -- in 'mUDPFctrl', task ID = 0x1deb0800 -> buf already freed by 0x1DEB0800, op=0x00160002Buffer:`

VLAN

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

VRRP

CR_0000169624 VRRP virtual ping fails in a QinQ mixed-mode configuration.

Web GUI

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

Version K.15.17.0007

File Transfer

CR_0000172816 The switch might reboot unexpectedly (crash) after using TFTP/SFTP file transfer to download software if the switch is not rebooted immediately afterwards. Workaround: reboot after every TFTP/SFTP download.

Version K.15.17.0006

CLI

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

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

Config

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

Crash

CR_0000151697 The 10G slot of the 6600/3500 unexpectedly reboots right after the log message: `Slot A: Lost Communications detected - Heart Beat Lost(01)`, causing an interrupt of 30 seconds. Occurs when there is a 10G module installed in a 3500/6600 switch.

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

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

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

Display Issue

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

Distributed Trunking

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

Event Log

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

IPv6

CR_0000164057 IPv6 counters are displayed very slowly while executing the `show ip counters` command. Workaround: Add the interface – example `show ip counters vlan X` returns display information at normal speed.

Link

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

Logging

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

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

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

OpenFlow

CR_0000170635 On the CLI, typing `openflow <tab>` shows the valid parameters and descriptions. The optional parameter `ip-control-table-mode` help text has been corrected to read Include IP control table in the OpenFlow packet processing pipeline. [Deprecated]. Please see `'openflow instance <INSTANCE-NAME> pipeline-model`.

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

OSPF

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

PIM

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

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

Routing

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

CR_0000162176 Under stress conditions, the switch sometimes enters a state where it does not send an ARP to a particular destination and it becomes unreachable on the customer network. Workaround/Proof of issue: Initiate a ping from the switch to the unreachable destination to restore connectivity to that destination through this switch.

Security Vulnerability

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

sFlow

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

Stacking

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

Transceivers

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

Version K.15.17.0005

SDN

CR_0000171571 Heartbeat packets between Network Protector and switch are being malformed by the switch. This causes the Network Protector application to think the tunnel connection between the controller and switch is invalid.

Version K.15.17.0004

CLI

CR_0000167157 The 2910al CLI command `show interface transceiver detail` indicates the wrong value for the maximum allowed distance for the J4858C X121 1G SFP LC SX transceiver.

Counters

CR_0000166949 The `show interfaces <port-list> hc` command does not display 64-bit counter values properly.

Crash

CR_0000155066 The switch may reboot unexpectedly with a Software Exception message similar to: Software exception at stackingFile.c:2224 -- in 'mStackDatWriter', task ID = 0x3c953b00 -> Internal Error ID: 6382d706) when a lot of TFTP file transfers to an external TFTP server have occurred.

CR_0000162155 Configuring an OpenFlow instance using secure mode, enabling OpenFlow, and then configuring the lowest-version for OpenFlow may cause the switch to reboot unexpectedly. Other triggers include updating the tls lowest-version for an app for which a cipher is already configured, and executing the no tls app <app> lowest-version <ver> cipher CLI command. The crash message references a mem-watch trigger.

CR_0000162400 When the switch continuously attempts to transfer a file to a destination that returns an error, for example because it ran out of space to store the file, the switch might eventually crash with the following message: Software exception at hwBp.c:218 -- in 'fault_handler', task ID = 0x3c403380 -> MemWatch Trigger: Offending task 'mftTask'.

CR_0000166245 An assert failure (crash) occurs during redundancy switchover when PIM Dense mode is disabled from a VLAN prior to the redundancy switchover.

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

CR_0000167603 After issuing the command `crypto key generate auto-run`, the system requires time to generate the key-pair. When the software is still busy processing the task and the command `crypto key generate ssh` is entered, the switch crashes with the following message: Software exception at rsa_key_generator.c:750 -- in 'mSess1', task ID = 0xa99c9c0 -> rsa key creation.

CR_0000167916 Within the same uptime/boot period, if DHCP is enabled/disabled multiple times, the following symptoms could be seen:

- Crash
- File transfer failure
- Loss of IP communication

CR_0000169054 Blade fails to boot after repeatedly inserting and removing it. This might cause a system crash with the failure message `Unable to initialize Fabric ASIC`.

CR_0000169893 Crash occurs when a user attempts to replace an ACL or QoS policy on multiple ports if an ACL or policy is already applied to some of the ports, but not all of them, where the new ACL or policy is being applied.

CR_0000169920 Using the `copy support-log` command on rare occasions might cause the switch to crash with unexpected crash messages.

Logging

CR_0000167753 When trying to apply the command `logging system-module acct`, the switch sends the error message: `C1-3500(config)# logging system-module acct Invalid value`.

Module Fault

CR_0000168875 Occasionally, a blade or slot may fail to boot on first try or may crash immediately before finalizing the boot process. The failed blade/slot would recover and reboot automatically by software.

Power

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

TFTP

CR_0000159058 When the switch is used as TFTP server and configuration files are transferred from the switch to an external TFTP client, the software creates a temporary file in memory that is removed after the transfer has completed. However, the temporary file is not deleted when an error occurs during the file transfer. When repeated transfers of configuration files fail, the temporary files accumulate and might deplete the available memory space. Once depleted, further file transfers fail and the switch might reboot unexpectedly (crash). Note that when the switch is rebooted, all temporary files are removed from memory.

Version K.15.17.0003

10-GbE

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

802.1X

CR_0000149780 The fix in CR 0000133762 causes Microsoft's Roaming User Profile feature to fail to work properly.

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

Authentication

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

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_0000145136 When the switch is configured with the console event critical setting, the event log output of show tech all lists only the critical events. With this fix, show tech all lists all event log entries.

CR_0000154706 When a user configures a blackhole route for an IPv4 or IPv6 address and then attempts to configure that same IP address as a VRRP virtual IP address, the invalid configuration is rejected with the error message Cannot configure a reject/blackhole route as backup virtual-ip-address. When the configuration order is reversed by first configuring the IP address as VRRP virtual IP address and then the blackhole route, the configuration is incorrectly permitted by the configuration parser.

CR_0000156237 When a user has enabled Spanning Tree in the CLI and configured a protocol version other than the default MSTP, the CLI Menu does not allow the user to modify Spanning Tree parameters. The menu indicates that the switch requires a reboot. When the switch is actually rebooted the same problem is present after the reboot.

CR_0000161668 After a user has changed the Spanning Tree Protocol Version to RPVST in the CLI Menu, the switch prompts the user to save the configuration and reboot the system to activate the changes. However, after saving and rebooting, those messages continue to be displayed.

Command Authorization

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

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

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

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

CPU Utilization

CR_0000151164 The switch occasionally reports CPU utilization of 99%. This is a false reading and does not affect switch performance.

CR_0000153428 With high volumes of routed IPv6 traffic, switch CPU utilization might remain at high levels for long periods of time. This issue is most prevalent with v1 zl modules.

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`.

CR_0000142381 When the BGP configuration includes a non-default weight and the `redistribute connected` command, 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 'eRouteCtrl'. Offending IP=0xedde38`. This issue was introduced with CR_0000138230.

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`.

CR_0000146176 After receiving multiple route changes or route flaps in a short period of time, the switch might reboot unexpectedly with a message similar to Software exception at `krt.c:2134 -- in 'eRouteCtrl', task ID = 0xa9bc400 -> Routing Stack: Assert Failed`.

CR_0000149153 When an exceptionally large amount of IP Address Manager (IPAM) output is generated by the output of `show tech all` and captured using the `copy command-output CLI` command, the system might crash with the following message: NMI event
SW:IP=0x00147168 MSR:0x02029200 LR:0x00120f7c cr: 0x44000400
sp:0x04d60f30 xer:0x00000000 Task='mSess3' Task ID=0x4d59728.

CR_0000151102 In a rare situation, after a failover to the Standby Management Module (SMM) or the stack's Standby switch, the switch might reboot unexpectedly with a message similar to Software exception at `asicMgrSlaveFilters.c:185 -- in 'mNSA', task ID = 0x1b1fea80 -> Internal Name Server Error`.

CR_0000153386 When a large number of 802.1X clients is being authenticated, reconfiguring port security modes such as **learn-mode** might cause the switch to reboot unexpectedly with a message similar to Software exception at multMgmtUtil.c:88 -- in 'mPpmgrCtrl', task ID = 0x13b1f940 -> Internal error.

CR_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.

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 these commands causes the switch to reboot unexpectedly with a message similar to Health Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x017cb590 IP=0x17cb590 Task='eRouteCtrl' Task ID=0xa96de00 sp:0x48cea20 lr:0x10086d4 msr: 0x02029200 xer: 0x20000000 cr: 0x44000400.

CR_0000154769 The switch may reboot unexpectedly when the management interface is accessed via SSH and the `show tech all` CLI command is executed, or when the SSH session is idle following execution of the CLI command `show run` a few minutes earlier.

CR_0000159125 When a system has Distributed Trunking enabled, a crash might occur when a packet with an incorrect flag is received on the ISC port. Instead of dropping the packet, the software attempts to process the packet, which triggers a crash similar to the following: Health Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x0065d2f8 IP=0x65d2f8 Task='tDevPollTx' Task ID=0xa9f9700 sp:0x2ecc828 lr:0x6081c0 msr: 0x02029200 xer: 0x20000000 cr: 0x48000800.

CR_0000159764 Due to a semaphore deadlock with an unknown trigger, a switch may crash with a message similar to the following: NMI event HW:IP=0x0151dec4 MSR:0x02029200 LR:0x0151e468 cr: 0x20000800 sp:0x02f01460 xer:0x20000000 Task='tDevPollRx' Task ID=0xaa28000.

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

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`.

Distributed Trunking

CR_0000151202 When IGMP hosts are connected to switches configured for Distributed Trunking and these switches are interconnected via the ISC, IGMP joins from these hosts might fail to pull in the multicast streams on which the hosts are joined.

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.

ICMP

CR_0000155702 The switch sends a ping request to a random IP address every 20 minutes.

IPv6

CR_0000140467 The switch does not generate an event log message when IPv6 Neighbor Discovery (ND) detects a duplicate address.

LLDP

CR_0000157298 When a PD sends an LLDP-MED TLV to a switch port in which the PD uses the invalid value of 0 Watts, the switch software actually applies the invalid 0 Watts. This causes the PD to reboot every time it transmits the 0 Watts in the TLV. The switch might log over-current warnings (00562 ports: port <port ID> PD Overcurrent indication) because the PD is already drawing power over the port when the software applies 0 Watts power. The value of 0 Watts in the TLV is henceforth be rejected with the error Invalid power value 0 deciWatts received from MED PD on port <port ID>.

Logging

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

Module Fault

CR_0000149727 When a chassis is rebooted, one or more modules may not be correctly initialized and suffer from an HSL Fatal error. When the problem occurs, Event Log messages such as the following will be logged:

```
00375 chassis: Slot J Downloading
00376 chassis: Slot J Download Complete
00374 chassis: Slot J Failed to boot-timeout- (AGENT_FAILED)
00375 chassis: Slot J Downloading
00376 chassis: Slot J Download Complete
00274 chassis: Slot J HSL0 Fatal ff8003f2: Task=eDevIdle Task
ID=0x1b1fe6c0 IP=0x1c5cd88
```

The same module may require multiple initialization attempts before it is properly booted up. Once the initialization of the affected module has succeeded, the module operates normally.

Multicast

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

Nonstop Switching

CR_0000133990 After a management module failover of an 8200zl switch configured for Nonstop switching, one or more of the following issues might be observed:

- The output of `show system fans` displays Fan Failed for all fans.
- The output of `show system power-supply` displays Not Present for all power supply slots.
- The output of `walkmib hpicfsensortable` displays `hpicfSensorIndex.0 = 0` repeatedly.
- Pressing the **LED Mode** button has no effect (the mode selection does not change).

OpenFlow

- CR_0000151412** Following creation of a meter for OpenFlow, meter statistics for `duration_sec` and `duration_nsec` return incorrect values.
- CR_0000151415** Querying the statistics of a port that is a member of an OpenFlow instance returns incorrect values for `duration_sec` and `duration_nsec`.
- CR_0000163370** Violation of OpenFlow requirement that if the match field `OXM_OF_IP_DSCP` is used the `ETH TYPE` must be `0x0800` or `0x86dd`.

OSPF

- CR_0000137616** When the switch is configured as an OSPF neighbor, and the neighbor changes time, OSPF adjacency temporarily drops.
- CR_0000151661** The local switch interface IP address becomes unreachable after the switch receives injected RIP/OSPF/Static Route with ECMP routes. This is triggered by ECMP routes with subnet x , and same connected route with subnet $y = x + 1$.
- CR_0000155308** When a large number of routes (on the order of 9000) are updated with a better path, the better paths are not always put into the routing table, which can cause unreachable subnets.
- CR_0000155425** When a high volume of Link State Acknowledgements are flooded to an OSPFv2 neighbor, the adjacency might go down because OSPF Hello packets are dropped.
- CR_0000160814** When a user reconfigures an OSPFv3 area from stub or normal to NSSA without rebooting the router or restarting the OSPFv3 protocol, the ASBR status is not updated on the OSPFv3 router when it becomes an NSSA ABR. Likewise, when the area is reconfigured from NSSA to stub or normal, the ASBR status is also not updated and the router continues to act as if it is still an ASBR.
- Due to the incorrect ASBR status, the route advertisements are not correct, which results in routes being installed on routers in an area when they should not be or routes not being advertised when they should have been.

PoE

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

Port Connectivity

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

QinQ

- CR_0000156812** A switch configured for **qinq mixedvlan** mode does not allow an untagged port to be removed from a C-VLAN and placed in an S-VLAN.

QoS

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

RADIUS

CR_0000149657 Configuration of multiple RADIUS servers via SNMP fails if a 'create and wait' mechanism is used.

Rate Limiting

CR_0000148906 Enabling outbound rate limiting on port causes adjacency loss and prevents OSPF hello's from being transmitted. If the rate-limit is removed the switch forms adjacencies again.

Routing

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

CR_0000160655 Switches configured for routing: When a VACL is applied to VLAN X, if a host on VLAN X then pings the switch agent's IP address for VLAN Y, the agent's response IP address is also applied to the VACL, and hosts become unreachable.

SNMP

CR_0000146616 OSPFv3 traps are not sent by the switch.

CR_0000151035 When an SNMP read/query (for example, using iMC or the CLI command `walkMib` or `getMib`) to the SNMP MIB ID: `entPhysicalIsFRU` is directed at a Fan Tray or SFP device, the 3800 series switches do not correctly report that they are Assets and are removable.

CR_0000154463 The 3800 is not sending the correct FRU and Physical Asset status to iMCv7 via SNMP when the SFP (J4858C) is installed in SFP ports 51 or 52. The iMC software is reporting `FRU=No`; `Physical` and `Physical Asset=No`. This improves the original SNMP fix (CR_0000151035).

CR_0000156209 When a configuration file is downloaded to the switch in which the SNMP community name string for unrestricted access is something other than `unrestricted`, the software resets the access-level to the default `restricted`. Although it is expected behavior to default to `restricted` when the string `unrestricted` is not precisely matched, the software has been modified to allow the use of both lower and upper-case characters in the word `unrestricted` when parsing a downloaded configuration file.

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

CR_0000160532 The string value for the temperature sensor's instance of the object `entPhysicalName` (.1.3.6.1.2.1.47.1.1.1.7) is incorrectly set to `Chassis`. It should return `Chassis Temperature`.

SSH

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

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

SSL

CR_0000162587 SSL Security vulnerability due to 56-bit DES-CBC-SHA. Due to security vulnerability, the cipher DES-CBC-SHA is now unavailable.

Stacking

CR_0000152463, CR_0000152757 After updating Management Stack Members to some versions of X.15.08.0001 or newer software, the Member switches mistakenly displays additional two configuration lines of SNMPv3 configuration in the running-config if snmp-server host is configured on the Commander.

CR_0000154380 A failover from Commander to Standby with multiple MSTP instances in operation might cause the stack members and connected devices to be unreachable.

Switch Hang

CR_0000153460 If a switch receives a VRRP packet after the invocation of the CLI command boot system flash primary, the switch might become unresponsive and the reboot will not complete without intervention.

CR_0000154152 If there is an active console session providing output at the time of reboot, the switch might become unresponsive and not complete the reboot without further intervention.

Switch Initialization

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

Trunking

CR_0000165004 If DT trunking keep-alive has been configured, and later the switch is rebooted, the ISC link between the DT pair becomes unstable, or goes down. Symptoms include blocked traffic, layer 2 loops, or duplicate packets. A temporary workaround for this issue is to reconfigure the DT keep-alive (but not reboot).

Web Management

CR_0000149777 After a 3800 series switch Stack Commander failover, the Web-management interface is not accessible via the Out of Band Management (OOBM) port.

CR_0000160654 When 51 or more VLANs are configured on the switch, the web interface does not display any VLAN under the **VLAN Management** and **Multicast IGMP** tabs.

Issues and workarounds

CLI

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

Workaround: Use the `lldp config PORT-LIST dot3TlvEnable poe_config` command syntax.

Switch Initialization

CR_0000169998 A port becomes an untagged member in more than one VLAN when the changes to the port's tagged/untagged VLAN membership are made in the CLI Menu.

Workaround: Reset the switch, reset the module, or power cycle the switch.

Upgrade information

Upgrading restrictions and guidelines

K.15.17.0008 uses BootROM K.15.30. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

For more information about BootROM, see the *HP Switch Software Management and Configuration Guide* for your switch.

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

Table 1 BootROM updates

| If your software version is: | Your next step should be: |
|---|--|
| K.11.11 through K.12.29 (BootROM K.11.00 - K.11.03) | Update and reload into software version K.12.31 or K.12.62 |
| K.12.31 through K.13.55 (BootROM K.12.12 - K.12.14) | Update and reload into software version K.13.58 or K.13.68 |
| K.13.58 or newer (BootROM K.12.17 or newer; use <code>show flash</code> command) | Update directly into software version K.15.17.0008 (BootROM K.15.30) |

Contacting HP

For additional information or assistance, contact HP Networking Support:

www.hp.com/networking/support

Before contacting HP, collect the following information:

- Product model names and numbers
- Technical support registration number (if applicable)
- Product serial numbers
- Error messages
- Operating system type and revision level
- Detailed questions

HP security policy

A Security Bulletin is the first published notification of security vulnerabilities and is the only communication vehicle for security vulnerabilities.

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.
- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

To find security bulletins:

1. Go to the HP Support Center website at www.hp.com/go/hpsc.
2. Enter your product name or number and click **Go**.
3. Select your product from the list of results.
4. Click the **Top issues & solutions** tab.
5. Click the **Advisories, bulletins & notices** link.

To initiate a subscription to receive future HP Security Bulletin alerts via email, sign up at:
www4.hp.com/signup_alerts

Related information

Documents

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

www.hp.com/support/manuals

- Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.
- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Related documents

The following documents provide related information:

- *HP Switch Software Access Security Guide K/KA/KB.15.17*
- *HP Switch Software Advanced Traffic Management Guide K/KA/KB.15.17*
- *HP Switch Software Basic Operation Guide*
- *HP Switch Software IPv6 Configuration Guide K/KA/KB.15.17*
- *HP Switch Software Management and Configuration Guide K/KA/KB.15.17*
- *HP Switch Software Multicast and Routing Guide K/KA/KB.15.17*

Websites

- Official HP Home page: www.hp.com
- HP Networking: www.hp.com/go/networking
- HP product manuals: www.hp.com/support/manuals
- HP download drivers and software: www.hp.com/networking/software
- HP software depot: www.software.hp.com
- HP education services: www.hp.com/learn

Documentation feedback

HP is committed to providing documentation that meets your needs. To help us improve the documentation, send any errors, suggestions, or comments to Documentation Feedback (docsfeedback@hp.com). Include the document title and part number, version number, or the URL when submitting your feedback.