



Hewlett Packard
Enterprise

WB.15.17.0013 Release Notes

Abstract

This document contains supplemental information for the WB.15.17.0013 release.

Part Number: 5200-1301
Published: June 2016
Edition: 1

© Copyright 2016 Hewlett Packard Enterprise Development LP

The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise 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. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein.

Confidential computer software. Valid license from Hewlett Packard Enterprise 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.

Links to third-party websites take you outside the Hewlett Packard Enterprise website. Hewlett Packard Enterprise has no control over and is not responsible for information outside the Hewlett Packard Enterprise website.

Acknowledgments

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

Contents

1 WB.15.17.0013 Release Notes.....	7
Description.....	7
Important information.....	7
Version history.....	7
Products supported.....	8
Compatibility/interoperability.....	9
Minimum supported software versions.....	9
Enhancements.....	10
Version WB.15.17.0013.....	10
Version WB.15.17.0012.....	10
Version WB.15.17.0011.....	10
Version WB.15.17.0010.....	10
Version WB.15.17.0009.....	10
Instrumentation Monitor.....	10
Version WB.15.17.0008.....	10
CLI.....	10
QoS.....	10
Version WB.15.17.0007.....	10
Version WB.15.17.0006.....	10
Version WB.15.17.0005.....	10
Version WB.15.17.0004.....	10
Configurable TLS.....	10
Memory.....	11
show interface command.....	11
Version WB.15.17.0003.....	11
Counters.....	11
DLDP.....	11
OpenFlow.....	11
RADIUS.....	12
TACACS.....	12
Trust Anchor Certificates.....	12
Fixes.....	13
Version WB.15.17.0013.....	13
Event Log.....	13
File Transfer.....	13
Menu.....	13
OOBM.....	13
SNMP.....	13
Spanning Tree.....	14
Trunking.....	14
VLAN.....	14
Version WB.15.17.0012.....	14
Banner.....	14
CLI.....	14
Console.....	15
Counters.....	15
DHCP.....	15
DHCP Snooping.....	15
IGMP.....	15
IPv6.....	16
PoE.....	16
Policies.....	16

Smart Link.....	16
Supportability.....	16
Syslog.....	16
Version WB.15.17.0011.....	17
Version WB.15.17.0010.....	17
ACLs.....	17
CLI.....	17
DHCP Snooping.....	17
OpenFlow.....	17
PIM.....	18
Port Counters.....	18
QinQ.....	18
RIP.....	18
TFTP.....	18
Version WB.15.17.0009.....	19
BPDU Protection.....	19
Certificate Manager.....	19
CLI.....	19
Crash.....	19
DHCP.....	19
DHCP Snooping.....	19
File Transfer.....	20
IGMP.....	20
Logging.....	20
MAC Authentication.....	20
Menu Interface.....	20
MLD.....	20
OpenFlow.....	20
PBR.....	20
PoE.....	20
Policy Based Routing.....	21
Port Security.....	21
QoS.....	21
RADIUS.....	21
RA-guard.....	21
Rate Limiting.....	21
RMON.....	22
SNMP.....	22
Stacking.....	22
Supportability.....	22
Switch Initialization.....	22
TFTP.....	22
VLAN.....	22
Version WB.15.17.0008.....	22
Crash.....	22
Display Issue.....	22
IPv6.....	23
OpenFlow.....	23
OpenFlow Crash.....	23
PoE.....	23
Routing.....	23
TACACS.....	24
UDP Crash.....	24
VLAN.....	24
Web GUI.....	24

Version WB.15.17.0007.....	24
CLI.....	24
File Transfer.....	25
Version WB.15.17.0006.....	25
CLI.....	25
Config.....	25
Crash.....	25
Display Issue.....	25
Event Log.....	25
Link.....	25
Logging.....	25
OpenFlow.....	26
PIM.....	26
Routing.....	26
Security Vulnerability.....	26
sFlow.....	26
Stacking.....	26
Transceivers.....	26
Version WB.15.17.0005.....	26
SDN	26
Version WB.15.17.0004.....	27
CLI.....	27
Config.....	27
Counters.....	27
Crash.....	27
Logging.....	28
OOBM.....	28
Stacking.....	28
TFTP.....	28
Version WB.15.17.0003.....	28
802.1X.....	28
Authentication.....	28
CLI.....	28
Command Authorization.....	29
Config.....	29
CPU Utilization.....	29
Crash.....	29
Crash Messaging.....	30
Display Issue.....	30
File Transfer.....	30
ICMP.....	30
IPv6.....	30
LLDP.....	30
Logging.....	30
Multicast.....	30
OOBM.....	30
OpenFlow.....	31
PoE.....	31
Port Connectivity.....	31
QoS.....	31
RADIUS.....	31
Routing.....	31
SNMP.....	31
SSH.....	31
SSL.....	32

Stacking.....	32
Switch Hang.....	32
Trunking.....	32
Web Management.....	32
Issues and workarounds.....	33
Certificate Manager.....	33
PoE.....	33
SNMP.....	33
Upgrade information.....	33
Upgrading restrictions and guidelines.....	33
Support and other resources.....	33
Accessing Hewlett Packard Enterprise Support.....	33
Accessing updates.....	34
Hewlett Packard Enterprise security policy.....	34
Documents.....	35
Websites.....	35
Customer self repair.....	35
Remote support.....	36
Documentation feedback.....	36

1 WB.15.17.0013 Release Notes

Description

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

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

Product series supported by this software:

- Aruba 2920 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 Hewlett Packard Enterprise, unless noted in the table.

Version number	Release date	Based on	Remarks
WB.15.17.0013	2016-05-25	WB.15.17.0012	Released, fully supported, and posted on the web.
WB.15.17.0012	2016-03-28	WB.15.17.0011	Released, fully supported, and posted on the web.
WB.15.17.0011	n/a	WB.15.17.0010	Never released.
WB.15.17.0010	2016-01-19	WB.15.17.0009	Released, fully supported, and posted on the web.
WB.15.17.0009	2015-11-10	WB.15.17.0008	Released, fully supported, and posted on the web.
WB.15.17.0008	2015-08-29	WB.15.17.0007	Released, fully supported, and posted on the web.
WB.15.17.0007	2015-06-22	WB.15.17.0006	Released, fully supported, and posted on the web.
WB.15.17.0006	n/a	WB.15.17.0005	Never released.
WB.15.17.0005	2015-05-11	WB.15.17.0004	Released, fully supported, but not posted on the web.
WB.15.17.0004	2015-04-23	WB.15.17.0003	Released, fully supported, but not posted on the web.
WB.15.17.0003	n/a	WB.15.16.0004	Never released.
WB.15.16.0011	2015-11-10	WB.15.16.0010	Please see the WB.15.16.0011 release note for detailed information on the WB.15.16 branch. Released, fully supported, and posted on the web.
WB.15.16.0010	2015-08-29	WB.15.16.0009	Released, fully supported, and posted on the web.

Version number	Release date	Based on	Remarks
WB.15.16.0009	2015-06-16	WB.15.16.0008	Released, fully supported, and posted on the web.
WB.15.16.0008	2015-04-17	WB.15.16.0007	Released, fully supported, and posted on the web.
WB.15.16.0007	n/a	WB.15.16.0006	Never released.
WB.15.16.0006	2015-02-06	WB.15.16.0005	Released, fully supported, and posted on the web.
WB.15.16.0005	2014-11-21	WB.15.16.0004	Released, fully supported, and posted on the web.
WB.15.16.0004	2014-10-30	WB.15.15.0006	Initial release of WB.15.16. Released, but never posted on the web.
WB.15.15.0014	2015-08-29	WB.15.15.0013	Please see the WB.15.15.0014 release note for detailed information on the WB.15.15 branch. Released, fully supported, and posted on the web.
WB.15.15.0013	2015-06-16	WB.15.15.0012	Released, fully supported, and posted on the web.
WB.15.15.0012	2015-04-17	WB.15.15.0011	Released, fully supported, and posted on the web.
WB.15.15.0011	n/a	WB.15.15.0010	Never released.
WB.15.15.0010	2015-02-06	WB.15.15.0009	Released, fully supported, and posted on the web.
WB.15.15.0009	2015-01-07	WB.15.15.0008	Released, fully supported, and posted on the web.
WB.15.15.0008	2014-09-15	WB.15.15.0007	Released, fully supported, and posted on the web.
WB.15.15.0007	2014-06-26	WB.15.15.0006	Released, fully supported, but not posted on the web.
WB.15.15.0006	2014-03-18	WB.15.14.0002	Initial release of WB.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
J9726A	Aruba 2920 24G Switch
J9728A	Aruba 2920 48G Switch
J9727A	Aruba 2920 24G PoE+ Switch
J9729A	Aruba 2920 48G PoE+ Switch
J9836A	Aruba 2920 48G PoE+ 740W 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

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
J9805A	HPE 640 Redundant/External PS Shelf	WB.15.13.0003

Enhancements

This section lists enhancements added to the WB.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 WB.15.17.0013

No enhancements were included in version WB.15.17.0013.

Version WB.15.17.0012

No enhancements were included in version WB.15.17.0012.

Version WB.15.17.0011

Never released.

Version WB.15.17.0010

No enhancements were included in version WB.15.17.0010.

Version WB.15.17.0009

Instrumentation Monitor

CR_0000164159 This feature enhances switch instrumentation and diagnostic capability.

Version WB.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 WB.15.17.0007

No enhancements were included in version WB.15.17.0007.

Version WB.15.17.0006

No enhancements were included in version WB.15.17.0006.

Version WB.15.17.0005

No enhancements were included in version WB.15.17.0005.

Version WB.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 WB.15.17.0003

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*.

DLDP

Device Link Detection Protocol (DLDP) is a feature that can detect unidirectional link status in a fiber or twisted pair cable, so that the link can be shut down. This feature is in Comware-based switches and is similar to the existing UDLD feature in ProVision switches. For more information, see the *HP Switch Software Basic Operation 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.

Fixes

This section lists released builds that include fixes found in the WB.15.17 branch of the software. 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 WB.15.17.0013

Event Log

CR_0000192892 Symptom: Audit event message is not logged when an invalid configuration fails to be downloaded onto the switch.

Scenario: When an identical, incorrect or invalid configuration file is rejected when downloaded on the switch, the audit event log message indicating the reason for file rejection is not recorded in the system event log.

Workaround: The error message rejecting the configuration file is displayed on the switch console though no RMON event is recorded in the switch event log.

File Transfer

CR_0000192894 Symptom: Setting the session idle-timeout to lower settings can cause a file transfer to hang indefinitely.

Scenario: When session idle-timeout is configured to lower values, a file transfer exceeding the configured idle-timeout may hang indefinitely when executed from a remote session to the switch.

Workaround: Configure session idle-timeout value to a higher value to allow file transfers to complete before the idle timer expires.

Menu

CR_0000198649 Symptom: Incorrect maximum number of supported authorized managers specified in the help text message of the Menu interface.

Scenario: The message text of the IP Authorized Managers "Help Screen" Menu interface states `A maximum of 10 addresses is supported.` The switch allows the configuration of up to 100 authorized managers.

Workaround: Use the CLI command `ip authorized-managers help` to determine the maximum number of authorized managers that can be configured on the switch.

OOBM

CR_0000194019 Symptom: A switch with OOBM port may experience an NMI crash and reboot.

Scenario: When there is a broadcast storm on the OOBM network, the switch might encounter a crash with an error message similar to `NMI event <...> Task='tDevPollRx' <...>` and reboot.

Workaround: Avoid broadcast storms on the OOBM network.

SNMP

CR_0000192914 Symptom: SNMP community access violation warning messages are not always reported in the switch event log.

Scenario: When Authorized IP Managers are configured on the switch, SNMP access from unauthorized management stations with correct community names are not reported in the switch event log.

Spanning Tree

CR_0000194044 Symptom: Traffic may be disrupted in an RPVST topology when VLAN configuration changes.

Scenario: In an RPVST topology, when there are ports configured for BPDU filter, PVST filter, and root guard, removing any VLAN from the switch configuration might cause traffic disruption in the network.

Workaround: Reapply all the configuration related to the root-guard, tcn-guard, bpdu-filter, and pvst-filter after removing VLAN.

CR_0000198794 Symptom: The switch may suffer occasional or chronic BPDU starvation, with log messages similar to `CIST starved for a BPDU Rx on port`.

Scenario: When the BPDU Throttling feature is enabled, it can trigger occasional or chronic BPDU starvation episodes. Spanning tree BPDU throttle configuration status can be confirmed by running the CLI command `show spanning-tree bpdu-throttle`.

Workaround: Disabling BPDU Throttling should stop the BPDU starvation symptoms. To disable BPDU Throttling feature, run the CLI command `no spanning-tree bpdu-throttle`.

Trunking

CR_0000198822 Symptom: The switch does not accept the LACP key option to configure an LACP trunk.

Scenario: When executing CLI command `lacp key <0-65535>`, the switch returns the error message `Invalid input: key`.

VLAN

CR_0000181782 Symptom: In certain switch software downgrade scenarios, the switch configuration may become unstable and the switch may potentially encounter software exception errors.

Scenario: When the switch is downgraded to an older switch software using a non-graceful method like changing switch software via ROM boot menu, the switch “max-vlans” configuration may become unstable while running the older switch software. This issue usually occurs when the switch is configured for the maximum supported number of VLANs using the CLI command `max-vlans <count>` with the maximum supported `<count>` VLANs for the currently running switch software.

Workaround: There are two workarounds for this issue:

1. Downgrade the switch using a graceful method like CLI command `boot [system [flash <primary | secondary>]]`.
2. Before downloading the switch software, remove the `max-vlans <count>` configuration that is not supported in the older switch software.

Version WB.15.17.0012

Banner

CR_0000190968 Symptom: Copying a configuration file with a banner text containing the quote (") character could cause a crash.

Scenario: Copying a configuration file with a banner message containing the quote (") character, where the message spans across multiple lines, might cause a crash with an error message similar to `Health Monitor: Restr Mem Access <...>`.

Workaround: Use short banner text or replace quote (") characters in the banner text message.

CLI

CR_0000192212 Symptom: The output of CLI command `show CPU` is not consistent.

Scenario: When the CPU goes to Idle state, the line for 1 minute average CPU usage is not displayed.

Console

CR_0000179094 Symptom: Sending special keys to a console switch configured in stacking mode may cause the switch to crash.

Scenario: Sending the **ESC** or **~** key to the console of a standby or member switch connected in a stack configuration may cause the switch to crash with an error message similar to `Software exception at multMgmtUtil.c <...>`.

Counters

CR_0000189924 Symptom: Incorrect values are displayed for transmit and receive counters of an interface.

Scenario: The Broadcast (Bcast) and Multicast (Mcast) transmit (Tx) and receive (Rx) counter values displayed in the output of the CLI command `show interfaces <PORT-LIST>` are inaccurate.

DHCP

CR_0000191729 Symptom: A switch acting as a DHCP Relay agent drops any DHCPINFORM packets with a TTL value set to 1.

Scenario: DHCPINFORM packets received with a TTL value of 1 are dropped by the DHCP Relay agent, so the DHCP client cannot acquire an IP address from the DHCP server.

Workaround: Configure the DHCP client network interface to use TTL values greater than 1.

DHCP Snooping

CR_0000183894 Symptom: DHCP Snooping may prevent DHCP clients from getting an IP address from a trusted server.

Scenario: When there are multiple DHCP servers configured for the same IP address scope and a DHCP server failover is triggered, new DHCP clients might not be able to obtain an IP address that is already registered in the switch DHCP Snooping binding database before the existing lease expires.

Workaround: Use one of these options:

1. Have the multiple DHCP servers configured with the same scope synchronized.
2. Delete the existing binding from the DHCP Snooping binding table using CLI command `no ip source-binding <...>`.

CR_0000189557 Symptom: Performing a software upgrade on the switch from software version `XX_15_16.XX` to `XX_15_17.XX` or later might fail.

Scenario: When DHCPv6 snooping static bindings are configured, a software upgrade on the switch from software version `XX_15_16.XX` to `XX_15_17.XX` or later might fail.

Workaround: Remove the DHCPv6 snooping static bindings configuration on the switch prior to software upgrade.

IGMP

CR_0000189793 Symptom: Deleting and reconfiguring an IGMP or PIM VLAN interface may not forward multicast traffic correctly.

Scenario: Enable IGMP or PIM on a VLAN. Delete VLAN from the configuration and re-configure the VLAN.

Workaround: Disable IGMP or PIM before deleting and reconfiguring VLAN interface.

IPv6

CR_0000189760 Symptom: An MLD-enabled switch may not properly interoperate with other third-party devices.

Scenario: When IPv6 is configured with the Router Alert option set for MLD, the switch may not properly interoperate with some third-party devices (such as CISCO).

PoE

CR_0000175786 Symptom: PoE devices that are power class 3 may experience random PoE power toggling.

Scenario: The switch may randomly report overcurrent indications on the system logs for the ports where connected PoE devices of power class 3 are drawing power via LLDP. When this event occurs, the connected PoE devices are losing power.

Workaround: Reduce the number of PoE devices of power class 3 connected on the switch at system boot.

CR_0000177617 Some vendor powered devices (PDs) supporting the POE+ standard can issue non-standard POE+ packets or packets with invalid TLVs while negotiating for power from the switch (PSE). Strict interpretation of the standard forces power to be cut off to such devices and could cause the PD to reboot continuously.

Workaround: Configure the associated port to be `poe-allocated-by value` and `poe-value <required-watts>` on the switch to avoid reboot.

Policies

CR_0000189858 Symptom: When service policy configuration is applied to a range of interfaces, the configuration is not properly displayed in the output of `show CLI` command.

Scenario: Apply a configured service policy to a range of ports using the CLI command `interface <port-list> service-policy <policy-name> in`. Only the first applied interface is displayed in the running configuration or the output of CLI command `show policy ports <port-list>`.

Workaround: Apply the policy to a single port at a time using the same CLI command.

Smart Link

CR_0000190943 Symptom: Traffic is not properly forwarded through smart links ports on switches configured in stacking mode.

Scenario: When multiple smart link groups are configured with ports tagged in different VLANs, traffic is not correctly forwarded when a smart link port is down

Workaround: Avoid configuring a second/subsequent smart link group whose port members are not part of the same VLANs as the existing smart link group.

Supportability

CR_0000183389 Symptom: CLI command `show tech all` may fail to run properly.

Scenario: CLI command `show tech all` may not complete or execute properly.

Syslog

CR_0000189320 Symptom: The switch might crash when enabling debug destination to syslog using the CLI command `debug destination logging`.

Scenario: When the switch is configured for logging to a remote syslog server with IPv6 address using temporary debug facility to system logging destination using the CLI command `debug destination logging`, the switch might crash.

Workaround: Configure the remote syslog server with an IPv4 address or redirect temporary debug to the local console or buffer facility using the CLI command `debug destination console | buffer`.

Version WB.15.17.0011

Never released.

Version WB.15.17.0010

ACLs

CR_0000181860 Symptom: While ACL Grouping is enabled, applying an ACL with no rules to a mixed range of ports that includes ports with already applied ACLs may lead to a switch reboot.

Scenario: Configure and apply an ACL to individual ports. Enable ACL grouping feature and configure an ACL with no rules defined. The switch may reboot when the ACL with no rules defined is applied to a range of ports.

Workaround: Remove the already applied ACLs from the port before applying the ACL to a mixed group of ports with and without previously applied ACLs.

CLI

CR_0000157943 When the CLI command `copy command-output 'show tech all'` is executed, it is possible that the switch will run out of free memory and trigger an unexpected reboot (crash) when memory allocation fails. The risk of this problem occurring is higher 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 will be 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 will be terminated automatically. When this happens, the following message will be displayed to the CLI and logged: `The command was terminated prematurely because the output exceeded the maximum memory limit.`

DHCP Snooping

CR_0000184104 Symptom: When DHCP enabled clients are roaming between DHCP snooping protected ports and are requesting different IP addresses without releasing the unexpired and previously assigned IP address, some DHCP Snooping protected ports may drop DHCP client requests, leaving DHCP clients unable to obtain new IP address leases.

Scenario: A DHCP enabled client connected to a DHCP snooping protected port is requesting an IP address lease then moves to another port in the same DHCP snooping protected VLAN and is requesting to lease a different IP address without releasing the previously leased IP address. When the new lease expires on the new port, it deems the new port unable to accept new DHCP requests.

Workaround: Remove and re-add the affected port from/to the DHCP snooping protected VLAN.

OpenFlow

CR_0000175735 Symptom: Downloading a configuration file to the switch may fail when one or more OpenFlow instances that have a controller assigned are present in the configuration file.

Scenario: When attempting to download a configuration file to the switch that contains OpenFlow instances with a controller assigned, the download may fail with the following error:

A listen-port or a controller, and a member VLAN must be added to the named instance before enabling it.

Workaround: Remove the OpenFlow configuration from the configuration file prior to download/restore, then restore the OpenFlow configuration from the CLI.

CR_0000177385 Symptom: Multiple updates of OpenFlow rules and meter configurations may lead to a switch crash with an error message similar to `Software exception at util.c:...`

Scenario: Multiple updates of OpenFlow rules and meter configurations may lead to a switch crash with an error message similar to `Software exception at util.c:...`

CR_0000182988 Symptom: Incorrect meter statistics are returned to the SDN controller.

Scenario: Statistics meter for matching traffic to the configured traffic flows is not correctly measured when sent to the SDN controller.

PIM

CR_0000177574 Symptom: In a PIM-SM topology with redundant path from RP to Source, when topology changes also force changes in the shortest path to Source, some of the receivers might not receive multicast streams via an existing alternate path.

Scenario: When a unicast routing change occurs in a PIM-SM network that triggers PIM-SM election of a new next hop PIM neighbor router via the shortest path, some receivers might not receive multicast traffic from the alternate route.

Workaround: Rejoin the multicast group.

Port Counters

CR_0000183662 Symptom: When the flow mod statistics are queried from the controller, incorrect values are received from the controller for the packet and byte count on a switch.

Scenario: When querying the flow statistics from the controller, incorrect multi-part reply packets are sent for flow stats with unknown message types. This happens when the flow table includes over 400 entries.

If the flow tables exceed 400 entries, the controller fails to pull more flows from the switch. This causes multipart reply packets to be sent to the controller with an unknown message type.

QinQ

CR_0000177736 Symptom: QinQ mode is not correctly removed when the switch is restored to a non-QinQ configuration.

Scenario: When a switch configured for QinQ mode is restored to factory-default configuration or to a non-QinQ mode configuration file, some residual QinQ configuration will cause QinQ mode to be re-enabled.

Workaround: Disable QinQ mode from CLI prior to restoring the switch to another non-QinQ configuration or to factory default.

RIP

CR_0000177096 Symptom: RIP peering may not be properly established when a VLAN interface is reconfigured.

Scenario: After deleting a VLAN that is configured for RIP and then reconfiguring that same VLAN, RIP peers are not properly formed on that VLAN.

Workaround: Disable and re-enable RIP router on the VLAN interface or at the global configuration level should result in a working peering with the RIP neighbor router.

TFTP

CR_0000180230 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 WB.15.17.0009

BPDU Protection

CR_0000176611 Under extended traffic oversubscription on flow-controlled ports, Spanning Tree BPDUs or other packets might occasionally be dropped.

Certificate Manager

CR_0000171714 After a reboot, the switch displays the wrong status for a TA profile with self-signed certificate, such as Pending Root Certificate Installation.

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.

CR_0000180373 After removing the static-group joins and immediately adding IGMP static-group joins for the same group, the CLI routine gives an error message and the token for that group is not deleted/freed.

Workaround: Do not remove and immediately re-add the same IGMP static-group joins for the same group.

Crash

CR_0000180705 In rare cases when attempting to configure the switch through the MENU or WEBUI interfaces or via a net management application, the switch might crash with the following signature.

```
.Active system went down: 09/10/15 12:55:32 K.15.18.0006 349 Health  
Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x00000000 IP=0x0  
Task='mSnmprCtrl' Task ID=0xa995840 sp:0x4206ea8 lr:0x86400 msr:  
0x02029200 xer: 0x00000000 cr: 0x24000400
```

Workaround: When configuring the switch, use only the CLI interface. Avoid using the MENU, WEBUI, or net management applications, such as IMC, to configure the switch.

CR_0000181774 The `show statistics policy` command might cause the switch to crash in certain configurations with maximum meters.

DHCP

CR_0000180195 Fix applied to make the DHCPACK packet being sent by the DHCP Server in response to a DHCPINFROM use the MAC Address of the client as destination instead of a broadcast address.

DHCP Snooping

CR_0000177144 There is a discrepancy between the DHCP-snooping binding database and the value reported by the dynamic binding counter.

File Transfer

CR_0000175506 In certain circumstances, a file transfer may not complete and will cause the switch to get into the permanent `Download is in progress, you cannot reboot now!` state.

IGMP

CR_0000157996 Removing and re-adding IGMP static groups could result in an "Inconsistent value" error message.

Workaround: After deletion of static group, wait for 3 seconds before re-adding it.

Logging

CR_0000155606 IPv4 duplicate address detection log message is added to the RMON logs.

MAC Authentication

CR_0000157903 With mac-auth failure-redirect feature configured as FQDN, loss of connectivity could be experienced at end points if DNS query is unable to resolve.

CR_0000176044 Updated Local Mac Authentication (LMA) OUIs list of Cisco IP-phones.

Menu Interface

CR_0000179336 While using the **IP Configuration Menu** interface to switch from **DHCP/Bootp** to **Manual** IP address configuration without first editing the switch's currently configured IP address for the respective VLAN interface, an `Invalid value` error message is received.

MLD

CR_0000135443 Node Local addresses in MLD Query/Report are not being dropped.

OpenFlow

CR_0000175712 Custom pipeline modification with traffic could cause the switch to crash with an error message similar to `Software exception at ovsTables.c`.

CR_0000177514 After a reboot with OpenFlow configuration, the switch might assume erroneous VLANs as OpenFlow member VLANs.

PBR

CR_0000175896 Modifying an already applied Policy Based Routing (PBR), with an action configured for a tunnel interface, could lead to a switch crash.

Workaround: Un-apply the policy, modify the policy, then reapply the policy.

PoE

CR_0000173739 When a powered PD is physically removed from a powered port, the PoE controller does not stop providing power to the port. This condition will trigger when the PSE is under a heavy load involving 12 or more active PDs. A PoE Controller firmware update is provided to update the PoE controller to version 38. The upgrade executes automatically when the switch is booted for the first time. Because the upgrade process needs to run, the boot process will take approximately 40 seconds longer than normal. When the upgrade has successfully completed, the following event log message will be recorded:

```
04753 Ports <port list>: PoE Software updated from version 04 to 38.
```

In the event that the POE controller firmware update is interrupted, an event log message similar to the following will be recorded:

```
Ports 1-12: PoE Software update failed with error code 0x00000006.  
Contact support for assistance.
```

Policy Based Routing

CR_0000173164 After a loss and restoration of connectivity between the switch and the PBR specified next-hop, the switch routes traffic conforming to match rules, as well as traffic conforming to the ignoring of rules to the PBR next-hop.

CR_0000178051 PBR service policy is displayed only for the first VLAN; the policy is applied to in the configuration.

Port Security

CR_0000148880 Switch fails to learn maximum MAC addresses on ports when port security is enabled.

QoS

CR_0000175792 The `show class config` and `show policy config` commands do not display complete output when large numbers of QoS classes and policies are configured.

RADIUS

CR_0000177823 During a RADIUS machine auth transition, the switch might incorrectly send the Class-ID of the user auth in the machine auth Accounting Stop packet. This results in the authentication-session of the user-auth getting cleared, so when we want to COA the client that there is no record of the session.

RA-guard

CR_0000177104 The error message displayed when enabling IPv6 ra-guard on dynamic trunk was updated to display IPv6 RA-guard is not supported for dynamic trunks.

Rate Limiting

CR_0000158994 Queue-based Rate Limiting for Egress Traffic & Guaranteed Minimum Bandwidth on Trunks.

Two new features have been implemented:

1. Guaranteed Minimum Bandwidth (GMB) on trunk interfaces. Up to now, it was not possible to configure GMB on aggregated interfaces ('trunks'). This has now been changed.

GMB allows a user to assign bandwidth percentages to a port's queues. The port queues will be serviced in descending order, up to the configured bandwidth percentage. When the configured limit has been reached, the software will service the next highest priority queue. When the queue has been fully serviced, but the limit has not yet been reached, remaining bandwidth will be offered to the next queue to be serviced. Any leftover bandwidth within a servicing window is then made available to the top priority queue.

It is also possible to configure 'strict priority queuing', which means that the highest priority queue may consume as much bandwidth as necessary, even if that will starve lower priority queues.

Note that even though GMB can now also be applied to a trunk, the actual GMB bandwidth percentages are applied to the physical ports that are a member of the trunk.

Configuring GMB on dynamic LACP trunks, Distributed Trunking interfaces, and Mesh ports will not be supported. The enhancement only applies to statically configured trunk ports.

2. Queue-based Rate Limiting for Egress Traffic Rate Limiting percentages can now also be configured on a per-port queue basis and will be applied to the traffic exiting the port.

The following new CLI command has been implemented to configure the feature: `[no] interface <port | trunk > rate-limit queues out percent [<queue %> <queue %> <queue %> <queue %> <queue %> <queue %> <queue %>]`

The following objects have been added to the HP-ICF-RATE-LIMIT-MIB in order to support the feature in SNMP: `hpEgressRateLimitPortQueueControlMode`

(.1.3.6.1.4.1.11.2.14.10.2.14.1.4.1.2.1.6)
hpEgressRateLimitPortQueueIndex
(.1.3.6.1.4.1.11.2.14.10.2.14.1.4.1.5.1.1) hpEgressRateLimitPortQueueMax
(.1.3.6.1.4.1.11.2.14.10.2.14.1.4.1.5.1.2)

CR_0000177775 Increased rate limiting values for ICMP traffic up to 100 GB, to accommodate interfaces with speed greater than 10 GB.

RMON

CR_0000144373 When RMON alarms are enabled on the switch, unintended characters are printed in the logs of the triggered alarm.

SNMP

CR_0000177848 Restoring backup configuration files with SNMPv3 enabled or QinQ SVLAN set, triggers an unexpected switch reboot even if the backup config is identical to the current config.

CR_0000181295 Running SNMP on dot3StatsDuplexStatus OID using an index of 0 causes the switch to crash.

Stacking

CR_0000173162 The J number of stacked devices is not properly reported in `entPhysicalVendorType` OID.

Supportability

CR_0000150068 Additional information reported in cli command 'show tech buffers'.

CR_0000156177 Core dump files are still generated when the feature is disabled.

Switch Initialization

CR_0000171369 When communicating with the switch (for example, via SCP, SSH, Telnet) over a connection with IP fragments, where some IP fragments are getting dropped, transfers stall or take an excessive amount of time.

TFTP

CR_0000165110 In rare cases, transferring a file via TFTP could result in a crash because of minor leaks in RAMFS.

VLAN

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.

Version WB.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`.

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'.`

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_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 outbound ACL 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

```

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.

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 WB.15.17.0007

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.

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 WB.15.17.0006

CLI

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

Config

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

Crash

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

CR_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.

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.

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 HPE 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.

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_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 WB.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.

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.

Config

CR_0000167908 When stacking is enabled, Manager and Operator passwords are set, and mirror-port or switch-interconnect are configured, the output of the command `show running-config` displays garbage entries, instead of Operator and Manager password configuration.

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_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 crashed 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 The switch reboots unexpectedly (crashes) if a user attempts to replace an ACL or QoS policy on multiple ports if an ACL or policy is already applied to some, but not all of the ports 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.`

OOBM

CR_0000162497 When a sustained broadcast storm has erupted in the network, the OOBM interface may be affected. Using the OOBM interface to manage the switch in such circumstances may result in slow responses from the switch or the session may not be established at all.

Stacking

CR_0000168556 In a stacking environment, when a switchover takes place, if the slave is unable to send a message to the commander within 200 ms, it can crash a Line Card.

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 WB.15.17.0003

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.

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_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.

Config

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

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_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_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_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.`

Crash Messaging

CR_0000153706 2920 Stack - boot-history and event log crash signature records do not report the same event. The event log entry looks more like a standard reboot message reported from commander to slave due to lack of communication.

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`.

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.

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.

OOBM

CR_0000157738 The `show oobm discovery` command sometimes indicates `Active Stack Fragment(local only without Active Stack Fragment(discovered))`, even if `show stacking` indicates both commander and member correctly with normal stacking connection.

After a stack in chain topology is split, the least commander fragment and the equal split standby fragment stays active until it discovers the other fragment is active over OOBM. If there is no OOBM connected, there are multiple active fragments or active commanders on the network.

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`.

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.

Port Connectivity

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

QoS

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

RADIUS

CR_0000149657 Configuration of multiple RADIUS servers via SNMP fails if a `createAndWait` mechanism is used.

Routing

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_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_0000158713 When reading the MIB data for a PSU Product ID J number, the number displayed is truncated by one character.

CR_0000160352 The string value for the temperature sensor's instance of the object `entPhysicalName` (.1.3.6.1.2.1.47.1.1.1.7) 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_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.

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

Certificate Manager

CR_0000172987 No warning or action confirmation message is provided at CLI while replacing CSR with a self-signed certificate.

PoE

CR_0000192808 Symptom: Dual-port Aruba APs, such as AP325, AP225, AP135, may occasionally power up with reduced power (802.3af mode) and AP's system status LED will lit up amber.

Scenario: Occasionally, when both Ethernet ports of dual-port Aruba APs, such as AP325, AP225, AP135 are connected to a PoE+ switch, AP's LED status may indicate a fault condition (amber) and only one of AP's ports E0 or E1 is on and will be receiving power.

Workaround: Disable LLDP dot3TLV on the switch whenever both ports of dual-port Aruba APs are plugged into the switch.

SNMP

CR_0000190877 Symptom: SNMP communities default configuration values are not consistently displayed between the output of CLI command `show running-config` and `show snmp-server`.

Scenario: When executing CLI command `show running-config`, only non-default configuration parameters for SNMP communities are displayed, such as read/write MIB access mode, and operator/manager MIB access level.

Workaround: Use the CLI command `show snmp-server` to display SNMP communities' complete configuration.

Upgrade information

Upgrading restrictions and guidelines

WB.15.17.0013 uses BootROM WB.15.05. 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.
-

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 HP 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 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.

Related documents

The following documents provide related information:

- *HP Switch Software Advanced Traffic Management Guide WB.15.17*
- *HP Switch Software Access Security Guide WB.15.17*
- *HP Switch Software Basic Operation Guide*
- *HP Switch Software Feature and Commands Index*
- *HP Switch Software IPv6 Configuration Guide WB.15.17*
- *HP Switch Software Management and Configuration Guide WB.15.17*
- *HP Switch Software Multicast and Routing Guide WB.15.17*
- *HP OpenFlow 1.3 Administrator Guide K/KA/KB/WB.15.17*
- *HP Service Insertion Guide K/KA/KB/WB.15.17*

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.