Hewlett Packard
Enterprise

WB.15.18.0012 Release Notes

Abstract

This document contains supplemental information for the WB.15.18.0012 release.

Part Number: 5200-2029
Published: August 2016
Edition: 1

Acknowledgments

Contents

1 WB.15.18.0012 Release Notes

Description

This release note covers software versions for the WB.15.18 branch of the software.

Version WB.15.18.0006 was the initial build of Major version WB.15.18 software. WB.15.18.0006 includes all enhancements and fixes in the WB.15.17.0003 software, plus the additional enhancements and fixes in the WB.15.18.0006 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.15.18.0012	2016-08-02	WB.15.18.0011	Released, fully supported, and posted on the web.
WB.15.18.0011	2016-05-31	WB.15.18.0010	Released, fully supported, and posted on the web.
WB.15.18.0010	2016-03-28	WB.15.18.0009	Released, fully supported, and posted on the web.
WB.15.18.0009	n/a	WB.15.18.0008	Never released
WB.15.18.0008	2016-01-19	WB.15.18.0007	Released, fully supported, and posted on the web.
WB.15.18.0007	2015-11-10	WB.15.18.0006	Released, fully supported, and posted on the web.
WB.15.18.0006	2015-08-15	WB.15.17.0003	Initial release of the WB.15.17 branch. Released, fully supported, and posted on the web.
WB.15.17.0013	2016-05-25	WB.15.17.0012	Please see the WB.15.17.0013 release not for detailed information on the WB.15.17 branch. 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.

Version number	Release date	Based on	Remarks
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	Initial release of the WB.15.17 branch. Never released.
WB.15.16.0012m	2016-01-19	WB.15.16.0011	Please see the WB.15.16.0012 release note for detailed information on the WB.15.16 branch. Released, fully supported, and posted on the web.
WB.15.16.0011	2015-11-10	WB.15.16.0010	Released, fully supported, and posted on the web.
WB.15.16.0010	2015-08-28	WB.15.16.0009	Released, fully supported, and posted on the web.
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.

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 found in the WB.15.18 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.15.18.0012

No enhancements are included in version WB.15.18.0012.

Version WB.15.18.0011

Authentication

CR_0000200562 Added 802.1x-2010 compliance support for HPE 2920 Switch Series. 802.1X-2010 mode can be enabled for authenticator and supplicant using the CLI command `[no] aaa port-access dot1x2010 [authenticator|supplicant].`

BootROM

CR_0000200859 The BootROM has been updated to version WB.16.01.

Enhanced Secure Mode

CR_0000199914 Symptom: Added Enhanced Secure Mode functionality. To transition from one security mode to the other. Enter the following command from a serial terminal connected to the switch: `secure-mode <standard | enhanced>`.

Version WB.15.18.0010

No enhancements were included in version WB.15.18.0010.

Version WB.15.18.0009

Never released.

Version WB.15.18.0008

Event Log

CR_0000189525 Added audit log message to the system logging for the following events:

- Termination of a secure session
- Failure to negotiate the cipher suite due to cipher mismatch for SSL and SSH sessions

CR_0000190131 Added RMON audit log messages when SNTP is disabled using the CLI `no sntp` command.

CR_0000190134 Added an audit log message regarding the console inactivity timer when the `console idle-timeout` command is used.

CR_0000190141 Added audit log messages when the default gateway IP address is configured or modified.

Zeroization

CR_0000183856 Added CLI command `erase all [zeroize]` to enable zeroization of the switch file storage.

Example:

```
HP Switch(config)# erase all zeroize

The system will be rebooted and all management module files except
software images will be erased and zeroized. This will take up to 60
minutes and the switch will not be usable during that time. Continue
(y/n)? y
```

The zeroization feature removes and “zeroizes” all the files from flash storage except software images. Information removed includes the following:

- Switch configurations
- System generated private keys
- User installed private keys
- Legacy manager/operator password files
- Crypto-key files
- FDR logs
- Core dumps

Hewlett Packard Enterprise recommends that zeroization be performed from the serial console so that the status information can be viewed during the zeroization process.

Version WB.15.18.0007

No enhancements were included in version WB.15.18.0007.

Version WB.15.18.0006

Instrumentation Monitor

CR_0000164159 This feature enhances switch instrumentation and diagnostic capability.

IP DirectedBroadcast

CR_0000145338 This feature enhances the security of the "IP Directed Broadcast" feature by denying traffic that is not specified within the configured access list.

Management

CR_0000166746 This feature enables zero touch provisioning for switch deployment.

*Requires IMC/BIM

OpenFlow

CR_0000173444 This feature allows the user to enable source and destination MAC Group tables in the OpenFlow pipeline.

CR_0000173447 This feature supports OpenFlow matching traffic based upon L4 information.

Port Filters

CR_0000142989 This feature provides granularity beyond Source Port filtering by allowing traffic exclusive to a specific VLAN to be forwarded.

Routing

CR_0000168848 This feature adds MD5 authentication to RIPv2 routing to enhance security.

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. 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` *`[no] interface <port | trunk > rate-limit queues out percent [<queue %> <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)`

Security Vulnerability

CR_0000161421 This feature provides support compliance for the cryptographic algorithm Suite B of US NIST (National Institute Standard and Technology).

TFTP

CR_0000156362 This feature allows both TFTP and SSH to be enabled in a switch concurrently.

Fixes

This section lists released builds that include fixes found in the 15.18 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.15.18.0012

GVRP

CR_0000204332 Symptom: The detailed information about mac-addresses dynamically learned by the switch is not correctly displayed in the output of CLI command `show mac-address` *`<mac-address>`*.

Scenario: When mac-addresses are learnt from a VLAN that was dynamically configured using GVRP, the CLI command `show mac-address` *`<mac-address>`* does not display any detailed information.

Workaround: Use the CLI command `show mac-address`.

Spanning Tree

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

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

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

TACACS

CR_0000201235 Symptom: Authentication and authorization requests may be delayed up to 1 second.

Scenario: The switch may delay sending TACACS authentication and authorization requests for up to 1 second.

Transceivers

CR_0000210703 Symptom: The OID entLastChangeTime value is not correctly updated.

Scenario: When a transceiver is inserted, moved or hotswapped, the switch does not correctly update the value reported in entLastChangeTime OID.

USB

CR_0000202216 Symptom: The switch may crash with an error message similar to `MemWatch Trigger: Offending task 'mSess1' <...>`.

Scenario: When executing `dir` command, without any other parameters, on a USB device connected and mounted into the switch while accounting is enabled, the switch may crash with an error message similar to `MemWatch Trigger: Offending task 'mSess1' <...>`.

Workaround: Execute `dir` command with a specified *`path`* parameter. For example, `dir /<dir_path>`.

Version WB.15.18.0011

Display Issue

CR_0000190925 Symptom: A 100% CPU usage spike every 10 minutes.

Scenario: With (KB/WB).15.18.xxxx code, a new security feature was introduced, to meet CC-NDPP (Common Criteria-Network Device Protection Profile) Certification criteria. This feature is designed to help users create strong cryptographic keys that are harder to predict. The key aspects of design includes (a) maintaining an entropy pool, (b) identifying the random sources, and (c) processing the sources, that is, feeding the random source to the NIST approved Deterministic Random Bit generator (DRBG) algorithm. Whenever the user generates a random number, this entropy algorithm ensures sufficient randomness in the system; if the system does not have sufficient randomness, as per requirement, cryptographic operations are blocked until new entropy is added to the system. To meet this NIAP entropy requirement, on HPN Aruba switches, the random data collection and processing happens once in every 10 minutes. The design implemented on the HPE/Aruba switches was approved by NIAP (**https://www.niap-ccevs.org/**).

Workaround: There are new changes added to the entropy behavior to ensure that it runs without the perception issue that all of CPU is being utilized every 10 minutes, even though important tasks are given the priority with no impact on performance.

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.

IGMP

CR_0000198564 Symptom: Receiving certain IGMP membership reports might cause the querier to stop sending GQ messages to other IGMP hosts already joined to other groups.

Scenario: An IGMP querier stops sending GQ messages to hosts already joined to other groups when it receives IGMP membership reports sent to reserved multicast address ranges (for example, Multicast IP address pattern of X.0.0.Y).

Workaround: Avoid sending IGMP membership reports to reserved multicast address ranges or configure IGMP querier for IP lookup-mode (`igmp lookup-mode ip`), if supported.

Menu

CR_0000198649 Symptom: An incorrect maximum number of supported authorized managers is 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 configurations related to the root-guard, tcn-guard, bpdu-filter, and pvst-filter after removing VLAN.

CR_0000198794 Symptom: The switch might 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`.

Switch Module

CR_0000192470 Symptom: After a period of uptime, switch blades might reset with an error message similar to `Software exception in ISR at interrupts_mac.c <...> -> Excessive MAC Interrupts at chipPort <...>`.

Scenario: When there is an excessive amount of received packets with shorter preamble than the industry standard, HPE switch blades might reset due to excessive interrupt handling.

Workaround: Reconfigure the peer device to use a long preamble.

Trunking

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

Scenario: When executing the 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:

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

Version WB.15.18.0010

Banner

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

Scenario: Copying a configuration file with a banner message containing the quote (") character spanning across multiple lines, might cause a switch 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 might 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 might 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_0000167762 Symptom: In high availability switches, after a failover occurs, the DHCP Snooping bindings learned from a TFTP server are not retained and all DHCP clients lose connectivity in case of a redundancy failover.

Scenario: DHCP Snooping bindings learned from a TFTP server are not correctly synced to the standby management module or switch; the entries are lost in the event of a switch failover to standby the management module or standby switch.

Workaround: The switch needs to re-learn all connected DHCP clients after a failover event.

CR_0000183894 Symptom: DHCP Snooping might 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 the following 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 switch software upgrade from software version XX_15_16.XX to XX_15_17.XX or later might fail.

Workaround: Remove the DHCPv6 snooping static bindings configuration from 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 the 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).

IPv6 ND

CR_0000191543 Symptom: In certain conditions, the switch is unable to discover an IPv6 neighbor.

Scenario: The switch is unable to discover an IPv6 neighbor when the point-to-point inter-router link is configured with /127 IPv6 prefix length.

Workaround: Do not use /127 IPv6 prefix length for the point-to-point inter-router link.

PoE

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

Scenario: The switch might randomly report over current 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 lose power.

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

CR_0000177617 Symptom: 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 a service policy configuration is applied to a range of interfaces, the configuration is not properly displayed in the output of the `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 the 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 link 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 or 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` might 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.15.18.0009

Never released.

Version WB.15.18.0008

AAA

CR_0000180339 Symptom: Users who are authenticated via a RADIUS server with permissions to execute default security group commands are not allowed to execute the default security group commands.

Scenario: Configure switch and RADIUS user profiles to authenticate with permissions to execute CLI commands from the default security group. Authenticated users with these permissions are not able to execute CLI commands assigned by default to the security group, such as `clear | copy | show security-logging`.

Workaround: Use locally-defined users for authentication in the default security group. Create a custom security group for RADIUS-authenticated users and associate these CLI commands to that group.

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 might 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 might 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.

DHCP

CR_0000182394 Symptom: Adding or updating DHCP Snooping lease database transfer options after configuring the lease file URL to SFTP removes the authentication credentials included in the configuration file for the SFTP server.

Scenario: Configure the switch to include the authentication credentials in the configuration file using the command `include-credentials`. Configure the DHCP snooping database lease file URL for SFTP using the command `dhcp-snooping database file sftp://USERNAME@<IP-ADDR>/<FILENAME>`. When adding or updating other database lease options, such as delay or timeout, the SFTP authentication credentials are removed for the configuration.

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 might 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 requests 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 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/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.

OSPF

CR_0000177561 Symptom: Incorrect interface priority value is displayed in the output of the `show ipv6 ospf3 neighbor` command for the tunnel interface.

Scenario: Enable OSPFv3 on a 6in4 tunnel interface and connect OSPF neighbor routes, then execute the `show ipv6 ospf3 neighbor` command. The incorrect priority value for tunnel interface is displayed.

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 causes QinQ mode to be re-enabled.

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

SNMP

CR_0000182311 Symptom: If a switch is reconfigured from MSTP to RPVST, while spanning-tree traps are already enabled on the switch, none of the RPVST SNMP traps are sent.

Scenario: When the switch is configured for MSTP, Spanning Tree mode, and SNMP notifications, changing the mode to RPVST also disables the configured Spanning Tree traps. Although the traps are displayed in the configuration as ‘enabled’ and the value of the object ‘hpSwitchStpCntl’ (.1.3.6.1.4.1.11.2.14.11.5.1.7.1.14.3) indicates that the traps are properly enabled, none of the configured notifications are sent to a trap receiver. When the traps are reconfigured or the switch is rebooted, the SNMP traps are transmitted again as expected.

Workaround: Re-enable SNMP Spanning Tree traps using CLI command `spanning-tree traps` or reboot the switch to restart the Spanning Tree SNMP traps transmission.

Spanning Tree

CR_0000175721 When setting the RPVST mode for spanning tree, the switch continuously displays the erroneous error message: `WARNING: Reboot switch and use CLI commands to configure MSTP parameters.`

Workaround: The error message can be ignored.

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.15.18.0007

ACLs

CR_0000178154 Configuring extended ACL with condition `gt`, `lt`, or `range` for source/destination port, reports an error message `Commit failed`.

Authorization

CR_0000172174 Using AAA authentication, a security user could gain access to both manager and security log commands.

CR_0000175376 Users not part of a local authorization group can have access to default security commands.

Certificate Manager

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

CR_0000179330 Configuring `tls lowest-versiopn` might cause the switch to crash with an error message similar to `Software exception at cli_crypto_action.c`.

Classifier

CR_0000174198 Policy statistics are not cleared when no direction (in/out) is specified with Clear Statistics policy CLI.

CR_0000174199 The `show statistics policy` command does not return the correct information when no direction (in/out) is specified.

CLI

CR_0000171261 A new CLI is introduced to enable resetting the PoE controller and restoring functionality on the affected ports: `power-over-ethernet poe-reset port <port name>`.

CR_0000178304 There is a potential memory leak caused by repetitive use of the CLI command `show crypto pki ta-profile`.

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 or 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='mSnmpCtrl' 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.

Event Log

CR_0000179527 Updated RIP syslog event IDs.

File Transfer

CR_0000175506 In certain circumstances, a file transfer does not complete and causes 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 deleting the static group, wait for 3 seconds before re-adding it.

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_0000174050 When OpenFlow and Service tunnels are configured, if interfaces are disabled and enabled while traffic is flowing, the system could crash with an error message similar to `Software exception at opflAccel.c`.

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_0000175907 OpenFlow rejects some flows while installing only flows with only `eth_src` in match list.

CR_0000176014 Deleting one flow deletes all previously created flows.

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_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.
```

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 triggers 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 takes approximately 40 seconds longer than normal. When the upgrade has successfully completed, the following event log message is 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 is 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.

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 or 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 a dynamic trunk has been updated to display `IPv6 RA-guard is not supported for dynamic trunks.`

Rate Limiting

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

Routing

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

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

SNMP

CR_0000175683 The switch may not send "Cold start" traps after a reboot.

CR_0000177261 Non-default values (other than 0) configured for egress rate (transmission-interval) that generates the SNMP trap notifications for changes to running configurations are not applied. (Example: `logging notify running-config-change transmission-interval 10`).

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_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.

Syslog

CR_0000179328 A small subset of event IDs sent to the syslog server have different values between releases.

Version WB.15.18.0006

802.1X

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-ANSI characters. When the CLI is used, the action is not allowed and an error message is displayed.

Certificate Manager

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.

CLI

CR_0000145812 A new command `tcp-push-preserve` is added. This command is enabled by default, and causes TCP packets with the "push" flag to be sent before other packets in the queue. Note that high concentrations of TCP packets with push flags under certain conditions can destabilize your network. Use the **no** form of this command to disable the feature.

CR_0000149525 The switch incorrectly allows a user to enable stacking when more than four MSTP instances are configured.

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 will indicate that the switch requires a reboot. When the switch is actually rebooted the same problem will be present after the reboot.

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

CR_0000170477 A user can successfully log in using the default username (manager/operator), even if a custom username is configured.

CR_0000172046 The commands `show lldp info local-device` and `show lldp info remote-device` may fail to display the correct information [Chassis ID] when the switch is standalone or connected to any remote device.

CR_0000174064 The Management and Configuration Guides shows a CLI command of `(no) lldp config <port-no> dot3TlvEnable poeplus_config`, but the CLI is using `(no) lldp config <port-no> dot3TlvEnable poe_config`. The CLI was changed to match the documentation, which better describes the action.

Command Authorization

CR_0000160066 The listen-port help command has changed: `[no] listen-port <PORT-NUM>`.

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.

CR_0000175601 After configuring the switch to deny writes to memory with the `aaa authorization group <group id> 6 match-command "write memory" deny` command, the user is still prompted to save configuration changes. If the user chooses to save the changes, they are saved to memory.

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_0000141119 The output of `show ip counters` is incorrect when routing is enabled for IP, IPv6, or multicasts.

CR_0000149229 The "Route changes" counter in the output of `show ip rip` increments with every RIP update the router receives, even if there are no route changes.

CPU Utilization

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_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 may 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_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_0000159764 Due to an unknown trigger, a switch may reboot 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_0000164064 When a free radius authenticated user attempts to HTTPS to the switch web management GUI of the 2530-24G, the switch reboots with `Health Monitor: Read Error Restr Mem Access Task='tHttpd'.`

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_0000168194 The switch may 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.`

CR_0000170286 When a module is inserted into or removed from a switch with a large number of VLANs and ports, port configuration for every port is updated, leading to an unexpected switch reboot. To address this, the burst of logs is throttled.

CR_0000170693 Enabling HPE Network Protector on the VAN SDN Controller and receiving DNS traffic causes packet buffer depletion in the switch and eventually can lead to PIM module reboot.

Crash Messaging

CR_0000150468 The crash message includes extraneous text about filing a CR (Change Request).

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`.

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_0000165004 If Distributed 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).

IPv6

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

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`. The fix for this provides a more meaningful error message.

Latency

CR_0000129743 When the switch receives a high volume of traffic for unknown destinations, the resulting ARPs sent by the switch in combination with other incoming traffic the switch must process can cause latency and dropped packets. In this situation, the event log might report `IpAddrMgr: IPAM Control task delayed due to slave message queues too full`.

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.

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 will actually apply the invalid 0 Watts. This will cause the PD to reboot every time it transmits the 0 Watts in the TLV. The switch may log overcurrent warnings (`00562 ports: port <port ID> PD Overcurrent indication.`) as the PD is already drawing power over the port when the software applies 0 Watts power. The value of 0 Watts in the TLV will henceforth be rejected with the error `Invalid power value 0 deciWatts received from MED PD on port <port ID>`.

Logging

CR_0000149891 When a user disables layer 3 on a VLAN, the event log message might state that layer 3 was disabled for the wrong VLAN.

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

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

Management

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

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_0000163370 Violation of OpenFlow requirement that if the match field OXM_OF_IP_DSCP is used the ETH TYPE must be 0x0800 **or** 0x86dd.

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 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.

Packet Buffers

CR_0000170693 Enabling Network Protector on the VAN SDN Controller and receiving DNS traffic causes packet buffer depletion in the switch and eventually can lead to PIM module reboot.

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.

CR_0000172606 The Web UI can now display a port range when setting QoS. Previously the Web UI displayed only the first port in the range.

RADIUS

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

Routing

CR_0000148889 The host cache list structure for certain routes has changed to improve lookup performance.

CR_0000160655 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 agents response IP address is also applied to the VACL, and hosts will become unreachable.

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.

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 will not reach its destination because the switch did 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 will temporarily resolve the reachability issue; however, the issue may reoccur after the ARP 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 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
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
```

sFlow

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

SNMP

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 will reset 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_0000160352 The string value for the temperature sensor’s instance of the object entPhysicalName (.1.3.6.1.2.1.47.1.1.1.1.7) 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 will terminate 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_0000146890 When the stacking cable is removed from a two-switch stack, both switches show "Stack Status" of `Fragment Active`.

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

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

Switch Initialization

CR_0000169998 VLAN port configuration changes made in the menu interface persist and cannot be reversed at the CLI.

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

TACACS

CR_0000177904 When more than one TACAS server is configured and all are not reachable, failover to local authentication does not occur.

Workaround: Configure single TACAS server with failover to local authentication. Use Radius servers and authentication.

Transceivers

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

UDP Crash

CR_0000172405 When UDP broadcast traffic is sent to a switch with UDP forwarder configured, an unexpected reboot 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:.`

Web GUI

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

Web Management

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

The following are known issues in the WB.15.18.0012 release.

PoE

CR_0000192808 Symptom: Dual-port Aruba APs, such as AP325, AP225, AP135, might occasionally power up with reduced power (802.3af mode) and AP's system status LED 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 on will receive 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.15.18.0012 uses BootROM WB.16.01. 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 HPE 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 HPE Support Center - Hewlett Packard Enterprise at **www.hpe.com/support/hpesc**.
2. Enter your product name or number and click **Go**.
3. Select your product from the list of results.
4. Click the **Top issues & solutions** tab.
5. Click the **Advisories, bulletins & notices** link.

To initiate a subscription to receive future Hewlett Packard Enterprise Security Bulletin alerts via email, sign up at:

www4.hpe.com/signup_alerts

Documents

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

Related documents

The following documents provide related information:

- *HP Switch Software Advanced Traffic Management Guide WB.15.18*
- *HP Switch Software Access Security Guide WB.15.18*

- *HP Switch Software Basic Operation Guide*
- *HP Switch Software Feature and Commands Index*
- *HP Switch Software IPv6 Configuration Guide WB.15.18*
- *HP Switch Software Management and Configuration Guide WB.15.18*
- *HP Switch Software Multicast and Routing Guide WB.15.18*
- *HP OpenFlow 1.3 Administrator Guide K/KA/KB/WB.15.18*
- *HP Service Insertion Guide K/KA/KB/WB.15.18*

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**
HPE Networking Software	**www.hpe.com/networking/software**
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**
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.