Hewlett Packard
Enterprise

A.15.16.0014m Release Notes

Abstract

This document contains supplemental information for the A.15.16.0014m release.

Part Number: 5200-2177
Published: September 2016
Edition: 1

Acknowledgments

Contents

1 A.15.16.0014m Release Notes

Description

These release notes cover software versions for the A.15.16 branch of the software.

Version A.15.16.0004 was the initial release of Major version A.15.16 software. A.15.16.0004 software was built from the same source as A.15.15.0006. A.15.16.0004 includes all enhancements and fixes in A.15.15.0006 software, plus the additional enhancements and fixes in the A.15.16.0004 enhancements and fixes sections of this release note.

Product series supported by this software:

- HPE 2615 PoE Switch Series
- HPE 2915 PoE 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
A.15.16.0014m	2016-08-19	A.15.16.0013m	Released, fully supported, and posted on the web.
A.15.16.0013m	2016-05-25	A.15.16.0012m	Released, fully supported, and posted on the web.
A.15.16.0012m	2016-01-19	A.15.16.0011	Released, fully supported, and posted on the web.
A.15.16.0011	2015-11-10	A.15.16.0010	Released, fully supported, and posted on the web.
A.15.16.0010	2015-08-29	A.15.16.0009	Released, fully supported, and posted on the web.
A.15.16.0009	2015-06-16	A.15.16.0008	Released, fully supported, and posted on the web.
A.15.16.0008	2015-04-17	A.15.16.0007	Released, fully supported, and posted on the web.
A.15.16.0007	n/a	A.15.16.0006	Never released.
A.15.16.0006	2015-02-06	A.15.16.0005	Released, fully supported, and posted on the web.
A.15.16.0005	2014-11-21	A.15.16.0004	Released, fully supported, and posted on the web.
A.15.16.0004	2014-10-30	A.15.15.0006	Initial release of A.15.16. Released, but never posted on the web.
A.15.15.0014	2015-08-29	A.15.15.0013	Please see the A.15.15.0014 release note for detailed information on the A.15.15 branch. Released, fully supported, and posted on the web.

Version number	Release date	Based on	Remarks
A.15.15.0013	2015-06-16	A.15.15.0012	Released, fully supported, and posted on the web.
A.15.15.0012	2015-04-17	A.15.15.0011	Released, fully supported, and posted on the web.
A.15.15.0011	n/a	A.15.15.0010	Never released.
A.15.15.0010	2015-02-06	A.15.15.0009	Released, fully supported, and posted on the web.
A.15.15.0009	2015-01-07	A.15.15.0008	Released, fully supported, and posted on the web.
A.15.15.0008	2014-09-15	A.15.15.0007	Released, fully supported, and posted on the web.
A.15.15.0007	2014-06-26	A.15.15.0006	Released, fully supported, but not posted on the web.
A.15.15.0006	2014-03-19	A.15.14.0002	Initial release of A.15.15. Released, fully supported, and posted on the web for early availability.
A.15.14.0012	2015-04-17	A.15.14.0011	Please see the A.15.14.0012 release note for detailed information on the A.15.14 branch. Released, fully supported, and posted on the web.
A.15.14.0011	2015-02-06	A.15.14.0010	Released, fully supported, and posted on the web.
A.15.14.0010	2014-11-17	A.15.14.0009	Released, fully supported, and posted on the web.
A.15.14.0009	2014-09-15	A.15.14.0008	Released, fully supported, and posted on the web.
A.15.14.0008	2014-07-16	A.15.14.0007	Released, fully supported, but not posted on the web.
A.15.14.0007	2014-07-01	A.15.14.0006	Released, fully supported, and posted on the web.
A.15.14.0006	2014-04-01	A.15.14.0002	Released, fully supported, but not posted on the web.
A.15.14.0005	n/a		Never built.
A.15.14.0004	n/a		Never built.
A.15.14.0003	n/a		Never built.
A.15.14.0002	2013-10-18	A.15.13.0003	Initial release of A.15.14, fully supported, and posted on the web for early availability.

Products supported

This release applies to the following product models:

Product number	Description
J9562A	HPE 2915-8G-PoE Switch
J9565A	HPE 2615-8-PoE Switch

Compatibility/interoperability

The switch web agent supports the following operating system and web browser combinations:

Operating System	Supported Web Browsers
Windows XP SP3	Internet Explorer 7, 8 Firefox 12
Windows 7	Internet Explorer 9, 10 Firefox 24 Chrome 30
Windows 8	Internet Explorer 9, 10 Firefox 24 Chrome 30
Windows Server 2008 SP2	Internet Explorer 8, 9 Firefox 24
Windows Server 2012	Internet Explorer 9, 10 Firefox 24
Macintosh OS	Firefox 24

Enhancements

This section lists enhancements found in the A.15.16 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 that precedes the enhancement description is used for tracking purposes.

Version A.15.16.0014m

No enhancements are included in version A.15.16.0014m.

Version A.15.16.0013m

No enhancements are included in version A.15.16.0013m.

Version A.15.16.0012m

No enhancements are included in version A.15.16.0012m.

Version A.15.16.0011

No enhancements are included in version A.15.16.0011.

Version A.15.16.0010

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 A.15.16.0009

Memory

Enhancements were made to optimize memory usage.

Version A.15.16.0008

No enhancements are included in version A.15.16.0008.

Version A.15.16.0007

Version A.15.16.0007 was never released.

Version A.15.16.0006

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.

Version A.15.16.0005

No enhancements are included in version A.15.16.0005.

Version A.15.16.0004

BYOD Redirect

CR_0000152339 BYOD redirect. The switch can now be configured for BYOD (Bring Your Own Device) redirect, which sends the device's credentials to a BYOD server such as IMC, that is configured to control network access.

DHCPv4

CR_0000128651 DHCPv4 server. The switch can now be configured as a DHCPv4 server. For more information, see the *HP Switch Software Management and Configuration Guide* for your switch.

DHCPv6

CR_0000144107 DHCPv6 hardware addresses. The switch can be configured with option 79 to instruct DHCPv6 relay agents to forward client link-layer addresses. For more information, see the *HP Switch Software Management and Configuration Guide* for your switch.

Generic Header ID

CR_0000144861 Generic header ID in configuration file. The switch now allows addition of a generic header ID to configuration files saved on a server. This is used for DHCP Option 67 download requests for configuration files. For more information, see the *HP Switch Software Management and Configuration Guide* for your switch.

Local MAC Authentication

CR_0000128955 Local MAC Authentication (LMA) is a software feature that simplifies deployment for devices such as IP phones and security cameras. In general, it provides dynamic attribute assignment (e.g., VLAN and QoS) through the use of a locally configured authentication repository. The most common use model for LMA is to automatically assign a VLAN to IP phones. In some cases, it can also provide rudimentary access security for the network. See "Web and MAC Authentication" in the *HP Switch Software Access Security Guide* for your switch.

MAC-based VLANs

CR_0000128831 MAC-Based VLANs (MBV) Enable/Disable. MBV enable/disable options are available using CLI and SNMP. For more information, see the "Web-based and MAC Authentication", and the "Port-Based and User-Based Access Control (802.1X)" chapters in the *HP Switch Software Access Security Guide* for your switch.

UDLD

CR_0000147189 UDLD Verify Before Forwarding. Unidirectional Link Detection (UDLD) has been enhanced to account for the situation when the link to the directly-connected device is up, but there is no link on one segment of the path to the remote device. For more information, see the *HP Switch Software Management and Configuration Guide* for your switch.

VLAN

CR_0000145339 VLAN Precedence. Beginning with 15.06 software, if a VLAN is added to a port while authenticated clients are connected to that port, the VLAN addition is delayed until all authenticated clients are disconnected. This enhancement allows a tagged VLAN to be applied immediately to a port that has connected authenticated clients. For more information, see the *HP Switch Software Advanced Traffic Management Guide* for your switch.

Fixes

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

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

Version A.15.16.0014m

IP Stacking

CR_0000210273 Symptom: Unable to upload switch software onto a stack member switch using web UI.

Scenario: When configured for IP Switch Stack Management, switch software cannot be uploaded onto stack member switches using web GUI.

Workaround: Upload switch software onto stack member switches using CLI interface.

Stacking

CR_0000213756 Symptom: IP Switch Stack Management may not work properly.

Scenario: When the configured primary VLAN is different than the factory-default VLAN (DEFAULT_VLAN), IP Stack Management may not work properly.

Workaround: Configure the factory-default VLAN DEFAULT_VLAN as the primary VLAN and add all candidate switches on the same stack to DEFAULT_VLAN.

Version A.15.16.0013m

802-1x

CR_0000170012 Symptom: Certain 801.x supplicant clients may not be successfully authenticated by the switch when configured as 802.1X authenticator for port access.

Scenario: Certain 801.1X supplicant clients, such as the HP 425 802.11n Dual Radio Access Point Series, fail to be successfully authenticated by a switch configured as 802.1x authenticator for port access, without an existing guest VLAN.

Workaround: Configure the switch with a guest VLAN for 802.1x port access authentication. Example: `aaa port-access authenticator <PORT-NUM> unauth-vid <VLAN-ID>`.

CR_0000199478 Symptom: User specific RADIUS applied ACLs are not displayed properly in the output of CLI command `show access-list radius <PORT-LIST>`, although the ACLs are correctly applied on the switch.

Scenario: If the switch is configured for User-Based 802.1X Authentication, when a subsequent user is authenticated on the same port where another user is already authenticated with RADIUS applied ACLs, the RADIUS applied ACLs on the port are not properly displayed in the output of the CLI command `show access-list radius <PORT-LIST>`.

Workaround: Use CLI command `show port-access authenticator clients <PORT-LIST>` detailed to verify the RADIUS ACL are correctly applied for authenticated users.

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 spanning 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.

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 and IP address from the DHCP server.

Workaround: Configure the DHCP client network interface to used 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 already registered in the switch DHCP Snooping binding database before the existing lease expires.

Workaround:

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 <…>`.

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.

Loop Protection

CR_0000189604 Symptom: Loop protection on the 2620 and 2530 incorrectly forwards traffic out of Smartlink ports.

Scenario: Configuring loop protection on the 2620 or the 2530 may result in traffic being forwarded out of Smartlink ports.

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.

Smart Link

CR_0000190943 Symptom: In a stacking configuration, all the switches connected to smartlink are unreachable.

Scenario: Create two smartlink groups with two different VLANs and assign IP to the VLAN.

vlan 2: port 1 (Master) and port 23(Slave) and
vlan 3: port 2 (Master) and port 24(Slave)

Now, disable the master port and ping the switch connected to the slave port. The ping fails.

Workaround: Make sure the ports in the second smartlink group are not in the range of the first smartlink group. (for example, if smartlink group 1 is created with ports 1 and 10 the smartlink should not have any ports in the rage 1-10).

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.

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.

Trunking

CR_0000189776 Symptom: While rebooting, the switch might prompt the user to save configuration when no new changes have been made to the running configuration (for example, `Do you want to save current configuration`).

Scenario: When trunks are configured in the startup configuration file, the switch indicates a mismatch between the startup (saved) and the running configuration (for example, `show config stat`) even though no changes have been made to the switch running configuration. On attempting to reboot the switch, the switch incorrectly prompts to save the running configuration.

Version A.15.16.0012m

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`.

Version A.15.16.0011

ARP

CR_0000177676 Roaming MAC addresses are not always properly relearned on certain MAC-move events.

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.

DHCP

CR_0000170807 The switch could crash when 'display this' is applied under the dhcp-server pool configuration mode with an error message similar to `Software exception at hwBp.c:218 -- in 'fault_handler'`.

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_0000155327 Slot crashes are logged as **Warning** rather than **Major** events.

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.

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.

CR_0000180767 The address manager always tries to log MAC moves using identical values for prior and current port numbers because of a typo. The logger detects such inconsistency and ignores the request.

Menu Interface

CR_0000179336 An `Invalid value` error message is received while switching from DHCP/Bootp to Manual IP address configuration via the Menu without editing the current IP address configured on a VLAN interface which already has a DHCP IP address.

MLD

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

Port Security

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

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`.

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.

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 A.15.16.0010

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`.

Switch Initialization

CR_0000163917 The switch can exhibit widely varying ping reply times ranging from less than 1 msec up to 25-30 msec.

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 A.15.16.0009

BPDU Protection

CR_0000153533 If the switch receives BDPU config information with missing ‘Forwarding’ or ‘Version’ details, it incorrectly treats the message as a valid BDPU, resulting in spanning tree instability.

CLI

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

CR_0000159271 In some configuration contexts (for example, IP-access list and VLAN), the IPv4 CLI commands (such as `IP source-lockdown`) are actually configuring the feature for IPv6.

CR_0000163219 After issuing the CLI command clear statistics global, two problems might appear in the output of `show interface ethernet <port ID>`:

1. The values of Bytes Rx and Bytes Tx are no longer displayed as comma-separated values. This applies to counter values from 2,147,483,647 through 4,294,967,295. Other counters than the number of bytes sent and received also appear to be affected by the same display issue (for example, Unicast counters and Deferred Tx).
2. After entering clear stat global, the format of the output of `show interface ethernet <port>` shifts two places. The missing space might appear at Giant Rx – Late Collisions, but where the space is added can differ.

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_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_0000168119 Switch may crash in an unknown state over a very long period when a rare set of Web operations occur.

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`.

DHCP Snooping

CR_0000160884 When DHCP-snooping is enabled, if any ports are configured as untrusted, DHCP packets are sent to those ports.

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.

IPv6

CR_0000167682 The security feature "IP Source Lockdown" is not operating correctly and disrupts IPv6 traffic. This same feature can't be consistently and reliably disabled as expected. This CR includes two issues:

1. IPv4 ip source-lockdown on a port blocks IPv6 traffic in VLANs that do not have IPv4 DSNOOP enabled.
2. When removing the configuration by disabling 'no ip source-lockdown' globally and then removing the feature from the ports 'no ip source-lockdown 11.13', the feature does not seem to be removed correctly and keeps blocking IPv6 traffic.

This issue occurs when both DIPLD and DIPLDv6 are enabled.

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 does 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.

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.

Security Vulnerability

CR_0000162428 If the CLI command `verify signature flash [primary]` or `[secondary]` is issued more than once, it shows inconsistent results though the signature has already been verified.

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

SFTP

CR_0000162987 Management modules go out of synchronization and fail to recover when large SFTP copies or a large number of SFTP copies are performed.

SSH

CR_0000171834 When logging in using Operator credentials for SSH and then executing the enable command with Manager credentials, the user name in the event log does not show the Manager username; it shows Operator mode.

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 A.15.16.0008

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.

Certificate Manager

CR_0000162594 When a TA certificate is present during boot up, the switch may hang/restart with the following error: `Software exception at certmgr_store.c:1921 -- in 'swInitTask`. Triggered when a corrupted certificate is present as TA certificate upon boot up. The system tries to double free and hangs.

CR_0000164093 When an IDEVID certificate is being used to establish TLS connections with a CNM server, the existing signature algorithm is updated from SHA-1 to DER, with new root certificate for the RA server.

CLI

CR_0000159808 When DHCPv6 Snooping is enabled and the switch has recorded a binding on a trunk, the output of the CLI command `show dhcpv6-snooping binding` displays the trunk ID as a + sign when the trunk ID exceeds four characters. For example, when a binding was learned on Trk11:

```
MAC Address IPv6-Address VLAN Port Time Left
------------ -------------- ---- ---- ---------
f0921c-2312c0 2001::82 1 + 5565
```

CR_0000163218 The output of the CLI command `show interface ethernet <interface>` becomes misaligned when the value of `Total Rx (bps)` reaches 100,000,000. When the 9th digit is added to the value of Total Rx, the adjacent line in the output (`Total Tx (bps)`) is shifted one column farther.

Crash

CR_0000170037 When a minimum TLS cipher suite version is enforced and a client negotiates a cipher suite, the switch might crash due to a watchdog timer expiry. The crash message may be similar to the following: `Software exception at bsp_interrupts.c:90 -- in 'fault_handler'`.

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.

Version A.15.16.0007

Version A.15.16.0007 was never released.

Version A.15.16.0006

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.

Certificate Manager

CR_0000159204 When a self-signed certificate is generated on the CLI, the certificate does not contain a valid start and end-date. This causes the certificate to be invalid, which causes problems

establishing HTTPS sessions or using syslog over TLS. When the self-signed certificate is generated in the web interface, this problem does not occur.

CLI

CR_0000156237 When a user has enabled Spanning Tree on 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.

Config

CR_0000145221 When a user enables Meshing, the software prompts the user to save the configuration and reboot the system. However, after saving the configuration, issuing the command to reboot the system causes the software to issue the following redundant message: `Do you want to save current configuration [y/n/^C]?`

CPU Utilization

CR_0000158909 When the CLI command `show system chassislocate member <ID>` is issued on a stack of switches, the CPU utilization rises to 100%.

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_0000152463 When the syslog feature `logging notify running-config-change` is enabled, inserting a new module into the chassis or reloading a module can cause the system to run out of message buffers. Once the message buffer pool is depleted, the system crashes with the typical `no msg buffer or no resources available` crash messages. For example: `Software exception at alloc_free.c:533 -- in 'mChassCtrl', task ID = 0xa99f140 -> No msg buffer Software exception in ISR at btmDmaApi.c:436 -> ASSERT: No resources available!`

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'.`

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 overcurrent 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 will henceforth be rejected with the error `Invalid power value 0 deciWatts received from MED PD on port <port ID>`.

Memory

CR_0000152126 Every time a user issues the command `terminal width` or `terminal length`, 40 bytes are allocated in memory that are never freed.

Port Access

CR_0000158890 After disabling and re-enabling a port, the port may end up in a state where it has established link, but does not pass any traffic. This issue can occur only on systems that do not have MSTP enabled.

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 resets the access-level to the default `restricted`. Although it is expected behavior to default to `restricted` when the string `unrestricted` is not precisely matched, the software has been modified to allow the use of both lower and uppercase characters in the word `unrestricted` when parsing a downloaded configuration file.

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.

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.

Version A.15.16.0005

IP Directed Broadcast

CR_0000160297 The IP directed broadcast feature does not function properly.

Version A.15.16.0004

802.1X

CR_0000149780 Already-authenticated clients that send an EAPOL-Start message are de-authenticated by the switch. This situation happens if the client runs Windows Vista and later operating systems that are set to "include learning".

Authentication

CR_0000148832 A switch configured with RADIUS authentication for primary login, and local authentication for secondary login fails to use local authentication when RADIUS servers do not respond. In that situation, the switch console is not accessible to valid users.

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_0000152440 The output of `show tech all` halts while displaying `lmaDbUtil traverseLmaProfTbl` with the message `=== The command has completed with errors. ===`.

Configuration

CR_0000152757 After configuring `snmp-server host` on the Commander, stack member configuration files include two lines with SNMPv3 configuration.

CPU Utilization

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

Crash

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

CR_0000150015 With DHCP snooping enabled, the switch might go into a continual boot cycle, with messages similar to `Health Monitor: Misaligned Mem Access HW Addr=0x0fc7ae2e IP=0x465ecf4 Task='eDrvPoll' Task ID=0xe0e2380 fp: 0x0685b4d4 sp:0x0685b4a0cpsr: 0x6000001f dfsr: 0x00000001.`

CR_0000153386 When a large number of 802.1X clients are 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_0000154053 When the switch has 802.1X-authenticated clients on a VLAN and the user deletes that VLAN, the switch might reboot unexpectedly with a message similar to `Software exception at multMgmtUtil.c:151 -- in 'eChassMgr', task ID = 0x3c945800 -> Internal error.`

CR_0000154769 With a static IGMP group configured, after issuing the `show run` command, changing the sFlow configuration might cause the switch to reboot unexpectedly with a message similar to `Health Monitor: Restr Mem Access HW Addr=0x60630015 IP=0x1045630 Task='mSnmpCtrl' Task ID=0xa98b4c0 sp:0x47ecc50 lr:0x104a0ac msr: 0x02029200 xer: 0x20000000 cr: 0x48000400.`

File Transfer

CR_0000145212 Software downloads via SSL fail with certain browsers, including Internet Explorer versions 7, 8, and 10.

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.

IGMP

CR_0000128678 In certain topologies the IGMPv2 "Leave Group" from one host can cause the multicast stream to be dropped, even though there are other hosts receiving that stream.

IP Phones

CR_0000137652 An IP phone that uses the "Automatic Port Synchronization" feature loses its IP address and possibly drops the current call. This has been observed when the switch is configured with the command `cdp mode pre-standard-voice`, and the PC to which the phone is connected goes into hibernation. In that situation the "Automatic Port Synchronization" feature causes the phone to drop and then re-establish link with the switch.

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

IPv6

CR_0000148594 IPv6 router advertisements that indicate an off-link prefix are not set as "preferred" in the switch, which causes incorrect information in the output of `show ipv6`, and can affect connectivity to hosts that use IPv6 Stateless Address Autoconfiguration. This issue also causes the sFlow "Agent Address" to be listed as 0.0.0.0.

Logging

CR_0000146773 In an IPv4 plus IPv6 environment, upon switch bootup the event log displays the set of source IP policy ("srcip") messages twice. With this fix, IPv6 policy messages are distinguished from IPv4 policy messages.

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.

Management

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

PoE

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

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

sFlow

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

CR_0000145712 sFlow statistics show a high rate of drops with moderate traffic levels.

CR_0000147660 In an IPv6-only environment with Stateless Address Autoconfiguration, sFlow incorrectly uses the link-local address as the agent ID.

SNMP

CR_0000131055 The MIB object `hpicfDownloadTftpConfig(1.3.6.1.4.1.11.2.14.11.1.3.5)` in switch software has a value of 1 for enabled and 2 for disabled, but the reverse is actually correct. With this fix the MIB object to enable and disable the TFTP client on the switch is changed to `hpicfDownloadTftpClientConfig(1.3.6.1.4.1.11.2.14.11.1.3.12)`. Also, the integer values are corrected so 1 is disabled and 2 is enabled.

CR_0000149657 When using the **createAndWait** mode to set parameters via SNMP, multiple RADIUS servers cannot be configured.

CR_0000151035 The switch incorrectly reports that MIB object `entPhysicalIsFRU = False` for removable fantrays, power supplies, and transceivers.

Switch Hang

CR_0000154152 If the switch is sending output to the console at the time the switch is rebooted, the switch might hang and not boot properly.

Web Management

CR_0000149099 When Spanning Tree Protocol (STP) is enabled via the Web user interface, "mstp" is shown as the default STP mode, and "mstp" is displayed as the operational mode after the user enables STP and saves the change. However, the command line interface shows that the switch operates in "rpvst" mode.

Workaround: From the Web user interface, use the dropdown menu to explicitly select "mstp" from the dropdown options, then save the change.

Issues and workarounds

The following are known issues in the A.15.16.0014m release.

Certificate Manager

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

Upgrade information

Upgrading restrictions and guidelines

A.15.16.0014m uses BootROM J.14.08. 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 Access Security Guide A.15.16*
- *HP Switch Software Advanced Traffic Management Guide A.15.16*
- *HP Switch Software Basic Operation Guide*
- *HP Switch Software IPv6 Configuration Guide A.15.16*
- *HP Switch Software Management and Configuration Guide A.15.16*
- *HP Switch Software Multicast and Routing Guide A.15.16*

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**

Website	Link
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.