YA/YB.15.18.0006 Release Notes

Abstract

This document contains supplemental information for the YA/YB.15.18.0006 release.

Acknowledgments

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

Contents

1 YA/YB.15.18.0006 Release Notes

Description

This release note covers software versions for the YA/YB.15.18 branch of the software.

Version YA/YB.15.18.0006 is the initial build of Major version YA/YB.15.18 software. YA/YB.15.18.0006 includes all enhancements and fixes in the YA/YB.15.17.0003 software, plus the additional enhancements and fixes in the YA/YB.15.18.0006 enhancements and fixes sections of this release note.

Product series supported by this software:

- HP 2530 Switch Series

Important information

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

Version history

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

Version number	Release date	Based on	Remarks
YA/YB.15.18.0006	2015-08-15	YA/YB.15.17.0003	Initial release of the YA/YB.15.18 branches. Released, fully supported, and posted on the web.
YA/YB.15.17.0007	2015-06-22	YA/YB.15.17.0006	Please see the YA/YB.15.17.0007 release note for detailed information on the YA/YB.15.17 branches. Released, fully supported, and posted on the web.
YA/YB.15.17.0006	2015-06-16	YA/YB.15.17.0005	Released, fully supported, and posted on the web.
YA/YB.15.17.0005		YA/YB.15.17.0004	Never released.
YA/YB.15.17.0004	2015-04-23	YA/YB.15.17.0003	Released, fully supported, but not posted on the web.
YA/YB.15.17.0003		YA/YB.15.16.0004	Initial release of the YA/YB.15.17 branches. Never released.
YA/YB.15.16.0009	2015-06-16	YA/YB.15.16.0008	Please see the YA/YB.15.16.0009 release note for detailed information on the YA/YB.15.16 branches. Released, fully supported, and posted on the web.
YA/YB.15.16.0008	2015-04-17	YA/YB.15.16.0007	Released, fully supported, and posted on the web.
YA/YB.15.16.0007	n/a	YA/YB.15.16.0006	Never released.
YA/YB.15.16.0006	2015-02-06	YA/YB.15.16.0005	Released, fully supported, and posted on the web.

Version number	Release date	Based on	Remarks
YA/YB.15.16.0005	2014-11-21	YA/YB.15.16.0004	Released, fully supported, and posted on the web.
YA/YB.15.16.0004	2014-10-30	YA/YB.15.15.0006	Initial release of the YA/YB.15.16 branches. Released, but never posted on the web.

Products supported

This release applies to the following product models:

Product number	Description
J9783A	HP 2530-8 Switch
J9782A	HP 2530-24 Switch
J9781A	HP 2530-48 Switch
J9777A	HP 2530-8G Switch
J9776A	HP 2530-24G Switch
J9775A	HP 2530-48G Switch
J9780A	HP 2530-8-PoE+ Switch
J9779A	HP 2530-24-PoE+ Switch
J9778A	HP 2530-48-PoE+ Switch
J9774A	HP 2530-8G-PoE+ Switch
J9773A	HP 2530-24G-PoE+ Switch
J9772A	HP 2530-48G-PoE+ Switch
JL070A	HP 2530-8-PoE+ Internal Power Supply Switch
J9856A	HP 2530-24G-2SFP+ Switch
J9855A	HP 2530-48G-2SFP+ Switch
J9854A	HP 2530-24G-PoE+-2SFP+ Switch
J9853A	HP 2530-48G-PoE+-2SFP+ 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

Operating System	Supported Web Browsers
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 for hardware products

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
J9856A	HP 2530-24G-2SFP+ Switch	YA.15.15.0006
J9855A	HP 2530-48G-2SFP+ Switch	YA.15.15.0006
J9854A	HP 2530-24G-PoE+-2SFP+ Switch	YA.15.15.0006
J9853A	HP 2530-48G-PoE+-2SFP+ Switch	YA.15.15.0006
J9783A	HP 2530-8 Switch	YB.15.12.0006
J9782A	HP 2530-24 Switch	YB.15.12.0006
J9780A	HP 2530-8-PoE+ Switch	YB.15.12.0006
J9779A	HP 2530-24-PoE+ Switch	YB.15.12.0006
J9781A	HP 2530-48 Switch	YA.15.12.0006
J9778A	HP 2530-48-PoE+ Switch	YA.15.12.0006
J9777A	HP 2530-8G Switch	YA.15.12.0006
J9774A	HP 2530-8G-PoE+ Switch	YA.15.12.0006
J9776A	HP 2530-24G Switch	YA.15.10.0003
J9775A	HP 2530-48G Switch	YA.15.10.0003
J9773A	HP 2530-24G-PoE+ Switch	YA.15.10.0003
J9772A	HP 2530-48G-PoE+ Switch	YA.15.10.0003

Enhancements

This section lists enhancements found in the YA/YB.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 YA/YB.15.18.0006

IP Directed Broadcast

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.

Routing

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

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. 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 YA/YB.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.

Autentication

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_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_0000160089 When a non-HP transceiver is inserted into the switch, the software will generate an error message in order to alert the user. This error message contained a spelling mistake, which has been corrected:

```
0533 FFI: port 27 is not a HP HP transceiver. Please go to:
www.hp.com/rnd/device_help/2_inform for more info.
```

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.

Counters

CR_0000141119 The output of `show ip counters` is incorrect when routing is enabled for IP, IPv6, or multicasts.

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_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:0x0685b4a0 cpsr: 0x6000001f dfsr: 0x00000001`.

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_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 HP 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.

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.

Flow Control

CR_0000169712 When flow-control is enabled, or enabled and then disabled, it erroneously causes a BDPU starvation condition. Symptoms include multiple BDPU starvation messages in the log, the switch declaring itself ROOT, unblocking of any blocked ports, and layer 2 loops

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.

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.`

MDI

CR_0000162682 The ports on the 2530 and 2530G series switches have the MDI and MDIX bits reversed. When a port is configured to use MDI, it will use MDIX, and vice versa. This will result in ports linking up, or not linking up, contrary to expectations.

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.

MSTP

CR_0000169263

PVST BPDUs are forwarded out of MSTP blocked ports when running YB.15.14.xxxx, YB.15.15.xxxx, YB.15.16.xxxx or YB.15.17.xxxx configured for MSTP with a redundant link in blocking state and a neighbor configured with RPVST.

Packet Buffers

CR_0000170693 Enabling HP 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.

PoE

CR_0000155423 POE functionality on all ports is shutting down and staying shut-down. The PoE "Detection Status" field indicates "Disabled." To recover, a reboot/power cycle/manual reset of the ports via software is required. The issue is only on 2530-24G-PoE+ SKU.

Port Connectivity

CR_0000161235 When a Gigabit transceiver is inserted in one of the uplink port bays and the switch is rebooted, after the reboot the adjacent copper port will no longer establish link at 100Mbps speeds. For example, when the transceiver is inserted into port 51, Ethernet port 49 will no longer establish link at 100Mbps. When the transceiver is inserted into port 52, the problem will occur with port 50.

QoS

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_0000160655 Switches configured for routing: When a VACL is applied to VLAN *X*, if a host on VLAN *X* then pings the switch agent's IP address for VLAN *Y*, the agents response IP address is also applied to the VACL, and hosts will become unreachable.

Self Test

CR_0000159678 When the switch is rebooted a self test runs on the ports. During the self test Fast Ethernet ports come on-line for a brief moment when a loopback test is executed. Some attached link partners may attempt to negotiate link with the switch port at that time. When the link negotiation fails, the link partner will not establish link once the ports come on-line properly.

sFlow

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

SSH

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_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_0000152647 When IP stacking is enabled on a switch, the default MTU is lowered from 1500 to 1488 bytes by design. However, after enabling IP stacking the MTU of the Primary VLAN was not set to 1488 bytes and still used the default 1500 bytes. This resulted in communication problems with the IP address assigned to the Primary VLAN when packets larger than 1460 bytes had to be transmitted.

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-HP 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_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.

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

Memory

CR_0000172439 Using `copy command-output` *show tech all* "…" generates large files (>70MB) creating the potential for high memory usage which will impact switch performance during command execution. **Workaround:** Dump `show tech all` content via CLI in the terminal window, then use copy & paste to transfer offline or use the terminal logging system to capture the output.

PoE

CR_0000174858 When high voltage input (750 - 1000V) is detected on a PoE+ RJ port, a `bad FET` HW failure is triggered by the switch and affected ports are powered down.

Workaround: Rebooting or power cycling the switch should recover the PoE controller and re-enable the affected ports.

Routing

CR_0000174012 Applying BPG route-map with set "weight" while there is more than one path could result in possible system reboot or hang. **Workaround:** Apply BPG route-map with set "local-pref" instead of using set "weight".

Upgrade information

Upgrading restrictions and guidelines

YA/YB.15.18.0006 uses BootROM YA.15.17 or YB.15.07. 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.

Contacting HP

For additional information or assistance, contact HP Networking Support:

www.hp.com/networking/support

Before contacting HP, collect the following information:

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

HP security policy

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

- Fixes for security vulnerabilities are not documented in manuals, release notes, or other forms of product documentation.

- A Security Bulletin is released when all vulnerable products still in support life have publicly available images that contain the fix for the security vulnerability.

To find security bulletins:

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

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

www4.hp.com/signup_alerts

Related information

Documents

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

www/hp.com/support/manuals

- Enter your product name or number and click **Go**. If necessary, select your product from the resulting list.

- For a complete list of acronyms and their definitions, see *HP FlexNetwork Technology Acronyms*.

Related documents

The following documents provide related information:

- *HP Switch Software Access Security Guide YA/YB.15.18*

- *HP Switch Software Advanced Traffic Management Guide YA/YB.15.18*

- *HP Switch Software Basic Operation Guide*

- *HP Switch Software IPv6 Configuration Guide YA/YB.15.18*

- *HP Switch Software Management and Configuration Guide YA/YB.15.18*

- *HP Switch Software Multicast and Routing Guide YA/YB.15.18*

Websites

- Official HP Home page: www.hp.com

- HP Networking: www.hp.com/go/networking

- HP product manuals: www.hp.com/support/manuals

- HP download drivers and software: www.hp.com/networking/software

- HP software depot: www.software.hp.com

- HP education services: www.hp.com/learn

Documentation feedback

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