# YA/YB.15.17.0007 Release Notes


## Abstract

This document contains supplemental information for the YA/YB.15.17.0007 release.



HP Part Number: 5998-8456
Published: June 2015
Edition: 1

**Acknowledgments**

# Contents

# 1 YA/YB.15.17.0007 Release Notes

## Description

This release note covers software versions for the YA/YB.15.17 branch of the software.

Version YA/YB.15.17.0003 was the initial build of Major version YA/YB.15.17 software. YA/YB.15.17.0007 includes all enhancements and fixes in the YA/YB.15.16.0004 software, plus the additional enhancements and fixes in the YA/YB.15.17.0003 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.15.17.0007 | 2015-06-22 | YA/YB.15.17.0006 | Released, fully supported, and posted on the web. |
| YA/YB.15.17.0006 | n/a | YA/YB.15.17.0005 | Never released. |
| YA/YB.15.17.0005 | n/a | 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 | n/a | YA/YB.15.16.0004 | 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 branch. 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. |
| 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 YA/YB.15.16. Released, but never posted on the web. |
| YA/YB.15.15.0013 | 2015-06-16 | YA/YB.15.15.0012 | Please see the YA/YB.15.15.0013 release note for detailed information on the YA/YB.15.15 branch. Released, fully supported, and posted on the web. |
| YA/YB.15.15.0012 | 2015-04-17 | YA/YB.15.15.0011 | Released, fully supported, and posted on the web. |

| Version number | Release date | Based on | Remarks |
|---|---|---|---|
| YA/YB.15.15.0011 | n/a | YA/YB.15.15.0010 | Never released. |
| YA/YB.15.15.0010 | 2015-02-06 | YA/YB.15.15.0009 | Released, fully supported, and posted on the web. |
| YA/YB.15.15.0009 | 2015-01-07 | YA/YB.15.15.0008 | Released, fully supported, and posted on the web. |
| YA/YB.15.15.0008 | 2014-09-15 | YA/YB.15.15.0007 | Released, fully supported, and posted on the web. |
| YA/YB.15.15.0007 | 2014-06-26 | YA/YB.15.15.0006 | Released, fully supported, but not posted on the web. |
| YA/YB.15.15.0006 | 2014-03-19 | YA/YB.15.14.0002 | Initial release of YA/YB.15.15. Released, fully supported, and posted on the web for early availability. |

# Products supported

This release applies to the following product models:

| Product number | Description |
|---|---|
| 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 |

| Operating System | Supported Web Browsers |
|---|---|
| | Firefox 12 |
| Windows 7 | Internet Explorer 9, 10<br>Firefox 24<br>Chrome 30 |
| Windows 8 | Internet Explorer 9, 10<br>Firefox 24<br>Chrome 30 |
| Windows Server 2008 SP2 | Internet Explorer 8, 9<br>Firefox 24 |
| Windows Server 2012 | Internet Explorer 9, 10<br>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.15.17 branch of the software. Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

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

## Version YA/YB.15.17.0007

No enhancements are included in version YA/YB.15.17.0007.

## Version YA/YB.15.17.0006

No enhancements were included in version YA/YB.15.17.0006.

## Version YA/YB.15.17.0005

No enhancements were included in version YA/YB.15.17.0005.

## Version YA/YB.15.17.0004

### Configurable TLS

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

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

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

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

```
[no] tls application { web-ssl | openflow | syslog | tr69 | all }

lowest-version { tls1.0 | tls 1.1| tls 1.2 | default }

cipher { aes256-sha256 | aes256-sha | aes128-sha256 | aes128-sha |
des3-cbc-sha | ecdh-rsa-aes128-gcm-sha256}
```

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

## Version YA/YB.15.17.0003

### DLDP

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

### RADIUS

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

### TACACS

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

### Trust Anchor Certificates

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

## Fixes

This section lists released builds that include fixes. 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.15.17.0007

### File Transfer

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

## Version YA/YB.15.17.0006

### CLI

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

### Config

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

### Crash

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

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

### Display Issue

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

## Event Log

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

## 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.

## Link

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

## Logging

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

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

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

## 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_0000166717** Login is permitted with the default username Manager, even when the Manager username has been changed to a custom username.

## sFlow

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

## Stacking

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

## Transceivers

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

## Version YA/YB.15.17.0005

Version YA/YB.15.17.0005 was never released.

## Version YA/YB.15.17.0004

### CLI

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

### Crash

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

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

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

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

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

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

- Crash
- File transfer failure
- Loss of IP communication

**CR_0000169893** The switch reboots unexpectedly (crashes) if a user attempts to replace an ACL or QoS policy on multiple ports if an ACL or policy is already applied to some, but not all of the ports where the new ACL or policy is being applied.

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

### Logging

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

### Memory

**CR_0000168160, CR_0000169917** Switch may crash in an unknown state over a very long period when a rare set of CLI operations occur.

**CR_0000169918** Switch leaks a small amount of memory during initialization, which results in a reduced amount of available memory being reported by `show system`.

**CR_0000169919** Switch may crash in an unknown state over a very long period when a rare set of SNMP operations occur.

### RADIUS

**CR_0000167582** RADIUS client authentication succeeds even after maximum ACE rules (1024) have been reached.

### TFTP

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

## Version YA/YB.15.17.0003

### 802.1X

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

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

### Authentication

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

### CLI

**CR_0000145136** When the switch is configured with the **`console event critical`** setting, the event log output of `show tech all` lists only the critical events. With this fix, `show tech all` lists all event log entries.

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

**CR_0000160089** When a non-HP transceiver is inserted into the switch, the software generates an error message 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 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.

## CPU Utilization

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

## 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 might crash with the following message: `NMI event SW:IP=0x00147168 MSR:0x02029200 LR:0x00120f7c cr: 0x44000400 sp:0x04d60f30 xer:0x00000000 Task='mSess3' Task ID=0x4d59728.`

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

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

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

## Display Issue

**CR_0000140830** When **`terminal length`** is changed from the default of 24, the config file display is truncated, and the outputs of `show logging` and `show interfaces` might be interleaved in the output of `show tech all`.

## File Transfer

**CR_0000148584** A configuration file with a blank community name in the **`snmp-server host`** entry cannot be downloaded to the switch. Although the switch does not allow the **`snmp-server host`** entry to be configured with a blank community name, earlier software bugs might cause this condition.

## ICMP

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

## IPv6

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

## LLDP

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

## Logging

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

## 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 uses MDIX, and vice versa. This results 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 not forwarded by the switch, causing clients to be dropped from the multicast stream.

## Multiple Symptoms

**CR_0000151207** The switch experiences high CPU utilization while idle. Also, a continuous ping to the switch shows that after several pings with quick response there is a ping with much slower response. These symptoms affect only YB-software switches.

### 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 no longer establishes link at 100 Mbps speeds. For example, when the transceiver is inserted into port 51, Ethernet port 49 no longer establishes link at 100 Mbps. When the transceiver is inserted into port 52, the problem occurs with port 50.

## 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 agent's response IP address is also applied to the VACL, and hosts 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 might attempt to negotiate link with the switch port at that time. When the link negotiation fails, the link partner does not establish link once the ports come on-line properly.

## SNMP

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

**CR_0000156209** When a configuration file is downloaded to the switch in which the SNMP community name string for unrestricted access is something other than `unrestricted`, the software resets the access-level to the default `restricted`. Although it is expected behavior to default to

`restricted` when the string `unrestricted` is not precisely matched, the software has been modified to allow the use of both lower and upper-case characters in the word *unrestricted* when parsing a downloaded configuration file.

### 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.

### 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 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.

### Stacking

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

**CR_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 is not set to 1488 bytes and still **ussd** the default 1500 bytes. This results in communication problems with the IP address assigned to the Primary VLAN when packets larger than 1460 bytes had to be transmitted.

### Switch Hang

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

### 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.

# Upgrade information

## Upgrading restrictions and guidelines

YA/YB.15.17.0007 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.15.17*
- *HP Switch Software Advanced Traffic Management Guide YA/YB.15.17*
- *HP Switch Software Basic Operation Guide*
- *HP Switch Software IPv6 Configuration Guide YA/YB.15.17*
- *HP Switch Software Management and Configuration Guide YA/YB.15.17*
- *HP Switch Software Multicast and Routing Guide YA/YB.15.17*

## Websites

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

# Documentation feedback

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