

YA/YB.15.15.0010 Release Notes

Abstract

This document contains supplemental information for the YA/YB.15.15.0010 release.

HP Part Number: 5998-7706
Published: March 2015
Edition: 1



© Copyright 2015 Hewlett-Packard Development Company, L.P.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

Acknowledgments

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

Contents

| | |
|--|----|
| 1 YA/YB.15.15.0010 Release Notes..... | 6 |
| Description..... | 6 |
| Important information..... | 6 |
| Version history..... | 6 |
| Products supported..... | 7 |
| Compatibility/interoperability..... | 8 |
| Minimum supported software versions..... | 8 |
| Enhancements..... | 8 |
| Version YA/YB.15.15.0010..... | 8 |
| Configurable TLS..... | 8 |
| Version YA/YB.15.15.0009..... | 9 |
| Version YA/YB.15.15.0008..... | 9 |
| Version YA/YB.15.15.0007..... | 9 |
| Version YA/YB.15.15.0006..... | 9 |
| Audit Logging | 9 |
| Broadcast Storm | 9 |
| Debug Capability | 9 |
| Inactivity Timer | 9 |
| Interface Authentication | 9 |
| Job Scheduler | 10 |
| LMA | 10 |
| Password Length | 10 |
| Reporting | 10 |
| Syslog Messages | 10 |
| TLS | 10 |
| Fixes..... | 10 |
| Version YA/YB.15.15.0010..... | 10 |
| Accounting..... | 10 |
| Certificate Manager..... | 11 |
| CLI..... | 11 |
| Config..... | 11 |
| Crash..... | 11 |
| LLDP..... | 11 |
| MDI..... | 12 |
| Port Connectivity..... | 12 |
| Self Test..... | 12 |
| SSH..... | 12 |
| TFTP..... | 12 |
| Web Management..... | 12 |
| Version YA/YB.15.15.0009..... | 12 |
| ARP | 12 |
| Authentication | 12 |
| CLI | 13 |
| CPU Utilization..... | 13 |
| Config | 13 |
| Crash | 13 |
| File Transfer | 14 |
| ICMP | 14 |
| IP Communication | 14 |
| IP Phones..... | 14 |
| Memory..... | 14 |

| | |
|--|----|
| Multiple Symptoms..... | 14 |
| PoE..... | 14 |
| Redundant Management..... | 14 |
| Self Test..... | 14 |
| Smart Link..... | 14 |
| Spanning Tree..... | 15 |
| Stacking..... | 15 |
| Switch Hang..... | 15 |
| TACACS..... | 15 |
| Version YA/YB.15.15.0008 | 15 |
| 802.1X | 15 |
| CLI | 15 |
| Crash | 15 |
| Logging | 15 |
| Management | 15 |
| PoE | 15 |
| SNMP | 16 |
| Switch Hang | 16 |
| Web Management | 16 |
| Version YA/YB.15.15.0007..... | 16 |
| Authentication | 16 |
| Fault Finder | 16 |
| IP Phones | 16 |
| IPv6 | 16 |
| Logging | 16 |
| sFlow | 17 |
| Version YA/YB.15.15.0006..... | 17 |
| BPDU Protection | 17 |
| CLI | 17 |
| Counters | 17 |
| Crash | 17 |
| Display Issue | 18 |
| Fastboot | 18 |
| IGMP | 18 |
| IPv6 | 18 |
| Jumbo Frames | 18 |
| LLDP | 18 |
| MSTP | 18 |
| MAC Table | 18 |
| Mirroring | 18 |
| Multicast | 19 |
| RADIUS | 19 |
| SNMP | 19 |
| Stacking | 19 |
| Switch Hang | 19 |
| TELNET | 19 |
| TFTP | 19 |
| Web Management | 19 |
| Upgrade information..... | 19 |
| Upgrading restrictions and guidelines..... | 19 |
| Contacting HP..... | 20 |
| HP security policy..... | 20 |
| Related information..... | 20 |
| Documents..... | 20 |
| Websites..... | 21 |

Documentation feedback.....21

1 YA/YB.15.15.0010 Release Notes

Description

This release note covers software versions beginning with YA/YB.15.15.0006.

Version YA/YB.15.15.0006 was the initial release of Major version YA/YB.15.15 software.

YA/YB.15.15.0006 software was built from the same source as YA/YB.15.14.0002.

YA/YB.15.15.0006 includes all enhancements and fixes in YA/YB.15.14.0002 software, plus the additional enhancements and fixes in the YA/YB.15.15.0006 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 the 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.15.15.0010 | 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. |
| YA/YB.15.14.0011 | 2015-02-06 | YA/YB.15.14.0010 | Please see the YA/YB.15.14.0011 release note for detailed information on the YA/YB.15.14 branch. Released, fully supported, and posted on the web. |
| YA/YB.15.14.0010 | 2015-01-07 | YA/YB.15.14.0009 | Released, fully supported, and posted on the web. |
| YA/YB.15.14.0009 | 2014-09-15 | YA/YB.15.14.0008 | Released, fully supported, and posted on the web. |
| YA/YB.15.14.0008 | 2014-07-16 | YA/YB.15.14.0007 | Released, fully supported, but not posted on the web. |
| YA/YB.15.14.0007 | 2014-07-01 | YA/YB.15.14.0006 | Released, fully supported, and posted on the web. |
| YA/YB.15.14.0006 | 2014-04-01 | YA/YB.15.14.0002 | Released, fully supported, but not posted on the web. |
| YA/YB.15.14.0005 | n/a | | Never built. |
| YA/YB.15.14.0004 | n/a | | Never built. |

| Version number | Release date | Based on | Remarks |
|------------------|--------------|------------------|--|
| YA/YB.15.14.0003 | n/a | | Never built. |
| YA/YB.15.14.0002 | 2013-10-18 | YA/YB.15.13.0003 | Initial release of YA/YB.15.14, fully supported, and posted on the web for early availability. |
| YA/YB.15.13.0014 | 2014-11-17 | YA/YB.15.13.0013 | Please see the YA/YB.15.13.0014 release note for detailed information on the YA/YB.15.13 branch. Released, fully supported, and posted on the web. |
| YA/YB.15.13.0013 | 2014-09-15 | YA/YB.15.13.0012 | Released, fully supported, and posted on the web. |
| YA/YB.15.13.0012 | 2014-07-31 | YA/YB.15.13.0011 | Released, fully supported, but not posted on the web. |
| YA/YB.15.13.0011 | n/a | YA/YB.15.13.0010 | Never released. |
| YA/YB.15.13.0010 | n/a | YA/YB.15.13.0009 | Never released. |
| YA/YB.15.13.0009 | n/a | YA/YB.15.13.0008 | Never released. |
| YA/YB.15.13.0008 | 2014-05-29 | YA/YB.15.13.0006 | Released, fully supported, and posted on the web. |
| YA/YB.15.13.0007 | n/a | | Never built. |
| YA/YB.15.13.0006 | 2014-03-24 | YA/YB.15.13.0005 | Released, fully supported, but not posted on the web. |
| YA/YB.15.13.0005 | 2014-01-09 | YA/YB.15.13.0004 | Released, fully supported, and posted on the web. |
| YA/YB.15.13.0004 | 2013-09-04 | YA/YB.15.13.0003 | Released, fully supported, but not posted on the web. |
| YA/YB.15.13.0003 | 2013-07-02 | First release | Initial release of YA/YB.15.13, 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 |

| Product number | Description |
|----------------|-------------------------|
| J9773A | HP 2530-24G-PoE+ Switch |
| J9772A | HP 2530-48G-PoE+ Switch |

Compatibility/interoperability

Minimum supported software versions

| 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 released builds that include enhancements. Software enhancements are listed in reverse-chronological order, with the newest at the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier editions.

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

Version YA/YB.15.15.0010

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.15.15.0009

No enhancements were included in version YA/YB.15.15.0009.

Version YA/YB.15.15.0008

No enhancements were included in version YA/YB.15.15.0008.

Version YA/YB.15.15.0007

No enhancements were included in version YA/YB.15.15.0007.

Version YA/YB.15.15.0006

Audit Logging

CR_0000138477 Audit Logging. Audit logging captures information including date, time, and outcome of an event, user identity, event start and stop timestamps, firmware versions, and begin and end of self tests, and includes that information in event log messages. See the *Management and Configuration Guide* for your switch.

Broadcast Storm

CR_0000126535 Port Shutdown with Broadcast Storm. Adds the `fault-finder broadcast-storm` command, with the option to disable the port for a configurable interval when a broadcast storm is detected. See "Port Trunking" in the *Management and Configuration Guide* for your switch.

Debug Capability

CR_0000132845 Additional Debug Capability. This enhancement adds tracking to identify possible switch hang situations during switch boot.

Inactivity Timer

CR_0000128427 Web User Interface Inactivity Timer. This new configuration command enables the administrator to set the idle timeout for the Web user interface, and provides a session timeout page to the user when the Web user interface session ends. See the *Management and Configuration Guide* for your switch.

Interface Authentication

CR_0000142449 Disable Username Prompts For Management Interface Authentication. This option allows the user to provide only the Manager or Operator password when logging into the switch, without first being prompted for username. When set, this option applies only if the switch uses

default usernames for both Manager and Operator logins. See “Secure Shell (SSH)” in the *Access Security Guide* for your switch.

Job Scheduler

CR_0000140513 Job Scheduler. This feature provides a way for customers to schedule recurring commands or “jobs” on their switch. Customers can schedule any CLI command they would otherwise enter interactively, including commands to enable or disable ports, LEDs, and power over ethernet (PoE). Jobs can also be scheduled to be triggered by certain pre-defined events such as switch reboot. The only restriction on such commands is that they cannot prompt for user input. See the *Basic Operation Guide* for your switch.

LMA

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 *Access Security Guide* for your switch.

Password Length

CR_0000128426 Minimum Password Length. Adds a command to set the minimum password length for Manager, Operator, and Port-Access passwords. The minimum password length is enforced when passwords are added or updated. See the *Access Security Guide* for your switch.

Reporting

CR_0000139639 Task Usage Reporting. The task usage reporting feature provides the ability to collect and display CPU usage data (with a refresh rate of 5 seconds) of running tasks on the switch. See “Task Usage Reporting” in the *Management and Configuration Guide* for your switch.

Syslog Messages

CR_0000141040 Hostname In Syslog Messages. The switch can be configured to include its hostname as the source or “origin” for messages sent to a syslog server. See “Troubleshooting” in the *Management and Configuration Guide* for your switch.

TLS

CR_0000139306 Syslog Over TLS. This enhancement to the existing Syslog feature enables the use of the Transport Layer Security (TLS) protocol to deliver Syslog messages. For more information, see the *Management and Configuration Guide* for your switch.

Fixes

This section lists released builds that include fixes. Software fixes are listed in reverse-chronological order, from newest to oldest. Unless otherwise noted, each software version listed includes all fixes added in previous versions listed below.

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

Version YA/YB.15.15.0010

Accounting

CR_0000152920 When RADIUS or Syslog Accounting is configured, every time an Accounting Start or Stop message is sent to the Accounting Server, the switch generates an RMON event message that is logged in the Event Log and is sent as SNMP trap and Syslog message. The RMON

messages are also logged for every Accounting user-level instead of only the service starting and stopping.

Certificate Manager

CR_0000159204 When a self-signed certificate is generated in 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 in the CLI and configured a protocol version other than the default MSTP, the CLI Menu does not allow the user to modify Spanning Tree parameters. The menu indicates that the switch requires a reboot. When the switch is actually rebooted the same problem is present after the reboot.

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

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 print the following redundant message: Do you want to save current configuration [y/n/^C]?

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_0000155066 The switch might 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 might 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 runs out of space to store the file, the switch might eventually crash with the 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 is henceforth rejected with the error `Invalid power value 0 deciWatts received from MED PD on port <port ID>.`

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.

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.

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.

CR_0000161371 When the switch is booting, the Out-of-band-management (OOBM) port might fail to initialize during self-test, resulting in the following message: `Switch Chassis needs replacement at scheduled downtime`. This is a software error and not a genuine hardware failure.

SSH

CR_0000153145 When a user copies a large file from the switch to a server using the SFTP client on the switch, the file transfer might be prematurely interrupted because the session disconnects before the file transfer has been completed. When this occurs, the following message is recorded in the system's Event Log: `03311 sftp: AM1: User: SFTP connection failure while connecting from <ip address>`.

TFTP

CR_0000159058 When the switch is used as a 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 file 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 YA/YB.15.15.0009

ARP

CR_0000152907 When a user changes the value of the ARP Cache Timer, the new value is applied to new ARP entries, but not to the ARP entries that already existed when the timer value was modified.

Authentication

CR_0000153244 The switch ages out authenticated clients before the configured interval, and ages out those clients even if they are actively sending traffic. This affects only YB-software switches.

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.

CPU Utilization

CR_0000155359 Three-stack 3800 device CPU utilization went to 100% while configuring ARP protection for 4094 VLANs.

Config

CR_0000152418 Routing must be enabled before the Local Proxy-ARP feature can be configured, but when routing is removed from the config, the Local Proxy-ARP configuration is not removed.

Crash

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_0000151340 Compressed core file is corrupted.

CR_0000152930 After deleting the last of any configured Smart Link groups, the switch might reboot unexpectedly.

CR_0000153035 With MAC-based authentication and mixed-mode enabled on a port that has both authenticated and unauthenticated clients, a redundancy failover might cause the switch to reboot unexpectedly with a message similar to `Software exception at bttfHwSrcBasedVlan.c:263 -- in 'mAdMUpCtrl', task ID = 0x1fecc6c0 -> ASSERT: failed.`

CR_0000153231 When attempting to reauthenticate clients on a specific port, the switch might reboot unexpectedly with a message similar to `Software exception at sw_sem.c:1111 -- in 'mWebAuth', task ID = 0xdf0a600 -> Deadlock found!. This affects only YB-software switches.`

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_0000154602 The switch experiences a loss of free memory for failed PEAP-MSCHAPv2 MAC-based authentication requests. When memory is no longer available, the switch will reboot unexpectedly with a message similar to `Software exception at wma_peap.c:713 -- in 'mWebAuth', task ID = 0x1de85340 -> ASSERT: failed.`

CR_0000155538 Disabling and re-enabling a port configured for Web or MAC-authentication during client authentication might cause the switch to reboot unexpectedly with a message similar to `Health Monitor: Restr Mem Access HW Addr=0xb1ba0c1a IP=0x108682b8 Task='mWebAuth' Task ID=0x1de8c680 sp:0x12f98530 lr:0x10868664 msr: 0x0000b032 xer: 0x00000000 cr: 0x88000400.` This affects only YB-software switches.

CR_0000155604 When a CLI command is entered with a backslash as the last character and then the `repeat` command is issued, the switch might reboot unexpectedly with a message similar to `Task mSess1 encountered an exception.`

CR_0000155710 Sending an ICMPv6 echo request packet with multiple fragment headers to the switch causes an NMI crash.

CR_0000155750 When using MAC Authentication on the 2620, the following software exception might occur: `wma_client_sm.c:1646 -- in 'mWebAuth', task ID = 0x1de85380.`

CR_0000159294 Software exception at `arenal_chassis_slot_sm.c:3374 -- in 'eChassMgr'`, task ID = 0x13b21a40.

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.

IP Communication

CR_0000153645 The Dynamic ARP Protection feature incorrectly blocks communication on **trusted** ports and on VLANs that are not configured with the `arp-protect` command. This affects only YB-software switches.

IP Phones

CR_0000157298 If an IP phone sends the switch an invalid power value of zero watts in an LLDP-MED TLV, the switch log shows `PD Over Current` indication and the phone might continuously reboot. This has been observed with the Avaya 9641G IP phone.

Memory

CR_0000152126 Issuing the `terminal length` or `terminal width` command causes a small loss of free memory.

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 shuts down and stays 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 occurs only on 2530-24G-PoE+ SKU. This affects only the YA software switches.

Redundant Management

CR_0000156759 After redundancy switchover with boot command when modules have not finished booting, an internal buffer might become corrupted. This could possibly lead to a crash.

Self Test

CR_0000159179 Boot time might take longer on a module with no transceivers present.

Smart Link

CR_0000152346 Upstream switches do not flush the MAC and ARP entries after a Smart Link switchover.

CR_0000152422 After deleting the active Master port from a Smart Link group, the Slave port takes over but does not send flush packets.

CR_0000152432 When Spanning Tree is enabled after Smart Link is configured, the Smart Link ports incorrectly take part in Spanning Tree.

Spanning Tree

CR_0000135741 Spanning Tree BPDUs received by the switch are forwarded even when Spanning Tree Protocol is enabled on the switch.

CR_0000155691 VLANs are not mapped to STG 1 when spanning-tree is disabled on 2530yb device. This affects only YB-software switches.

Stacking

CR_0000152647 When configured for IP Stacking, the commander or stack member does not respond to packets that are 1461 bytes or greater.

Switch Hang

CR_0000154477 Attempting to apply a 32-character **local-mac profile** name to a 32-character **local-mac mac-group** name causes the switch to become unresponsive, requiring a reboot to recover.

TACACS

CR_0000155541 TACACS authentication is not working with encrypted credentials in FIPS devices.

Version YA/YB.15.15.0008

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".

CLI

CR_0000152440 The output of `show tech all` halts while displaying `lmaDbUtil traverseLmaProfTbl`, with the message `=== The command has completed with errors. ===`.

Crash

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`.

Logging

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_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.

SNMP

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 `entPhysicalsFRU = False` for removable fantrays, power supplies, and transceivers.

CR_0000152809 The switch accepts incorrect values in an SNMPv1 query, instead of generating an error message.

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.

CR_0000154477 Attempting to apply a 32-character local-mac profile name to a 32-character local-mac mac-group name causes the switch to become unresponsive, requiring a reboot to recover.

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.

Version YA/YB.15.15.0007

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.

Fault Finder

CR_0000147935 The switch fault-finder feature does not disable a port in response to link flapping, although it is configured to do so.

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 for IP phones to use MAC authentication and for PCs to use 802.1X authentication.

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.

sFlow

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

Version YA/YB.15.15.0006

BPDU Protection

CR_0000144148 If VLAN 1 is not enabled on the link between a switch running rapid PVST and a switch running any Spanning Tree version, a rapid PVST switch configured for BPDU protection does not shut down the port when it receives a BPDU from the neighboring switch. However, the BPDUs are correctly dropped.

CLI

CR_0000143577 The switch allows users to configure a 1000BASE-T port with the setting `speed-duplex 1000-full`, which is not a valid setting for 1000BASE-T ports according to the IEEE spec.

Counters

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

CR_0000142065 After issuing the command `clear statistics global`, the output of `show interfaces <portlist> hc` displays some of the counters in hexadecimal.

CR_0000142198 When a trunk configured for sFlow polling is simultaneously queried via SNMP, all counter values for the trunk are zero.

CR_0000143860 On a switch configured with rapid PVST and BPDU protection, the output of the command `show spanning-tree bpdu-protection` shows zero errant BPDUs received, even when the switch has disabled a port due to receiving a BPDU. This is a display issue only, both rapid PVST and BPDU protection function properly.

CR_0000147144 The "Unknown Protos" counter incorrectly reports the same value as "Bytes Tx". This display issue affects only YB-software switches.

Crash

CR_0000142238 From the menu, after selecting "Status and Counters" and "Port Address Table" for an active port, the switch might reboot unexpectedly with a message similar to `Read Error Restr Mem Access HW Addr=0x2020201c IP=0x4ee7ce8 Task='mSess1' Task ID=0xe087cc0 fp: 0x06cefc48 sp:0x06cefc20 cpsr: 0x2000001f dfsr: 0x00000005`.

CR_0000144879 The switch might reboot unexpectedly in these situations:

1. The switch is running 15.08 or earlier software, is configured to drop frames that have a destination address of `01:00:0c:cc:cc:cd`, and has PVST filtering or PVST protection enabled. Then the switch is updated to 15.09 or later software.
2. The switch is running 15.09 or later software, is configured to drop frames that have a destination address of `01:00:0c:cc:cc:cd`, and then PVST filtering or PVST protection is enabled.

The switch reboots unexpectedly with a message similar to `Software exception at bttfLearn.c:2616 -- in 'mLpmgrCtrl', task ID = 0xa98a9c0 -> Mac Table Error`.

CR_0000146306 The switch uses TCP connections internally for inter-process communication. In a situation where an internal loopback TCP socket pair receives stimulus after an extended period of idle time, the switch might reboot unexpectedly with a message similar to `NMI event`

SW:IP=0x00e20c1c MSR:0x02029200 LR:0x00e077d0 cr: 0x44000400
sp:0x02b03c58 xer:0x00000000 Task='InetServer' Task ID=0xab31000.

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`.

Fastboot

CR_0000141043 If the fastboot setting is changed by the user, and the switch experiences a power interruption or reboot while the new setting is being written to flash, upon bootup the MAC address on a switch or stack member might be erased. Note that this fix has a side effect: If the fastboot setting is changed by the user and the switch software is downgraded (changed to an earlier version), upon bootup the fastboot setting might revert to what it was before the user-initiated change, even though the switch reports that it has been changed. Workaround: Change the fastboot setting twice - first change it back to what it was before the user-initiated change, then change fastboot to the desired setting.

IGMP

CR_0000138408 Joins sent by clients in response to a Group Specific Query are not forwarded by the Querier, causing the clients to lose the stream.

CR_0000140514 After disabling IGMP forwarding on a port, multicast traffic incorrectly continues to flow from that port..

IPv6

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

Jumbo Frames

CR_0000143977 The switch might send untagged frames larger than 1518 bytes, which are dropped by network devices that do not have jumbo frames enabled. This affects only YB-software switches.

LLDP

CR_0000140297 The PortID information is truncated at 25 characters, in the output of `show lldp info remote-device`.

MSTP

CR_0000134194 With Spanning Tree enabled, configuring a live port as an `admin-edge-port` causes the output of `show run` to display a fixed path-cost for that port in the IST (for example, `spanning-tree instance ist 5 path-cost 20000`). Note that this is a display issue only, the switch uses the automatic path-cost based on the link speed.

MAC Table

CR_0000143371 A MAC table entry does not age out while there is traffic destined to the MAC address, even if no traffic is received from that MAC address.

Mirroring

CR_0000144479 After copying a config file from an external device to the switch and booting with that config, the output of `show monitor` does not display any of the configured Network Monitoring sessions.

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.

RADIUS

CR_0000138258 In some situations, the switch response to Change of Authorization and Disconnect Messages from the RADIUS server is sent from an incorrect source IP address, which the RADIUS server therefore ignores.

SNMP

CR_0000143599 The switch does not allow users to configure RMON alarms via SNMP. This issue was introduced with CR_0000112411.

CR_0000147370 After using SNMP to configure a RADIUS server on the switch, the switch does not allow a login until the switch is rebooted.

Stacking

CR_0000135643 With the default terminal size of 80x24, connecting to the stack commander via TELNET or SSH results in the list of stack member switches displayed below the command prompt, with each additional member overwriting the previous one, leaving only the last stack member visible to the user.

Switch Hang

CR_0000146247 With both authentication and accounting enabled, the switch might become unresponsive to management, requiring a reboot to recover.

TELNET

CR_0000142571 While a user is being authenticated by a RADIUS server, issuing the `show access-list radius all` command from a TELNET session might cause the TELNET session to hang.

TFTP

CR_0000143546 With sFlow sampling enabled on the uplink port, in some situations a TFTP transfer from the switch fails with the message `Error in sending file. Exceeded max number of retransmits.`

Web Management

CR_0000137933 When connecting to a switch via HTTPS across a slow link, after the user logs in the screen freezes and does not display the switch management page. This issue has been observed across a 512 kbps WAN link, using several different Web browsers.

Upgrade information

Upgrading restrictions and guidelines

YA/YB.15.15.0010 uses BootROM YA.15.17 or YB.15.06. 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 Manual Supplement for A.15.15, RA.15.15, WB.15.15, and YA/YB.15.15*
- *HP Switch Software Basic Operation Guide*
- *HP Switch Software Feature Index — Extended*

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.