WB.15.17.0007 Release Notes

Abstract

This document contains supplemental information for the WB.15.17.0007 release.

HP Part Number: 5998-8453a
Published: July 2015
Edition: 2

Acknowledgments

Contents

1 WB.15.17.0007 Release Notes

Description

This release note covers software versions for the WB.15.17 branch of the software.

Version WB.15.17.0003 was the initial build of Major version WB.15.17 software. WB.15.17.0003 includes all enhancements and fixes in the WB.15.16.0004 software, plus the additional enhancements and fixes in the WB.15.17.0003 enhancements and fixes sections of this release note.

Product series supported by this software:

- HP 2920 Switch Series

Important information

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

Version history

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

Version number	Release date	Based on	Remarks
WB.15.17.0007	2015-06-22	WB.15.17.0006	Released, fully supported, and posted on the web.
WB.15.17.0006	n/a	WB.15.17.0005	Never released.
WB.15.17.0005	2015-05-11	WB.15.17.0004	Released, fully supported, but not posted on the web.
WB.15.17.0004	2015-04-23	WB.15.17.0003	Released, fully supported, but not posted on the web.
WB.15.17.0003	n/a	WB.15.16.0004	Never released.
WB.15.16.0009	2015-06-16	WB.15.16.0008	Please see the WB.15.16.0009 release note for detailed information on the WB.15.16 branch. Released, fully supported, and posted on the web.
WB.15.16.0008	2015-04-17	WB.15.16.0007	Released, fully supported, and posted on the web.
WB.15.16.0007	n/a	WB.15.16.0006	Never released.
WB.15.16.0006	2015-02-06	WB.15.16.0005	Released, fully supported, and posted on the web.
WB.15.16.0005	2014-11-21	WB.15.16.0004	Released, fully supported, and posted on the web.
WB.15.16.0004	2014-10-30	WB.15.15.0006	Initial release of WB.15.16. Released, but never posted on the web.
WB.15.15.0013	2015-06-16	WB.15.15.0012	Please see the WB.15.15.0013 release note for detailed information on the WB.15.15 branch. Released, fully supported, and posted on the web.

Version number	Release date	Based on	Remarks
WB.15.15.0012	2015-04-17	WB.15.15.0011	Released, fully supported, and posted on the web.
WB.15.15.0011	n/a	WB.15.15.0010	Never released.
WB.15.15.0010	2015-02-06	WB.15.15.0009	Released, fully supported, and posted on the web.
WB.15.15.0009	2015-01-07	WB.15.15.0008	Released, fully supported, and posted on the web.
WB.15.15.0008	2014-09-15	WB.15.15.0007	Released, fully supported, and posted on the web.
WB.15.15.0007	2014-06-26	WB.15.15.0006	Released, fully supported, but not posted on the web.
WB.15.15.0006	2014-03-18	WB.15.14.0002	Initial release of WB.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
J9726A	HP 2920-24G Switch
J9728A	HP 2920-48G Switch
J9727A	HP 2920-24G-PoE+ Switch
J9729A	HP 2920-48G-PoE+ Switch
J9836A	HP 2920-48G-PoE+ 740W Switch

Compatibility/interoperability

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

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

Minimum supported software versions

NOTE: If your switch or module is not listed in the below table, it runs on all versions of the software.

Product number	Product name	Minimum software version
J9805A	HP 640 Redundant/External PS Shelf	WB.15.13.0003

Enhancements

This section lists enhancements found in the WB.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 WB.15.17.0007

No enhancements are included in version WB.15.17.0007.

Version WB.15.17.0006

No enhancements were included in version WB.15.17.0006.

Version WB.15.17.0005

No enhancements were included in version WB.15.17.0005.

Version WB.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.

`show interface` command

CR_0000166947 The option `smartrate` was added to the `show interface [ <PORT-LIST>]` command. This option is used to display port diagnostics on a Smart Rate port only. If the command is run on a non-Smart Rate port, a message similar to the following displays: `Port A1: This command is only applicable to Smart Rate ports. Syntax: show interface [ <PORT-LIST> ] smartrate`.

Version WB.15.17.0003

Counters

Per queue counters provide visibility into the performance of the egress queue for diagnostics and monitoring of QoS implementation. For more information, see the *HP Switch Software Advanced Traffic Management Guide*.

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*.

OpenFlow

Fully-flexible OpenFlow allows the switch to create resources such as matching tables, ACL, and so forth, to support requirements of SDN applications; only on v3 modules. For more information, see the *HP OpenFlow 1.3 Administrator Guide*.

Multi-VLAN per OpenFlow instance allows multiple VLANs to be supported in one OpenFlow instance. For more information, see the *HP OpenFlow 1.3 Administrator 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 WB.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 WB.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.

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.

OpenFlow

CR_0000170635 On the CLI, typing `openflow <tab>` shows the valid parameters and descriptions. The optional parameter `ip-control-table-mode` help text has been corrected to read `Include IP control table in the OpenFlow packet processing pipeline. [Deprecated]. Please see 'openflow instance <INSTANCE-NAME> pipeline-model.`

CR_0000170688 When enabling HP NetworkProtector on the VAN SDN Controller, the switch loses packet buffers until they are depleted and eventually the switch stops functioning and loses management access.

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.

Routing

CR_0000162176 Under stress conditions, the switch sometimes enters a state where it does not send an ARP to a particular destination and it becomes unreachable on the customer network. Workaround/Proof of issue: Initiate a ping from the switch to the unreachable destination to restore connectivity to that destination through this switch.

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 WB.15.17.0005

SDN

CR_0000171571 Heartbeat packets between Network Protector and switch are being malformed by the switch. This causes the Network Protector application to think the tunnel connection between the controller and switch is invalid.

Version WB.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.

Config

CR_0000167908 When stacking is enabled, Manager and Operator passwords are set, and mirror-port or switch-interconnect are configured, the output of the command `show running-config` displays garbage entries, instead of Operator and Manager password configuration.

Counters

CR_0000166949 The `show interfaces <port-list> hc` command does not display 64-bit counter values properly.

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_0000169054 Blade fails to boot after repeatedly inserting and removing it. This might cause a system crash with the failure message `Unable to initialize Fabric ASIC`.

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, CR_0000169923 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.

OOBM

CR_0000162497 When a sustained broadcast storm has erupted in the network, the OOBM interface may be affected. Using the OOBM interface to manage the switch in such circumstances may result in slow responses from the switch or the session may not be established at all.

Stacking

CR_0000168556 In a stacking environment, when a switchover takes place, if the slave is unable to send a message to the commander within 200 ms, it can crash a Line Card.

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 WB.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_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.

Command Authorization

CR_0000160066 The `listen-port help` command has changed:

Usage: `[no] listen-port <PORT-NUM>`

Description: Specify TCP the port on which the OpenFlow agent of the switch waits (listens) for incoming connections from a OpenFlow controller. Default port number is 6633.

The Description should be changed to read: Description: Specify the TCP port on which the OpenFlow agent of the switch listens for incoming connections from an OpenFlow controller. Default port number is 6633.

Config

CR_0000149526 Enabling stacking on a switch that has a trunk configured creates an invalid entry for the trunk in the config file. The resulting configuration file cannot be downloaded to the switch.

CPU Utilization

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

CR_0000153428 With high volumes of routed IPv6 traffic, switch CPU utilization might remain at high levels for long periods of time. This issue is most prevalent with v1 zl modules.

Crash

CR_0000146176 After receiving multiple route changes or route flaps in a short period of time, the switch might reboot unexpectedly with a message similar to `Software exception at krt.c:2134 -- in 'eRouteCtrl', task ID = 0xa9bc400 -> Routing Stack: Assert Failed.`

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.

CR_0000159764 Due to a semaphore deadlock with an unknown trigger, a switch may crash with a message similar to the following: `NMI event HW:IP=0x0151dec4 MSR:0x02029200 LR:0x0151e468 cr: 0x20000800 sp:0x02f01460 xer:0x20000000 Task='tDevPollRx' Task ID=0xaa28000.`

Crash Messaging

CR_0000153706 2920 Stack - boot-history and event log crash signature records do not report the same event. The event log entry looks more like a standard reboot message reported from commander to slave due to lack of communication.

Display Issue

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

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.

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.

OOBM

CR_0000157738 The `show oobm discovery` command sometimes indicates `Active Stack Fragment(local` only without `Active Stack Fragment(discovered)`, even if show stacking indicates both commander and member correctly with normal stacking connection.

After a stack in chain topology is split, the least commander fragment and the equal split standby fragment stays active until it discovers the other fragment is active over OOBM. If there is no OOBM connected, there are multiple active fragments or active commanders on the network.

OpenFlow

CR_0000151412 Following creation of a meter for OpenFlow, meter statistics for `duration_sec` and `duration_nsec` return incorrect values.

CR_0000151415 Querying the statistics of a port that is a member of an OpenFlow instance returns incorrect values for `duration_sec` and `duration_nsec`.

CR_0000163370 Violation of OpenFlow requirement that if the match field OXM_OF_IP_DSCP is used the ETH TYPE must be 0x0800 *or* 0x86dd.

PoE

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

Port Connectivity

CR_0000161856 If `ip igmp static-group <group-address>` is added to the switch configuration for any VLAN, then upon a warm or cold reboot of the switch, the switch does not establish a link on any Ethernet ports. This issue is also present on stand-alone 2920, with stacking disabled.

QoS

CR_0000162179 When attempting to remove a configuration line from a QoS policy, the switch returns `commit failed`. The customer cannot delete the line and has to reload the configuration to recover. Occurs when multiple policies are configured.

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.

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_0000154463 The 3800 is not sending the correct FRU and Physical Asset status to iMCv7 via SNMP when the SFP (J4858C) is installed in SFP ports 51 or 52. The iMC software is reporting FRU=No; Physical and Physical Asset=No. This improves the original SNMP fix (CR_0000151035).

CR_0000158713 When reading the MIB data for a PSU Product ID J number, the number displayed is truncated by one character.

CR_0000160352 The string value for the temperature sensor's instance of the object `entPhysicalName` (.1.3.6.1.2.1.47.1.1.1.1.7) is incorrectly set to `Chassis`. It should return `Chassis Temperature`.

SSH

CR_0000159714 The output of the `display device` command over SSH displays incorrectly as a misaligned single line of output due to no carriage returns between multiple lines. This occurs more frequently if the terminal width is set > 80 characters, when SSH senses the terminal settings on Login.

CR_0000165393 When the SSH client has a keepalive mechanism configured that requires a response from the SSH server on the switch, the SSH client 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.

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, 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_0000154380 A failover from Commander to Standby with multiple MSTP instances in operation might cause the stack members and connected devices to be unreachable.

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.

Trunking

CR_0000165004 If DT trunking keep-alive has been configured, and later the switch is rebooted, the ISC link between the DT pair becomes unstable, or goes down. Symptoms include blocked traffic, layer 2 loops, or duplicate packets. A temporary workaround for this issue is to reconfigure the DT keep-alive (but not reboot).

Web Management

CR_0000149777 After a 3800 series switch Stack Commander failover, the Web-management interface is not accessible via the Out of Band Management (OOBM) port.

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

Routing

CR_0000174881 The switch does not initiate an ARP request to the next hop IPv4 address for routed IPv4 traffic entering a VLAN that has an inbound Routed Access List (RACL) applied using the command `vlan vid ip access-group identifier in`.

As a result, the IPv4 routed traffic will not reach its destination because the switch did not create an ARP entry in the switch ARP Table for the next hop IPv4 address, which is required to route the traffic. The issue may be intermittent because there could be other sources trying to reach the same next hop IPv4 address, which will result in creating an ARP entry. Due to the ARP age-out time of 20 minutes, the issue may reoccur after 20 minutes. For example, if the routed IPv4 traffic also enters the switch via a VLAN that does not have inbound RACL or if you ping it from the affected switch. Pinging from the switch to the unreachable IPv4 destination address will temporarily resolve the reachability issue; however, the issue may reoccur after the APR age-out expires or after invoking the CLI command `clear arp`.

Example of an IPv4 inbound RACL configuration that could encounter this issue for packets routed through the switch:

```
ip access-list extended "102"
  10 permit ip 0.0.0.0 255.255.255.255 0.0.0.0 255.255.255.255
  exit
ip routing
ip route 0.0.0.0 0.0.0.0 192.168.0.1
vlan 10
  name "VLAN10"
  untagged A1
  ip access-group "102" in
  ip address 10.0.0.1 255.255.255.0
  exit
vlan 20
  name "VLAN20"
  untagged A2
  ip address 192.168.0.100 255.255.255.0
  exit
```

Upgrade information

Upgrading restrictions and guidelines

WB.15.17.0007 uses BootROM WB.15.05. 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 WB.15.17*
- *HP Switch Software Advanced Traffic Management Guide WB.15.17*
- *HP Switch Software Basic Operation Guide*
- *HP Switch Software IPv6 Configuration Guide WB.15.17*
- *HP Switch Software Management and Configuration Guide WB.15.17*
- *HP Switch Software Multicast and Routing Guide WB.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.