RA.15.14.0012 Release Notes

Abstract

This document contains supplemental information for the RA.15.14.0012 release.

HP Part Number: 5998-8034
Published: May 2015
Edition: 1

Acknowledgments

Contents

1 RA.15.14.0012 Release Notes

Description

This release note covers software versions for the RA.15.14 branch of the software.

Version RA.15.14.0002 was the initial release of Major version RA.15.14 software. RA.15.14.0002 software was built from the same source as RA.15.13.0003. RA.15.14.0002 includes all enhancements and fixes in RA.15.13.0003 software, plus the additional enhancements and fixes in the RA.15.14.0002 enhancements and fixes sections of this release note.

Product series supported by this software:

- HP 2620 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
RA.15.14.0012	2015-04-17	RA.15.14.0011	Released, fully supported, and posted on the web.
RA.15.14.0011	2015-02-06	RA.15.14.0010	Released, fully supported, and posted on the web.
RA.15.14.0010	2015-01-07	RA.15.14.0009	Released, fully supported, and posted on the web.
RA.15.14.0009	2014-09-15	RA.15.14.0008	Released, fully supported, and posted on the web.
RA.15.14.0008	2014-07-16	RA.15.14.0007	Released, fully supported, but not posted on the web.
RA.15.14.0007	2014-07-01	RA.15.14.0006	Released, fully supported, and posted on the web.
RA.15.14.0006	2014-04-01	RA.15.14.0002	Released, fully supported, but not posted on the web.
RA.15.14.0005	n/a		Never built.
RA.15.14.0004	n/a		Never built.
RA.15.14.0003	n/a		Never built.
RA.15.14.0002	2013-10-18	RA.15.13.0003	Initial release of RA.15.14, fully supported, and posted on the web for early availability.
RA.15.13.0014	2014-11-17	RA.15.13.0013	Please see the RA.15.13.0014 release note for detailed information on the RA.15.13 branch. Released, fully supported, and posted on the web.
RA.15.13.0013	2014-09-15	RA.15.13.0012	Released, fully supported, and posted on the web.
RA.15.13.0012	2014-07-31	RA.15.13.0011	Released, fully supported, but not posted on the web.

Version number	Release date	Based on	Remarks
RA.15.13.0011	n/a	RA.15.13.0010	Never released.
RA.15.13.0010	n/a	RA.15.13.0009	Never released.
RA.15.13.0009	n/a	RA.15.13.0008	Never released.
RA.15.13.0008	2014-05-29	RA.15.13.0006	Released, fully supported, and posted on the web.
RA.15.13.0007	n/a		Never built.
RA.15.13.0006	2014-03-24	RA.15.13.0005	Released, fully supported, but not posted on the web.
RA.15.13.0005	2014-01-09	RA.15.13.0004	Released, fully supported, and posted on the web.
RA.15.13.0004	2013-09-04	RA.15.13.0003	Released, fully supported, but not posted on the web.
RA.15.13.0003	2013-07-02	RA.15.12.0006	Initial release of RA.15.13, fully supported, and posted on the web for early availability.
RA.15.12.0016	2014-10-06	RA.15.12.0015	Please see the RA.15.12.0015 release note for detailed information on the RA.15.12 branch. Released, fully supported, but not posted on the web.
RA.15.12.0015	2014-03-17	RA.15.12.0014	Released, fully supported, and posted on the web.
RA.15.12.0014	2014-01-17	RA.15.12.0013	Released, fully supported, and posted on the web.
RA.15.12.0013	2013-11-20	RA.15.12.0012	Released, fully supported, but never posted on the web.
RA.15.12.0012	2013-11-05	RA.15.12.0011	Released, fully supported, but not posted on the web.
RA.15.12.0011	2013-10-10	RA.15.12.0010	Released, fully supported, but not posted on the web.
RA.15.12.0010	2013-08-28	RA.15.12.0008	Released, fully supported, and posted on the web.
RA.15.12.0009	n/a		Never built.
RA.15.12.0008	2013-06-25	RA.15.12.0007	Released, fully supported, but not posted on the web.
RA.15.12.0007	2013-03-25	RA.15.12.0006	Released, fully supported, but not posted on the web.
RA.15.12.0006	2013-02-28	First release	Initial release of RA.15.12, fully supported, but not posted on the web.

Products supported

This release applies to the following product models:

Product number	Description
J9623A	HP 2620-24 Switch
J9626A	HP 2620-48 Switch

Product number	Description
J9625A	HP 2620-24-PoE+ Switch
J9627A	HP 2620-48-PoE+ Switch
J9624A	HP 2620-24-PPoE+ Switch

Compatibility/interoperability

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

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

Enhancements

This section lists enhancements found in the RA.15.14 branch of the software. Software enhancements are listed in reverse-chronological order, with the newest on the top of the list. Unless otherwise noted, each software version listed includes all enhancements added in earlier versions.

NOTE: The number that precedes the enhancement description is used for tracking purposes.

Version RA.15.14.0012

No enhancements were included in version RA.15.14.0012.

Version RA.15.14.0011

No enhancements were included in Version RA.15.14.0011.

Version RA.15.14.0010

No enhancements were included in Version RA.15.14.0010.

Version RA.15.14.0009

No enhancements were included in Version RA.15.14.0009.

Version RA.15.14.0008

No enhancements were included in Version RA.15.14.0008.

Version RA.15.14.0007

Additional Debug Capability

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

Version RA.15.14.0006

No enhancements were included in Version RA.15.14.0006.

Version RA.15.14.0005

RA.15.14.0005 was never built.

Version RA.15.14.0004

RA.15.14.0004 was never built.

Version RA.15.14.0003

RA.15.14.0003 was never built.

RA.15.14.0002

All Task Core Dump

CR_0000140648 All Task Core Dump. The coredump file now includes all tasks that are operating when the switch crashes.

Certificate Manager

CR_0000115812 Certificate Manager. Certificate Manager enables Public Key Infrastructure (PKI) capability on the switch providing authentication of network entities. See "Certificate Manager" in the *Access Security Guide* for your switch.

Chassis Locate LED at Boot

CR_0000134999 Chassis Locate LED at Boot. The `chassislocate` command has an optional parameter that configures it to run in the future instead of immediately. See "Troubleshooting" in the *Management and Configuration Guide* for your switch.

DHCPv4 Snooping Max Binding

CR_0000129524 DHCPv4 Snooping Max Binding. DHCP snooping max-binding prevents binding entries from getting exhausted. This feature is on a per-port basis and restricts the maximum number of bindings allowed on a port/interface. The maximum bindings for a particular port includes both statically configured and dynamically learned. The number of bindings on a per port basis is incremented upon a lease offer and decremented upon a lease expiry or release. See "Port Security" in the *Access Security Guide* for your switch.

Download Software via DHCP

CR_0000129156 Download Software via DHCP. Adds the option to specify the location of switch software via DHCP.

Fan Information, and Link-Flap Options

CR_0000128236 Fan Information, and Link-Flap Options. Fan information is now included when displaying global system information. Also, the `fault-finder link-flap` command is added to detect unstable links that are constantly going up and down, and a new action of

`warn-and-disable` is added. See "Monitoring and Analyzing Switch Operation" and "Troubleshooting" in the *Management and Configuration Guide* for your switch.

FIPS Upgrade

CR_0000140539 FIPS Mocana 5.7 Upgrade. The internal security/cryptography code has been improved to prevent circumvention.

IPv6 QoS

CR_0000127640 IPv6 QoS. Enables the switch to mark matching TCP or UDP packets with an 802.1p priority. See "Quality of Service: Managing Bandwidth Effectively" in the *Advanced Traffic Management Guide* for your switch.

IPv6 QoS Setting

CR_0000127665 IPv6 QoS Setting. Adds IPv6 as an option for the qos device-priority command. See the *Advanced Traffic Management Guide* for your switch.

LACP-MAD

CR_0000127160 Link Aggregation Control Protocol-Multi-Active Detection. Link Aggregation Control Protocol-Multi-Active Detection (LACP-MAD) is a detection mechanism deployed by switches to recover from a breakup of the Intelligent Resilient Framework (IRF) stack due to link or other failure. See "Port Trunking" in the *Management and Configuration Guide* for your switch.

Loop Protection

CR_0000128607 VLAN-Based Loop Protection. VLANs can now be configured for loop protection. See "Multiple Instance Spanning Tree Operation" in the *Advanced Traffic Management Guide* for your switch.

Mismatch Log Messages

CR_0000127014 Filtering PVID Mismatch Log Messages. This enhancement filters out PVID mismatch log messages on a per-port basis. PVID mismatches are logged when there is a difference in the PVID advertised by a neighboring switch and the PVID of the switch port which receives the LLDP advertisement. However, if these events are logged too frequently, they can overwhelm the log buffer and push relevant logging data out of log memory, making it difficult to troubleshoot another issue. See "Troubleshooting" in the *Management and Configuration Guide* for your switch.

RADIUS Server Support

CR_0000128342 RADIUS Server Support. While a RADIUS-assigned client session is active on a given port, any RADIUS-imposed values are applied as shown in "RADIUS Server Support for Switch Services" in the *Access Security Guide* for your switch.

Rate Limiting

CR_0000135776 VLAN-Based Rate Limiting. This enhancement provides specific bandwidth for a specific VLAN for the ingress traffic on this VLAN. The specified VLAN drops all traffic that exceeds the configured rate. See "Port Traffic Controls" in the *Management and Configuration Guide* for your switch.

Smartlink

CR_0000131581 Smartlink. Smartlink is a switch feature that provides effective, simple and fast-converging link redundancy in network topology with dual uplink between different layers of the network. It requires an active (master) and a backup (slave) link. The active link carries the uplink traffic. Upon failure of the active link, a switchover is triggered and the traffic is directed to the backup link. See "Smartlink" in the *Advanced Traffic Management Guide* for your switch.

SNMP Trap

CR_0000135708 SNMP Trap When MAC Address Table Changes. This enhancement causes an SNMP trap to be generated once a laptop/PC is removed from the back of an IP phone and the laptop/PC MAC address ages out of the MAC table. See "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

Updated IGMP

CR_0000127927 Updated IGMP Type Numbers and Keywords. For an updated list of IGMP type numbers and keywords, see "RADIUS Server Support for Switch Services" in the *Access Security Guide* for your switch.

Zeroization Feature

CR_0000134260 Zeroization Feature. When using enhanced secure mode, several commands have differences from standard secure mode in their options or output. See "Secure Mode" in the *Access Security Guide* for your switch.

Fixes

Software fixes are listed in reverse-chronological order, from newest to oldest software version. Unless otherwise noted, each software version listed below includes all the software fixes and enhancements added in previous versions listed below.

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

Version RA.15.14.0012

802.1X

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

Authentication

CR_0000160903 802.1x clients re-authenticate even though no re-authentication has been configured, when the MAC AGE timer is configured to anything other than the default. The lower the MAC-age timer value set, the more frequently the re-authentication might occur.

Certificate Manager

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

CLI

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

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

1. The values of Bytes Rx and Bytes Tx are no longer displayed as comma-separated values. This applies to counter values from 2,147,483,647 through 4,294,967,295. Other counters

than the number of bytes sent and received also appear to be affected by the same display issue (for example, Unicast counters and Deferred Tx).

2. After entering `clear stat global`, the format of the output of `show interface ethernet <port>` shifts two places. The missing space might appear at Giant Rx – Late Collisions, but where the space is added seems can differ.

Crash

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.

PIM

CR_0000156038 The multicasts are flooded, causing a behavior equal to a broadcast storm, which causes high CPU utilization when pim-sparse neighbors are configured.

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_0000162789 There is a limit of 100 entries in a RADIUS ACL. When more than one RADIUS user on a port has an ACL, each user should have a 100 entry limit. However, clients get an error if the total of all clients is greater than 100. When this happens, the client is rejected and cannot access the network.

SSH

CR_0000165393 When the SSH client has a keepalive mechanism configured that requires a response from the SSH server on the switch, the SSH client will terminate the session after the first keepalive packet is transmitted. This happens because the switch drops the client's keepalive packet due to an incorrect packet length calculation.

This issue has been observed using an openSSH client with the ServerAliveInterval configured and the parameter 'want_reply' enabled.

SSL

CR_0000162587 SSL Security vulnerability due to 56 bit DES-CBC-SHA. Due to security vulnerability the cipher DES-CBC-SHA is now unavailable.

Stacking

CR_0000164406 If IP stacking is configured, and a user connects via browser to the stack commander via its (http) web management address and selects the drop down box to connect to a stack member, the user is not connected to the stack member and is returned back to the stack commander view instead.

Version RA.15.14.0011

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 enables 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 changes 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.

Crash

CR_0000149153 When an exceptionally large amount of IP Address Manager (IPAM) output is generated by the `show tech all` command 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 occur.

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 message: `Software exception at hwBp.c:218 -- in 'fault_handler', task ID = 0x3c403380 -> MemWatch Trigger: Offending task 'mftTask'.`

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.

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.

Version RA.15.14.0010

ACLs

CR_0000155581 2620 ACL duplicates permitted packets on the output port, on platforms that support L3 forwarding, have an ACL with 'permit' rules, and also have the 'log' keyword.

ARP

CR_0000152907 Changing the **ip arp-age** value should apply to existing ARP cache entries, but it does not.

CLI

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

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

Config

CR_0000145221 The switch prompts users to save the configuration when no changes have been made. This has been observed after configuring meshing, saving the config, and rebooting the switch.

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_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_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 reboots unexpectedly with a message similar to `Software exception at wma_peap.c:713 -- in 'mWebAuth', task ID = 0x1de85340 -> ASSERT: failed.`

CR_0000155359 Enabling the arp-protect command on 4094 VLANs causes CPU utilization to increase to 100%.

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.`

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 2620, the following software exception may occur: `wma_client_sm.c:1646 -- in 'mWebAuth', task ID = 0x1de85380`

CR_0000156908 A banner configured with more than 1048 characters causes the switch to go into a continuous "boot loop" when the switch is rebooted. The switch logs a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x54202800 IP=0x54202800 Task='swInitTask' Task ID=0xaa1a840 sp:0x2e288a0 lr:0x54202800 msr: 0x02029200 xer: 0x20000000 cr: 0x44000400.`

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 Directed Broadcast

CR_0000160297 The IP directed broadcast feature does not function properly.

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.

Meshing

CR_0000155857 Enabling meshing and then configuring IGMP, causes error message: `W 08/12/14 10:56:52 02413 igmp: Internal api IgmpInterface_getPortMode failed: bad port mode.`

Redundant Management

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

Self Test

CR_0000159179 Boot time might take longer on a modules 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.

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 encrypt credentials in FIPS devices.

Version RA.15.14.0009

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".

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.

Version RA.15.14.0008

Crash

CR_0000152222 With multiple authentication protocols active in a high-stress environment, the switch might reboot unexpectedly with a message similar to `NMI event HW:IP=0x0103191c MSR:0x02029200 LR:0x00121208 cr: 0x20000800 sp:0x02d56220 xer:0x20000000 Task='tDevPollRx' Task ID=0x2d3fc78.`

Version RA.15.14.0007

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. This fix was inadvertently omitted from the original RA.15.14.0007 fix list.

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. This fix was inadvertently omitted from the original RA.15.14.0007 fix list.

CLI

CR_0000142154 The output of `show tech` halts after displaying `show debug buffer`, 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`.

IPv6

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

Logging

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

CR_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.

sFlow

CR_0000142777 When sFlow is enabled, 802.1X authentication might fail, causing users to be randomly locked out of the network for 20 minutes.

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

SNMP

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.

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

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

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.

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 RA.15.14.0006

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_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.

Crash

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.

IP Phones

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.

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.

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.

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

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.

sFlow

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

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.

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`.

Transceivers

CR_0000143444 Software does not allow the dual-speed J8177C Gigabit-copper transceiver to be configured for 100 Mbps operation, responding with a message such as `Value auto-100 is not applicable to port A21`. This is the same fix as CR_0000132781 in 15.13.0003, which was inadvertently removed by CR_0000126473 in 15.13.0004 software.

Version RA.15.14.0005

RA.15.14.0005 was never built.

Version RA.15.14.0004

RA.15.14.0004 was never built.

Version RA.15.14.0003

RA.15.14.0003 was never built.

Version RA.15.14.0002

802.1X

CR_0000134257 After 802.1X frame counters reach a maximum value of 2,147,483,647, the counters are displayed as negative values that become smaller until they reach zero. When the counters reach zero, they begin incrementing again.

Accounting

CR_0000133762 If a Windows system is configured for both computer authentication and user authentication, accounting might not function properly.

Authentication

CR_0000134114 With both 802.1X and MAC Authentication configured on a port, it is possible for an already-authenticated client to be erroneously moved to the unauthenticated VLAN.

BootROM

CR_0000135159 This software version includes a BootROM update to BootROM version RA.15.11.

CLI

CR_0000136428 CLI output for `show ip igmp vlan x conf` displays a plus sign under the Interconnect Trunk column heading, and nothing (blank) under the Port column heading.

CR_0000137287 The output of `show run vlan <VLAN_ID>` omits the no in the configuration entry `no ip igmp fastleave`. Note that the output of show run gives correct information.

Config

CR_0000131054 Setting an operator or manager password on the switch causes four features to be disabled: auto run, DHCP-based config file download from an external tftp server, DHCP-based software image download from an external tftp server, and tftp server functionality within the switch.

With this fix, more accurate messages are sent regarding the specific features that are disabled by setting the operator or manager password.

CR_0000135481 After boot, a config file that has a trap destination community name with an open parenthesis "(" or a close parenthesis ")" cannot be downloaded to the switch.

CR_0000138447 After a switch software update, SNMP community access privileges are incorrectly changed by the switch. The output of `show snmp-server` and the output of a `"walkmib"` command give different results, and neither output represents how the switch actually behaves for Manager or Operator access. This issue was introduced with CR_0000122623; if the access settings were configured on a switch without the CR_0000122623 fix, after updating to software with the CR_0000122623 fix the settings are changed.

CR_0000139251 When a configuration file is downloaded to the switch, a default SNMPv3 user named "initial" is created on the switch even though it is not in the config file.

Crash

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

CR_0000127791 In a rare situation the switch might reboot unexpectedly with a message similar to `Software exception at rt_table.c:4453 -- in 'eRouteCtrl', task ID = 0xa9c4c00 -> Routing Stack: Assert Failed. This improves the original Crash fix (CR_0000120116).`

CR_0000137288 With SNTP configured, in a rare situation after a time update the switch might reboot unexpectedly with a message similar to `Health Monitor: Invalid Instr Misaligned Mem Access HW Addr=0x31352e30 IP=0x31352e30 Task='mDebugCtrl' Task ID=0x3c9558c0 sp:0x11f92cd0 lr:0x31352e31 msr: 0x02029200 xer: 0x00000000 cr: 0x28000800.`

CR_0000138879 After boot, a switch that has a syslog server and an IPv6 address configured might become unresponsive to management, and after a period of time the switch might reboot repeatedly with a message similar to `NMI event SW:IP=0x001517d4 MSR:0x02029200 LR:0x0015178c cr: 0x28000400 sp:0x03aae0e0 xer:0x00000000 Task='mDebugCtrl' Task ID=0xa9f8000.`

DHCP

CR_0000128754 If the switch is a DHCP client and the DHCP reply contains option 43 with sub-option codes that conflict with RFC 2132 options, the switch might use incorrect settings such as an incorrect subnet mask.

CR_0000137877 A switch acting as a DHCP relay agent sends two DHCP packets, one of which incorrectly has the source MAC address of the client instead of the switch.

Dynamic ARP Protection

CR_0000132073 When a VLAN is configured for dynamic ARP protection and also DHCP snooping, ARP packets should be forwarded but are incorrectly dropped when the `arp-protect` configuration does not include the `validate ip` option.

Event Log

CR_0000127436 After the switch uptime reaches 497 days, the timestamp entries in the event log become erratic with gaps of several hours or days. In some cases the timestamps revert to previous months and years, even though SNTP updates with those wrong timestamps report the correct date and time.

GVRP

CR_0000130090 After rebooting the switch, the configuration `unknown-vlans disable` does not work on trunks.

ICMP

CR_0000134682 The switch does not log an unsolicited ICMP reply unless it has first pinged some (any) IP address. Also, unsolicited ICMP reply log messages are sometimes associated with the DEFAULT_VLAN instead of the VLAN of the incoming unsolicited ICMP reply.

IGMP

CR_0000132149 Although the RFC requires that the switch with the lowest IP address becomes querier, a switch that is acting as querier stops being querier when it receives a query from a switch with a higher IP address.

CR_0000134412 The switch sends an IGMP General Query with an incorrect layer 2 destination address.

CR_0000135527 A non-querier switch that receives a Join from the querier fails to send further Joins to the querier, resulting in loss of multicast traffic.

Jumbo Frames

CR_0000137961 When jumbo frames are enabled on any VLAN, OSPF fails to establish an adjacency after a switch reboot, and RIP updates might not be accepted by the router.

Link

CR_0000137549 Gigabit fiber transceivers operate in auto-negotiation mode even if the port is configured for 1000 Mbps full-duplex operation (`speed-duplex 1000-full`). If both sides of the link were configured as 1000-full, the link will go down after the switch at one side of the link is updated with affected software. This issue was introduced in software version 15.12.0006.

Loop Protection

CR_0000127150 Loop protection fails to detect a loop on a port configured for 802.1X authentication, if 802.1X is not enabled globally.

MAC Authentication

CR_0000129991 MAC Authentication fails when the `peap-mschapv2` parameter is included in the `aaa authentication CLI` command.

MSTP

CR_0000132175 In a complicated sequence of events with multiple MSTP instances and UDLD configured on only one path between switches, after link failure and link restoration it is possible for MSTP to begin forwarding on a port that should be blocked, causing a network topology loop.

OpenFlow

CR_0000134471 OpenFlow flows are not programmed correctly when RPVST+ is disabled on the OpenFlow member VLAN.

Passwords

CR_0000130921 If the switch is configured with a username and password, changing the password causes the username to also change. The username is changed to the default "manager" or "operator", depending which password is changed.

RADIUS Accounting

CR_0000137793 An interim-update status request generates incorrect accounting information in the RADIUS server. This issue was introduced with CR_0000123330.

Routing

CR_0000123230 The switch does not forward traffic to a host that has a static route configured with a 32-bit subnet mask. Traces show that the switch never sends an ARP request for that host.

sFlow

CR_0000128439 When an sFlow-sampled inbound packet is to be routed, the sFlow data gives the wrong output port on the switch.

SNMP

CR_0000122623 After rebooting a switch configured for SNMP with the parameters operator unrestricted, the switch does not allow the user to set any read/write MIB objects.

CR_0000134672 The entStateOper OID from the Entity State MIB gives an incorrect value of 1 (unknown) instead of 3 (enabled), for some switches.

CR_0000135477 A trap from an undocumented OID can be triggered under certain conditions. With this fix, OID 1.3.6.1.4.1.11.2.3.7.11.107.0.2 has been added to the MIB.

SSL

CR_0000127972 A self-signed certificate cannot use a common name (CNAME) longer than 40 characters. With this fix, the limit is 90 characters.

Stacking

CR_0000121075 When stacking is enabled, the switch is accessible via the Web even after disabling the Web server, and via TELNET even after disabling TELNET.

TFTP

CR_0000123187 TFTP file transfers initiated via TELNET or SSH fail, if the console inactivity-timer setting causes the TELNET or SSH session to end during the transfer. This issue does not affect file transfers initiated via the console or via SFTP.

Transceivers

CR_0000132781 Software does not allow the dual-speed J8177C Gigabit-copper transceiver to be configured for 100 Mbps operation, responding with a message such as `Value auto-100 is not applicable to port A21.`

CR_0000136125 The switch allows the user to configure the 1000BASE-T transceiver (J8177B/C) for 100-Megabit operation, but that setting is not supported. The transceiver operates at Gigabit speed despite the 100-Megabit setting.

Trunking

CR_0000126473 The switch does not allow a static LACP trunk to be configured as active or passive. This fix adds a new interface command: `lacp static [active | passive].`

Web Management

CR_0000135883 The "Rx Errors" column is missing from the Web user interface.

CR_0000137792 A self-signed SSL certificate generated via the Web interface cannot use a common name (CNAME) longer than 40 characters. With this fix, the limit is 90 characters.

Upgrade information

Upgrading restrictions and guidelines

RA.15.14.0012 uses BootROM RA.15.11. 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 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.