

I.10.107 Release Notes

Abstract

This document contains supplemental information for the I.10.107 release.



© 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 U.S. registered trademarks of the Microsoft group of companies.

Contents

1 I.10.107 Release Notes.....	6
Description.....	6
Important information.....	6
Products supported.....	6
Compatibility/interoperability.....	6
Enhancements.....	6
Fixes.....	7
Version I.10.107.....	7
SFTP.....	7
Web Management.....	7
Version I.10.105.....	7
Stacking.....	7
Web Management.....	7
Version I.10.104.....	7
Command Authorization.....	7
Config.....	7
Version I.10.103.....	7
Crash.....	7
DHCP Snooping.....	8
Version I.10.102.....	8
MAC Tables.....	8
Web Management.....	8
Version I.10.101.....	8
Config.....	8
RADIUS.....	8
Version I.10.99.....	8
Loop Protection.....	8
Multicast.....	8
SNMP.....	8
Version I.10.98.....	8
802.1X.....	8
CLI.....	9
Crash.....	9
Multiple Symptoms.....	9
Secure Copy.....	9
SNMP.....	9
Version I.10.97.....	9
CLI.....	9
IGMP.....	9
QoS.....	9
SNMP.....	9
Version I.10.94.....	10
Authentication.....	10
QoS.....	10
Secure Copy.....	10
Version I.10.93.....	10
CLI.....	10
Version I.10.92.....	10
CLI.....	10
Crash.....	10
MAC Authentication.....	10

Web Management.....	10
Version I.10.91.....	10
SSL.....	10
Version I.10.90.....	11
802.1X.....	11
Version I.10.89.....	11
FFI/Config.....	11
SSL.....	11
Version I.10.88.....	11
Authentication.....	11
SSH.....	11
Version I.10.87.....	11
CLI.....	11
Web Management.....	11
Version I.10.86.....	11
Management.....	11
Version I.10.85.....	12
DHCP.....	12
LLDP-MED.....	12
Routing.....	12
Version I.10.84.....	12
CLI.....	12
DHCP Snooping.....	12
Spanning Tree.....	12
Version V.10.83.....	12
Console.....	12
Crash.....	12
LLDP-MED.....	12
SNMP/Config.....	12
Stacking.....	13
STP.....	13
UDLD.....	13
Version I.10.82.....	13
Authentication.....	13
Config.....	13
GVRP.....	13
LLDP.....	13
Stacking.....	13
Unauthenticated VLAN.....	13
Version I.10.81.....	14
SNMP/Config.....	14
Version I.10.80.....	14
CDP.....	14
CPU Utilization.....	14
Crash.....	14
Version I.10.79.....	14
802.1X.....	14
Authentication.....	14
CDP.....	14
DHCP Snooping.....	14
Management.....	14
SSH.....	14
UDLD.....	14
Version I.10.78.....	15
802.1X.....	15

Authentication.....	15
Command Authorization.....	15
DHCP Snooping.....	15
GVRP.....	15
RADIUS.....	15
Trunking.....	15
UDLD.....	15
Upgrade information.....	15
Upgrading restrictions and guidelines.....	15
Contacting HP.....	15
HP security policy.....	16
Related information.....	16
Documents.....	16
Websites.....	16
Documentation feedback.....	16

1 I.10.107 Release Notes

Description

This release note covers software versions for the I.10 branch of the software.

This document covers software versions beginning with I.10.78. For information about earlier software versions, please see the I.10.77 release notes.

Product series supported by this software:

- HP 2800 Switch Series

Important information

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

Products supported

This release applies to the following product models:

Product number	Description
J4903A	HP 2824 Switch
J4904A	HP 2848 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

No enhancements have been introduced since I.10.77.

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 preceding the fix description is used for tracking purposes.

Version I.10.107

SFTP

CR_0000154313 With SSH enabled, attempting SFTP transfers might cause the switch to reboot unexpectedly with a message similar to TLB Miss: Virtual Addr=0x0000001c IP=0x8008b24c Task='tSftp0', Task ID=0x85717f10 fp:0x85d83a38 sp:0x85717d58 ra:0x8008b1c8 sr:0x1000fc01.

Web Management

CR_0000162905 When a user connects to an IP address on the switch using a browser with Java version 7U51 or later, the web interface is blocked because the Java applets are not code-signed. This issue was fixed in a previous version, but required a re-implementation.

Version I.10.105

Stacking

CR_0000146549 If the switches are configured to disable HTTP (no web-management) and instead use HTTPS (web-management ssl), some stack members might not be accessible from the commander.

Web Management

CR_0000145618 The Web user interface is inaccessible to clients using Java version 7, update 51 (Java 7u51).

Version I.10.104

Command Authorization

CR_0000137774 When issuing a command such as `show tech` (which invokes many sub-commands), if any of the sub-commands are on the HP-Command-Exception DenyList, the command fails and the user is removed from enable mode.

Config

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.

Version I.10.103

Crash

CR_0000131197 With MSTP enabled, a large number of MAC address moves and/or learns might cause the switch to reboot unexpectedly with a message similar to Software exception at `svc_misc.c:514` -- in 'mMstpCtrl', task ID = 0x1637388, -> No memory available.

CR_0000139768 When the switch receives multiple requests to download the config file via SFTP, the switch might reboot unexpectedly with a message similar to Software exception at `exception.c:373` -- in 'tSsh0', task ID = 0x145d168 -> Memory system error at 0x15a5d58 - memPartFree.

DHCP Snooping

CR_0000126311 The CLI entry `dhcp-snooping option 82 untrusted-policy keep` is not included in the config file if no `dhcp-snooping option 82` is also configured. If the config file is saved to a TFTP server, it does not function properly when subsequently loaded on a switch.

Version I.10.102

MAC Tables

CR_0000120855 MAC address entries in the hardware and software tables might become out of sync. This has been observed to cause problems with DHCP snooping. For example, a client does not receive a DHCP Offer because the switch does not have the client's MAC address in its table and therefore DHCP snooping does not allow the switch to forward the DHCP Offer.

Web Management

CR_0000123053 The Web interface allows the password to be viewed.

Version I.10.101

Config

CR_0000116462 If an untagged port member of a port-based VLAN is changed to a tagged member of the same VLAN, all inbound tagged traffic is dropped.

RADIUS

CR_0000116468 When only one VLAN has an IP address configured, and it is not the primary VLAN, the RADIUS Request does not include the NAS-IP-ADDRESS attribute.

CR_0000117215 If the encryption keys are not configured the same for primary and secondary RADIUS servers on the switch, the RADIUS server might reject clients with wrong username-password.

Version I.10.99

Loop Protection

CR_0000110201 If you disable a port already disabled by loop-protect, it might still show as enabled after timer expiry.

Multicast

CR_0000107597 The switch floods GMRP (GARP Multicast Registration Protocol) packets that are received on Spanning Tree backup and alternate ports, instead of dropping the packets.

CR_0000110677 GMRP Frames on 2800s should flood to the VLAN just as multicast traffic does, but they are not flooding as expected.

SNMP

CR_0000113034 The `SNMPget` of object **dot3adAggPortListPorts** returns extraneous comma and space characters, which can affect scripts based on the `SNMPget` output.

Version I.10.98

802.1X

PR_0000073291 Some devices are not set to the configured unauthorized VLAN when authenticator clientlimit is set to value 1. Seen mainly on devices that are HP printers or when using JetDirect cards.

CLI

CR_0000105415 The config may display incorrectly with regard to how it displays the ports in a particular VLAN. For example: `untagged 3-Trk1` instead of `untagged 3-50,Trk1`.

Crash

PR_0000073576 The switch can hang or reboot if transferring a config file > ~4300 bytes using SCP in SFTP mode. Smaller configuration files do not exhibit a problem.

Multiple Symptoms

PR_0000073630 Several Issues Resolved:

- SFTP sessions do not close properly.
- Error message `Error while reading: received a short buffer from FXP_READ, but not EOF.`
- Crash message `Software Exception at xception.c:373 -- in 'tSsh0', -> Memory system error.`

Secure Copy

PR_0000073633 File transfer fails when using Secure Copy (SCP) or Secure FTP (SFTP) to download the switch operating system. The error message `error while reading: received a short buffer from FXP_READ, but not at EOF has been observed.`

SNMP

CR_0000107406 The following command, if run against ports 1-24, might result in a trap message reporting the wrong VLAN, if routing is enabled: `port-security x learn-mode configured action send-alarm mac-address xx:xx:xx:xx:xx:xx`. Running this command against ports 25-48 does not exhibit the problem.

Version I.10.97

CLI

CR_0000103448 Enabling and Disabling loop-protect on a range of ports might result in ports 4 and higher to be disabled and left in an error state. For example `loop-protect 1-24` then `no loop-protect 1-24` may result in ports 4-24 being disabled.

IGMP

CR_0000105407 When an IGMPv2 host leaves a group, the switch may send a malformed GSQ message.

QoS

CR_0000105258 The switch may change the priority of routed packets. This CR_0000105258 improves the QoS fix in PR_0000070680 in I.10.94.

SNMP

CR_0000105142 LLDP information from some devices causes an snmpwalk of the switch to truncate after the `lldpRemanAddrIfId` OID (iso.0.8802.1.1.2.1.4.2.1.4).

Version I.10.94

Authentication

PR_0000070500 When the 802.1X authenticator times out waiting for a supplicant response, instead of transitioning to the connecting state and restarting the attempt to acquire a supplicant by transmitting Identity-Requests, it falls silent.

QoS

PR_0000060662 The Web user interface displays **Status** at the top of screen even though there is no status information provided.

Secure Copy

PR_0000072803 After disabling SCP (Secure Copy Protocol) and enabling TFTP, the switch's config file retains the `no tftp client` entry that was automatically added when SCP was enabled.

Version I.10.93

CLI

PR_0000071004 The output of the command `show port-access authenticator config` displays the direction as `both`, even if the direction was configured to be `in` or `out`.

Version I.10.92

CLI

PR_0000041836 The switch asks users if they want to save the configuration even though no changes were made. Note that configuration changes made via SNMP will still trigger this behavior even after this fix.

Crash

PR_0000067243 The switch may reboot unexpectedly with a message similar to the following:
`Software exception with task mAcctCtrl?.`

MAC Authentication

PR_0000071595 MAC authentication on Cisco IP phones may fail.

Web Management

PR_0000070015 A VLAN QoS priority that is set in the web user interface is not saved to the switch startup-config.

Workaround: Go to **Configuration > System Info** and click **Apply Changes** to manually save the configuration.

Version I.10.91

SSL

PR_0000070330 After copying the CA certificate to the switch the following error message is received: Error setting CA Signed Request Configuration - No certificate is installed. This improves the SSL fix (PR_0000039989) in I.10.89.

Version I.10.90

802.1X

PR_0000067682 When using 802.1X in client mode, the command `aaa port-access authenticator 1 clientlimit 2` should allow two clients to authenticate on that port. After one client is removed and the timeout period has passed, the switch does not allow a new second client to authenticate.

Version I.10.89

FFI/Config

PR_0000039989) FFI - If an FFI event is triggered and the link is then brought down and back up again, the same FFI event is triggered again in about 20 seconds, even if the trigger condition is not met. Config - This fix makes the downgrade of the port to auto-10/100 visible in the running configuration. Note that this may trigger the switch to ask `Do you want to save current configuration?` upon logout or switch reload.

SSL

PR_0000064686 After copying the CA certificate to the switch, the following error message is received: Error setting CA Signed Request Configuration - No certificate is installed.

Version I.10.88

Authentication

PR_0000058441 User authentication fails if the user's RADIUS configuration includes a non-HP VSA before any HP VSAs.

Workaround: Configure the user in RADIUS with at least one HP VSA before any non-HP VSAs.

SSH

PR_0000062389 After connecting to the switch with operator privileges, a subsequent SSH connection receives only operator privileges instead of manager privileges.

Version I.10.87

CLI

PR_0000058067 When the switch is configured with a default gateway, the output of `show ip route` gives incorrect values for Metric and Distance. Communication with the default gateway works properly.

Web Management

PR_0000060662 The web user interface displays the word **Status** at top of screen even though there is no status information provided.

Version I.10.86

Management

PR_0000053533 The ProCurve Manager (PCM) `test communication parameters test` might fail on the second attempt.

Version I.10.85

DHCP

PR_0000055868 DHCP can fail if uplinked to a non-DHCP Snooping device.

LLDP-MED

PR_0000057609 LLDP-MED packets are sent from the switch before checking that the port has authenticated clients connected.

Routing

PR_0000057394 The switch does not route properly until after ARP cache is cleared.

Version I.10.84

CLI

PR_0000041272 CLI output from the commands `show port-access web clients` or `show port-access web clients detailed` displays only the client information from the first port that is active (has authenticated or unauthenticated clients). All other ports do not show any clients, even if the port has several authenticated or unauthenticated clients.

PR_0000051188 If the switch uses DHCP to obtain an IP address, the output of `show ip` does not display the correct default gateway. This is a display issue only; the correct gateway address is used by the switch.

DHCP Snooping

PR_0000046276 With DHCP snooping enabled, a MAC-Authentication client whose session times out cannot reauthenticate.

Spanning Tree

PR_0000057003 The switch might experience Spanning Tree instability upon changing the system time via CLI, TimeP, or SNTP, if the time change occurs while the switch is receiving high volumes of broadcast traffic (on the order of 1 Mbps) on its Spanning Tree root port. This issue might also affect switch management traffic, causing unresponsive SNMP, TELNET, and SSH sessions.

Version V.10.83

Console

PR_0000001136 Rarely, the switch console may hang after a software image transfer to the switch.
Workaround: `<Ctrl-C>` restores the command prompt.

Crash

PR_0000050061 The switch might sometimes reboot unexpectedly during a topology change with an error similar to the following: `Software exception at exception.c:373 -- in mRadius005', task ID = 0x2594760 -> Memory system error at 0x243fb68 - memPartFree.`

LLDP-MED

PR_0000050798 In some cases the LLDP-MED inventory for an attached IP phone is not properly received or stored by the switch.

SNMP/Config

PR_0000039221 The switch can misinterpret the community name as if it were a trap level, in the `snmp-server host` command. This fix modifies the command with keywords `community` and

trap-level. The new comand syntax is as follows: snmp-server host <ip addr> [community <community string>] [trap-level <none | all | not-info | critical | debug>] [informs].

Stacking

PR_0000052110b When a commander accesses a member switch and the user issues the `show tech all` command, in some situations the session from commander to member can become unresponsive.

Workaround: from the commander switch, `kill` the unresponsive session. This PR 0000052110b is an improvement of the original fix (PR_0000052110) in I.10.82.

STP

PR_0000037812 When using force-version RSTP, the switch sends the root bridge ID in Spanning Tree BPDUs instead of its own bridge ID.

UDLD

PR_0000047414 When UDLD is enabled, communication with the switch might be inconsistent, affecting the switch response to ping, TELNET, 802.1X requests, SNMP requests, and SNTP packets.

Version I.10.82

Authentication

PR_0000052226 When port authentication methods are in use on a switch, if all of the clients are disconnected, the switch might change the Class of Service (CoS) settings. This PR_0000052226 improves the Authentication fix in I.10.78 software (PR_0000044893).

PR_0000053003 After a client is authenticated by 802.1X, if the switch receives a subsequent successful web or MAC Authentication for that same client, the switch overwrites the 802.1X client RADIUS attributes.

Config

PR_0000037570 After using the CLI to assign a port in a VLAN number higher than 32, the configuration cannot be saved via the Menu interface.

GVRP

PR_0000046133 Switches do not use multiple GARP Information Propagation (GIP) contexts when the switch has been configured for MSTP operation; the same GIP context is used for all ports participating in GVRP. There should be multiple GIP contexts - one for each spanning-tree (the IST and each of the MSTIs). This fix improves the GVRP fix in I.10.78 (PR_0000040758).

LLDP

PR_0000051224 In some cases LLDP packets are transmitted from a switch port before the client is authenticated.

Stacking

PR_0000052110 When a commander accesses a member switch and the user issues the `show tech all` command, in some situations the session from commander to member can become unresponsive.

Workaround: from the commander switch, `kill` the unresponsive session.

Unauthenticated VLAN

PR_0000045072 An unauthenticated VLAN cannot be configured for 802.1X authentication when another authentication method is also in use on a port. This fix also adds the `unauth-period` parameter for MAC authentication.

Version I.10.81

SNMP/Config

PR_0000043775 The switch allows invalid configuration parameters to be set via SNMP.

Version I.10.80

CDP

PR_0000051209 Switch forwards CDP packets to other ports even when CDP is globally enabled.

CPU Utilization

PR_0000044632 Data transfer in one VLAN with DIPLD and IP Routing enabled elevates CPU to 99%.

Crash

PR_0000049246 The command `aaa accounting commands stop-only radius` causes the switch to crash with `Software exception 'mRadius005`.

Version I.10.79

802.1X

PR_0000047025 After the switch reboots and before IP communication is initialized, the switch accepts authentication requests from 802.1X clients. Because the switch cannot communicate with the RADIUS server yet, it sends EAP-Failure notifications to the client, which causes client authentication to fail.

PR_0000048284 802.1X showing in an open state and receiving packets, under certain conditions causes the port to be in a down state with no traffic being passed.

Authentication

PR_0000045069 In some situations the switch authenticates an EAP 802.1X client but does not allow communication from the client.

CDP

PR_0000047116 CDP packets are not dropped even when the switch is configured with the command `no cdp run`.

DHCP Snooping

PR_0000040580 Configuration of trust status for DHCP snooping on ports participating in a dynamic trunk yields undesirable results when the ports of the trunk are removed. This configuration should not be allowed on dynamic trunks (for example, `dhcp-snooping trust Dyn`), and this fix enforces that limitation at the CLI with an error message.

Management

PR_0000044146 Ping and Telnet to the switch fail at exactly 1243 days of uptime.

SSH

PR_0000014531 Rarely, after some period of time with normal SSH connectivity, the switch may become unresponsive to further SSH management.

UDLD

PR_0000043071 UDLD transmits a burst of packets when any port on the switch goes down (one packet is sent for each port that goes down), falsely triggering a failure state.

Version I.10.78

802.1X

PR_0000039909 802.1X authentication appears to work, but the client cannot communicate on the network for approximately 30 seconds.

Authentication

PR_0000038263 Some frames are allowed on the switch port despite the default `aaa parameter controlled-directions both`.

PR_0000044893 When port authentication methods are in use on a switch, if all of the clients are disconnected, the switch may change the Class of Service (CoS) settings.

Command Authorization

PR_0000043525 HP-Command-String authorization does not work as expected.

DHCP Snooping

PR_0000044797 When a PXE protocol DHCP-offer packet is sent from a boot server through a trusted port, the switch drops the packet.

GVRP

PR_0000040758 Switches do not use multiple GARP Information Propagation (GIP) contexts when the switch has been configured for MSTP operation; the same GIP context is used for all ports participating in GVRP. There should be multiple GIP contexts - one for each spanning-tree (the IST and each of the MSTIs).

RADIUS

PR_0000042522 The `class` attribute is not included in the accounting-request to the RADIUS server; RFC 2865 states that this should occur.

Trunking

PR_0000018102 When either or both links of a two-link trunk from switch to server is disabled, all devices on the VLAN become inaccessible by IP.

UDLD

PR_0000009505 UDLD misconfiguration (where UDLD is enabled on one side and disabled on the other) could lead to a unicast packet storm, which results in MSTP running with multiple roots.

Upgrade information

Upgrading restrictions and guidelines

I.10.107 uses BootROM I.08.07. If your switch has an older version of BootROM, the BootROM will be updated with this version of software.

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*.

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.