# Release Notes:

## Version K.15.10.0016 Software

*for the HP Series 3500, 3500yl, 5400zl, 6200yl, 6600, and 8200zl Switches*

- This software is supported on the following switches

  HP 3500-24 Switch (J9470A)
  HP 3500-24-PoE Switch (J9471A)
  HP 3500-48 Switch (J9472A)
  HP Switch 3500-48-PoE (J9473A)
  HP 3500yl-24G-PWR Intelligent Edge Switch (J8692A)
  HP 3500yl-48G-PWR Intelligent Edge Switch (J8693A)
  HP 3500yl-24G-PoE+ Switch (J9310A)
  HP 3500yl-48G-PoE+ Switch (J9311A)
  HP 5406zl Intelligent Edge Switch (J8697A)
  HP 5406zl Switch with Premium SW (J9642A)
  HP 5412zl Intelligent Edge Switch (J8698A)
  HP 5412 zl Switch with Premium SW (J9643A)
  HP 5406zl-48G Intelligent Edge Switch (J8699A)
  HP 5412zl-96G Intelligent Edge Switch (J8700A)
  HP 5406zl-48G-PoE+ Switch (J9447A)
  HP 5412zl-96G-PoE+ Switch (J9448A)
  HP 5406-44G-PoE+/2XG-SFP+ v2 zl Switch (J9533A)
  HP 5412-92G-PoE+/2XG-SFP+ v2 zl Switch (J9532A)
  HP 5406-44G-PoE+/4G-SFP v2 zl Switch (J9539A)
  HP 5412-92G-PoE+/4G-SFP v2 zl Switch (J9540A)
  HP 6200yl-24G-mGBIC Switch (J8992A)
  HP 6600-24G Switch (J9263A)
  HP 6600-24G-4XG Switch (J9264A)
  HP 6600-24XG Switch (J9265A)
  HP 6600-48G Switch (J9451A)
  HP 6600-48G-4XG Switch (J9452A)
  HP 8206zl Switch (J9475A)
  HP 8206 v2 zl Switch with Premium SW (J9640A)
  HP 8212zl Switch (J8715A, J8715B)
  HP 8212zl Switch with fan tray (J9091A)
  HP 8212 v2 zl Switch with Premium SW (J9641A)
  HP 8206-44G-PoE+/2XG v2 zl Switch with Premium SW (J9638A)
  HP 8212-92G-PoE+/2XG v2 zl Switch with Premium SW (J9639A)

These release notes include information on the following:

**Manual Part Number**

5998-3751
July 2013

**Trademark Credits**

Microsoft®, Windows®, and Windows NT® are US registered trademarks of Microsoft Corporation.
Adobe® and Acrobat® are trademarks of Adobe Systems Incorporated. Java™ is a US trademark of Sun Microsystems, Inc.

**Software Credits**

SSH on HP Networking Switches is based on the OpenSSH software toolkit. This product includes software developed by the OpenSSH Project for use in the OpenSSH Toolkit. For more information on OpenSSH, visit

www.openssh.com.

SSL on HP Networking Switches is based on the OpenSSL software toolkit. This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. For more information on OpenSSL, visit

www.openssl.org.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com) Disclaimer

HEWLETT-PACKARD COMPANY MAKES NO WARRANTY OF ANY KIND WITH REGARD TO THIS MATERIAL, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Hewlett-Packard shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this material.

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.

Hewlett-Packard assumes no responsibility for the use or reliability of its software on equipment that is not furnished by Hewlett-Packard.

**Warranty**

See the *Software End User License Agreement and Hardware Limited Warranty* booklet, available through www.hp.com/networking/support.

A copy of the specific warranty terms applicable to your Hewlett-Packard products and replacement parts can be obtained from your HP Sales and Service Office or authorized dealer.

Hewlett-Packard Company
8000 Foothills Boulevard, m/s 5551
Roseville, California 95747-5551
www.hp.com/networking

# Contents

## Software Management



## Support Notes



## Clarifications



## Known Issues

## Enhancements

## Software Fixes

# Software Management

## Premium License for Selected Switch Features

Switch software licensing enables advanced features in selected HP switches. For software version K.15.01.0031 and later, the following table shows the software licenses available for supported switches:

| **License Type** | **Premium*** Supports advanced routing features, including: – OSPF v2, OSPF v3 – PIM – sparse mode, PIM – dense mode – VRRP – QinQ (IEEE 802.1ad) | | | |
|---|---|---|---|---|
| **Switch Family** | **3500 and 3500yl** | **5400zl** | **6600** | **8200zl** |
| **License Product** | J8993A | J8994A | J9305A | J9474A |
| * Notes: • Legacy HP 8212zl switch (J8715A) included advanced features, a Premium License upgrade is not required. • HP 6200yl switch included advanced features, a Premium License upgrade is not required. • A previously installed license can be removed from a switch and transferred to another switch within the same product series. | | | | |

For more information on features enabled through a Premium License, see the data sheets and software documentation for your switch.

Each Premium License product provides license-to-use for a single switch. To install a license, see the documentation provided with the license product. For an overview, see "General Procedure" below.

**Note** When updating to software version K.15.01.0031 or later, a Premium License upgrade is not required for supported switches that already contain a premium license.

### General Procedure

The general procedure for installing a software license involves several different numbers:

- registration ID – This number comes with the license you purchase, and represents your right to install the particular type of license on a particular type of switch.
- hardware ID – This number is provided by the switch that you are licensing, and includes the switch's serial number and an identifier for the feature that you are licensing.
- license key – This number is generated by the My Networking portal, based on the registration ID and the hardware ID that you provide. When you install this number into the switch, it enables the feature that you are licensing.

The procedure for installing a licensed feature into a switch is:

1. **Locate the registration ID.** When you purchase a software license, you receive a folded license registration card. The registration ID is located on the inside of the card, typically in the upper left corner.

2. **Get the switch's hardware ID.** Establish a console connection to the switch CLI and enter Manager level, using the **enable** command if necessary and the switch password if required. For example:

   ```
   Switch> enable
   Switch#
   ```

   From the Manager level, issue the **licenses hardware-id <license_type>** command. For example:

   ```
   Switch# licenses hardware-id premium
   ```

   The CLI returns a hardware ID number. Copy the hardware ID number from the screen (using Ctrl-C) or write it down. (Copying the number is easier and more accurate.) You will enter the number on the My Networking portal in the next step.

3. **Get the license key.** Point your Web browser at the My Networking portal (**http://my.procurve.com**) and sign in. Click the My Licenses tab, enter the registration ID, and then enter the hardware ID. At the end of the procedure a license key is displayed. (It is also e-mailed to you.) Copy the license key from the screen (using Ctrl-C) or write it down.

4. **Enter the license key into the switch.** On the CLI console, save the configuration of the switch (**write memory**). Then, from a Manager-level prompt, issue a **licenses install premium <license-key>** command. (The license key number is not case sensitive.) For example:

   ```
   Switch# licenses install premium AA000GG000-A-0123ABC-ABCD123-0A2B3C4-0123ABC
   ```

5. Reboot the switch. For example:

   ```
   Switch# boot
   ```
   or:
   ```
   Switch# reload
   ```

   The licensed features should now be active on the switch.

E-PCM or E-PCM+ can be used to simplify the process of adding licenses. Just provide the registration ID from the Premium License and use E-PCM to identify which switch to install the license. E-PCM will communicate with the My Networking Portal directly and add the license to the switch without user intervention.

## Getting Further Software Management Information

The *Basic Operation Guide* for your switch product provides further software management information on the following topics:

- Downloading switch documentation and software from the Web
- Saving configurations while using the CLI
- Best practices for software updates

To access the guide, visit www.hp.com/networking/support or click on the following link:

http://h20000.www2.hp.com/bizsupport/TechSupport/Product.jsp?lang=en&cc=us&taskId=101&contentType=Support-Manual&docIndexId=64180&prodTypeId=12883&prodCatId=82675

# HP Switch, Routing Switch, and Router Products Software Keys

| Software Letter | HP Products |
|---|---|
| **A** | Switch 2615-8-PoE and Switch 2915-8G-PoE |
| **C** | 1600M, 2400M, 2424M, 4000M, and 8000M |
| **CY** | Switch 8100fl Series (8108fl and 8116fl) |
| **E** | Switch 5300xl Series (5304xl, 5308xl, 5348xl, 5372xl, 5304xl-32G, and 5308xl-48G) |
| **F** | Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324 |
| **G** | Switch 4100gl Series (4104gl, 4108gl, 4140gl, 4148gl, and 4160gl) |
| **H** | Switch 2600 Series, Switch 2600-PWR Series: H.07.81 and earlier, or H.08.55 and greater,<br>Switch 2600-8-PWR requires H.08.80 or greater.<br>Switch 6108: H.07.*xx* and earlier |
| **I** | Switch 2800 Series (2824 and 2848) |
| **J** | **J.*xx.xx*.biz** Secure Router 7000dl Series (7102dl and 7203dl) |
| **J** | **J.*xx.xx*.swi** Switch 2520G Series (2520G-8-PoE, 2520G-24-PoE) |
| **K** | 3500 Series, 3500yl Series, 5400zl Series, 6200yl-24G Switch, Switch 6600 Series (6600-24G, 6600-24G-4XG, 6600-24XG, 6600-48G, 6600-48G-4XG), and 8200zl Series Switches |
| **KA** | Switch 3800 Series |
| **L** | Switch 4200vl Series (4202vl-72, 4202vl-48G, 4204vl, 4204vl-44G-4SFP, 4208vl, 4208vl-96, 4208vl-64G, and 4208vl-68G-4SFP) |
| **M** | Switch 3400cl Series: M.08.51 though M.08.97, or M.10.01 and greater;<br>Series 6400cl Series: M.08.51 though M.08.95, or M.08.99 to M.08.100 and greater. |
| **N** | Switch 2810 Series (2810-24G and 2810-48G) |
| **P** | Switch 1810G (1810G-8, 1810G-24) |
| **PA/PB** | Switch 1800G Series (Switch 1800-8G - PA; Switch 1800-24G - PB) |
| **PK** | Switch 1810-48G |
| **PL/PM** | 1810 v2 Switches (1810-8G v2, 1810-24G v2 - PL; 1810-8 v2, 1810-24 v2 - PM) |
| **PS** | PS1810 Switches (PS1810-8G, PS1810-24G) |
| **Q** | Switch 2510-24 |
| **R** | Switch 2610 Series (2610-24, 2610-48, 2610-24/12PWR, 2610-24-PWR, and 2610-48-PWR) |
| **RA** | Switch 2620 Series |
| **S** | Switch 2520 Series (2520-8-PoE, 2520-24-PoE) |
| **T** | Switch 2900 Series |
| **U** | Switch 2510-48 |
| **VA/VB** | Switch 1700 Series (Switch 1700-8 - VA and Switch 1700-24 - VB) |
| **W** | Switch 2910al Series |
| **WA** | HP Access Point 530 |
| **WB** | Switch 2920 Series |
| **WM** | HP Access Point 10ag |
| **WS** | HP Wireless Edge Services xl Module and the HP Redundant Wireless Services xl Module |
| **WT** | HP Wireless Edge Services zl Module and the HP Redundant Wireless Services zl Module |
| **Y** | Switch 2510G Series (2510G-24 and 2510G-48) |
| **YA** | 2530 Switches (2530-48, 2530-48-PoE+, 2530-8G, 2530-24G, 2530-48G, 2530-8G-PoE+, 2530-24G-PoE+, 2530-48G-PoE+) |

| Software Letter | HP Products |
|---|---|
| **YB** | 2530 Switches (2530-8, 2530-24, 2530-8-PoE+, 2530-24-PoE+) |
| **Z** | HP 6120G/XG and 6120XG Blade Switches |
| ***numeric*** | Switch 9408sl, Switch 9300 Series (9304M, 9308M, and 9315M), Switch 6208M-SX and Switch 6308M-SX (Uses software version number only; no alphabetic prefix. For example 07.6.04.) |

# Operating System and Web Browser Compatibility Table

The switch Web agent supports the following combinations of OS browsers:

| Operating System | Supported Web Browsers |
|---|---|
| Windows XP SP3 | Internet Explorer 7, 8<br>Firefox 3.5 |
| Windows Vista SP2 | Internet Explorer 8, 9<br>Firefox 10,11 |
| Windows 7 | Internet Explorer 8, 9<br>Firefox 12<br>Chrome 19 |
| Windows Server 2008 SP2 | Internet Explorer 8, 9<br>Firefox 12 |
| MAC OS | Firefox 12 |

# Minimum Software Versions

### For HP Series 3500, 3500yl, 5400zl, 6200yl, 6600 and 8200zl Switches and Hardware Features

| HP Device [Note 1] | Product Number | Minimum Supported Software Version |
|---|---|---|
| HP 8-port 10GBase-T v2 zl Module | J9546A | K.15.04.0002 |
| HP 3500yl-24G-PoE+ Switch | J9310A | K.15.02.0004 |
| HP 3500yl-48-PoE+ Switch | J9311A | K.15.02.0004 |
| HP 2-Port SFP+/2-Port CX4 10GbE yl Module | J9312A | K.15.02.0004 |
| HP 24-port 10/100/1000 PoE+ v2 zl Module | J9534A | K.15.02.0004 |
| HP 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module | J9535A | K.15.02.0004 |
| HP 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl Module | J9536A | K.15.02.0004 |
| HP 24-port SFP v2 zl Module | J9537A | K.15.02.0004 |
| HP 8-port 10-GbE SFP+ v2 zl Module | J9538A | K.15.02.0004 |
| HP 24-port 10/100 PoE+ v2 zl Module | J9547A | K.15.02.0004 |
| HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module | J9548A | K.15.02.0004 |
| HP 20-port Gig-T / 4-port SFP v2 zl Module | J9549A | K.15.02.0004 |
| HP 24-port Gig-T v2 zl Module | J9550A | K.15.02.0004 |
| HP 12-port Gig-T / 12-port SFP v2 zl Module | J9637A | K.15.02.0004 |
| HP 8206zl Switch Base System | J9475A | K.14.34 |
| HP 24-Port 10/100/1000 PoE+ zl Module | J9307A | K.14.34 |
| HP 20-Port 10/100/1000 PoE+/4-port MiniGBIC zl Module | J9308A | K.14.34 |
| HP 24-port 10/100 PoE+ zl Module | J9478A | K.14.34 |
| HP 5406zl-48G-PoE+ Switch | J9447A | K.14.34 |
| HP 5412zl-96G-PoE+ Switch | J9448A | K.14.34 |
| HP 3500-24 Switch | J9470A | K.14.31 |
| HP 3500-24-PoE Switch | J9471A | K.14.31 |
| HP 3500-48 Switch | J9472A | K.14.31 |
| HP 3500-48-PoE Switch | J9473A | K.14.31 |
| HP Switch 6600-48G | J9263A | K.14.24 |
| HP Switch 6600-48G-4XG | J9452A | K.14.24 |
| HP Switch 6600-24G | J9263A | K.14.03 |
| HP Switch 6600-24G-4XG | J9264A | K.14.03 |
| HP Switch 6600-24XG | J9265A | K.14.03 |
| HP ONE Services zl Module | J9154A | K.13.51 |

| HP Device [Note 1] | Product Number | Minimum Supported Software Version |
|---|---|---|
| HP Wireless Edge Services zl Module and the HP Redundant Wireless Services zl Module | J9051A and J9052A | K.12.43 |
| Premium Features on Series 3500yl and 5400zl Switches | J8993A and J8994A | K.11.33 |
| HP Switch 5400zl 24p Mini-GBIC Module | J8706A | K.11.33 |
| HP Switch 5400zl 4p 10-GbE CX4 Module | J8708A | K.11.33 |
| HP Switch 6200yl-24G-mGBIC | J8992A | K.11.33 |
| HP Switch 3500yl 2p 10GbE X2 + 2p CX4 Module | J8694A | K.11.17 |
| HP Switch 8212zl Base System | J8715A and J8715B | K.12.31 |

**Note 1** For minimum software requirements for supported transceivers, visit www.hp.com/networking/support.
- In the first text box, type **J4858** (for 100-Mb and Gigabit information), or **J8436** (for 10-Gigabit information).
- Select any of the products that display in the drop down list. Click the **Display selected** button.
- Select **Product support information**. Then click on **Manuals** and find the **Transceiver Support Matrix**.

## ROM Updates Required!

BootROM updates are needed to be able to boot specified switch software versions. In most cases, selected software versions are used to automatically update the BootROM. Therefore, to successfully update to K.15 software, you may have to update software in multiple steps, depending on your current software and BootROM versions. Please use the steps in the table below.

| If your software version is: | Your next step should be: |
|---|---|
| **K.12.31 through K.13.55** (BootROM K.12.12 - 12.14) | Update and reload into software version K.13.58 or K.13.68 |
| **K.13.58 or newer** (BootROM K.12.17 or newer; use **show flash** command) | Update directly into software version K.15.10.0016 (BootROM K.15.30) |

**Caution** When updating to interim software versions, refer to the Release Notes supplied with those versions and observe any precautions noted.

If your switch is running a software version earlier than K.15, your BootROM will be updated when you upload K.15 software to your switch. During the software update, the switch will automatically boot **twice**, first to update the BootROM to the proper version, and then to load the system software. 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.**

To confirm that the BootROM and system software have updated successfully following a reload into software version K.15.01.0031 or later, follow the process below at your switch CLI.

```
Switch# show flash

Image           Size(Bytes)   Date   Version
-----           ----------  -------- -------
Primary Image   : 11537788   04/23/10  K.15.01.0031 <--Indicates that system software is updated
Secondary Image :  9839140   11/06/09  K.14.47
Boot Rom Version: K.15.09 <-- Indicates the BootROM is updated
Default Boot    : Primary
```

# Support Notes

## What's New

### Summary of New Features

Starting with software version K.15.01.0031, some key new features are summarized below. To access or use these new features, see the software documentation for your switch.

| New Features in K.15.01.0031 (or later) | Description: |
|---|---|
| Nonstop Switching for 8200zl series switches | Provides high-availability support for business-critical and real-time applications.<br>• Allows layer 2 switching to continue during Management Module switchover.<br>• Transition from the Active Management Module to the Standby Management Module is quick and seamless, and does not require a reboot.<br>• Both Management Modules support identical features and configuration files |
| IPv6 Layer 3 support | • K.13 provided IPv6 foundation services:<br>– IPv6 Host<br>– Dual stack (IPv4/IPv6)<br>– MLD snooping<br>• K.14 provided additional security and control:<br>– IPv6 ACL<br>– IPv6 QoS<br>• K.15 provides Layer 3 support services:<br>– OSPFv3<br>– Static routing<br>– DHCPv6 Relay<br>– Other features, including Port-based ACLs, Auto tftp, syslog, SSH Server, SNMP server (v1, v2, v3), SNTP client, Web server, IP Auth Manager. |
| New Web Agent | The Web browser interface provides a new look and feel for simplified configuration. Java services and other client software are no longer needed. |
| Additional feature enhancements | • VRRP enhancements, including:<br>– Simplified troubleshooting of VRRP configurations<br>– Physical IP is no longer identical with Virtual IP<br>• Route Maps enhancements for route management<br>• QoS and Mirroring Policies enhancements, allowing them to be applied dynamically<br>• **show mesh**, **show class** and **show policy** command enhancements |
| New software version designation | **VVV.UU.BB.FFFFaaaaa** software code designations, where:<br>• **VVV** is a switch platform identifier (for example, 'K').<br>• **UU** is a major version number (for example, "15"), to specify significant changes in features or functions.<br>• **BB** is a minor version number for versions that may include significant changes in features or functions, including support of new hardware or enhancements. If the major number is incremented, the minor version number will reset to '01".<br>• **FFFF** specifies a unique build number. It may be used to identify a specific bug-fix release that may, or may not, carry over to a subsequent build.<br>• **aaaaa** is a character string suffix to identify a type of build, for example, a special feature build (such as 'spcl') or a maintenance build (such as "m"). This is an optional string. Non-maintenance releases will not have a suffix. |

## Additional Features

### Event Log Capacity

Beginning with Version K.15.01.0031 the capacity of the event log has been increased. In prior versions, the event log was stored as ASCII text strings on the switch; the maximum number of event log messages that could be stored was 2000 messages. With Version K.15.01.0031, the event log is now stored in a compressed form rather than ASCII text. Since compression can be variable, the new capacity of the event log will also be variable. Typically, the new capacity will be between 3,000 and 5,000 entries.

Due to the new method of storing the event log, event log entries created in K.15.01.0031 and later versions cannot be read by K.14.*xx* and earlier versions, and vice-versa. When booting from K.15.01.0031 (or later) into K.14.*xx* or earlier versions, the K.15 event log stored in memory will be erased. When booting from K.14.*xx* into K.15.01.0031 (or later), the K.14 event log stored in memory will also be erased.

### Event Log for Nonstop Switching (5400zl and 8200zl Switches)

With the introduction of Nonstop Switching, both Active and Standby management modules can create event log entries. To identify the slot and status of the management module creating the entry, the following tags are now used:

- AM1 - Active Management Module in Slot 1
- AM2 - Active Management Module in Slot 2
- SM1 - Standby Management Module in Slot 1
- SM2 - Standby Management Module in Slot 2

**Example:**

```
Switch 8212zl(config)# show log -r
 Keys:   W=Warning   I=Information
         M=Major     D=Debug E=Error
----  Reverse event Log listing: Events Since Boot  ----
I 03/16/10 18:03:29 00083 dhcp: AM1: DEFAULT_VLAN: updating IP address and subnet mask
I 03/15/10 15:34:00 00077 ports: AM1: port B1 is now off-line
I 03/15/10 15:34:00 00435 ports: AM1: port B1 is Blocked by STP
I 03/14/10 18:03:28 00083 dhcp: AM1: DEFAULT_VLAN: updating IP address and subnet mask
I 03/14/10 07:48:56 00077 ports: AM1: port B1 is now off-line
I 03/14/10 07:48:55 00435 ports: AM1: port B1 is Blocked by STP
I 03/13/10 14:02:11 00077 ports: AM1: port B2 is now off-line
I 03/13/10 14:02:11 00435 ports: AM1: port B2 is Blocked by STP
```

By default, only log entries from the Active management module will be shown.

To see all management module entries use the "**-s**" option.

**Example:**

```
Switch 8212zl(config)# show log -r -s
Keys:   W=Warning   I=Information
        M=Major     D=Debug E=Error
----  Reverse event Log listing: Events Since Boot  ----
I 03/16/10 18:03:29 00083 dhcp: AM1: DEFAULT_VLAN: updating IP address and subnet mask
I 03/15/10 15:34:00 00077 ports: SM2: port B1 is now off-line
I 03/15/10 15:34:00 00077 ports: AM1: port B1 is now off-line
I 03/15/10 15:34:00 00435 ports: SM2: port B1 is Blocked by STP
I 03/15/10 15:34:00 00435 ports: AM1: port B1 is Blocked by STP
I 03/14/10 18:03:28 00083 dhcp: AM1: DEFAULT_VLAN: updating IP address and subnet mask
I 03/14/10 07:48:55 00077 ports: SM2: port B1 is now off-line
I 03/14/10 07:48:55 00435 ports: SM2: port B1 is Blocked by STP
I 03/14/10 07:48:56 00077 ports: AM1: port B1 is now off-line
I 03/14/10 07:48:55 00435 ports: AM1: port B1 is Blocked by STP
I 03/13/10 14:02:11 00077 ports: SM2: port B2 is now off-line
I 03/13/10 14:02:11 00435 ports: SM2: port B2 is Blocked by STP
I 03/13/10 14:02:11 00077 ports: AM1: port B2 is now off-line
I 03/13/10 14:02:11 00435 ports: AM1: port B2 is Blocked by STP
```

Typically, the need to view both Active and Standby event messages would be limited (for example, troubleshooting a failover or a failure of the Standby module). Because the Standby module is in a "hot standby" mode, it still executes many of the same operations that the Active module does, which is why duplicate event log messages from the Standby module would be displayed.

# Clarifications

## HP Security Policy and Release Notes

Per HP policy, a Security Bulletin must be the first published notification of a security defect. Fixes to security defects are not documented in release notes, also by HP policy.

The official communication for security defect fixes will always be through HP Security Bulletins. For more information on security bulletins, and information on how to subscribe to them, please see **http://bizsupport2.austin.hp.com/bc/docs/support/SupportManual/c02645131/c02645131.pdf**.

Visit the HP Networking Web site for more information on security and HP Networking products:

**http://h17007.www1.hp.com/us/en/solutions/security/index.aspx**

**Note**

Version K.15.01.0031 is a major software release, and was developed from Version K.14.41.

Features, enhancements, software fixes and known issues in K.15.01.0031 and later versions will differ from K.14.42 and later versions.

This section provides clarifications of software features starting with Version K.15.01.0031. For prior software versions, see the Release Notes provided with those versions.

## Version K.15.01.0031 Clarifications

### Delays During Configuration Changes to Physical Ports

Beginning with K.15.01.0031, configuration changes to ports may require up to 10 seconds to take effect, especially on switches with high CPU utilization. After a configuration command, perform an appropriate **show** or **show running-config** command to confirm the configuration change. If configuration scripts are used, the script should be modified either to check for successful completion of the previous command before executing the next command, or to sleep for 10 seconds after the configuration command is executed.

### Nonstop Switching (5400zl and 8200zl Switches)

For more information on Nonstop switching, see the “Chassis Redundancy” chapter in the *Management and Configuration Guide* for your switch.

#### Unsupported zl Modules

ZL modules/controllers that do not support the Nonstop switching feature include the following:

- HP ONE Services zl Module (J9289A)
- HP Threat Management Services zl Module (J9155A)
- HP Threat Management Services zl Module with 1-year IDS/IPS subscription (J9156A)
- HP Wireless Edge Services zl Module (J9051A) and Redundant Wireless Services zl Module (J9052A)
- HP MSM765zl Mobility Controller (J9370A)

During a Nonstop switching failover, unsupported modules will not failover seamlessly to the Standby module. A Nonstop switching failover will cause a forced reboot on these modules. After rebooting, these modules will then sync with the newly active management module and begin operation again. Module traffic will be disconnected until the module completes the reboot process.

**Hot Swapping of Management Modules**

Use the shutdown button on the front of the management module before removal. The shutdown button ensures that the management module will be shutdown properly. If Nonstop Switching is enabled, using the shutdown button prior to removal will ensure failover to the Standby module will be successful.

**Rapid Routing Switchover and Stale Timer**

With K.15.01.0031, Nonstop switching only supports Layer 2 functions on the switch. During a failover, traffic routed through the switch at Layer 3 will see an interruption. When a failover from Active to Standby occurs, the routing table is "frozen". All routes that existed at the time of the failover are marked as "stale". While dynamic routing protocols running at the time may act as if the routing protocol has been restarted and rebuilds the table, the switch on which the failover occurred will continue to rout traffic using the "stale routes".

The "Stale timer" begins counting when the switchover occurs. When the "Stale timer" expires, any routes that are still marked as stale are purged from the routing table. Due to the nature of Rapid Routing switchover, if there are multiple simultaneous failures, network loops could occur or traffic could flow through unpredictable paths.

Caution should be taken if setting the "rapid-switchover" timer higher than the default. To disable "Rapid Routing Switchover" and to ensure that all routing is based on the most current routing protocol information, set the "rapid-switchover" timer to 0.

## Password Length and Special Character Issues

K.15.01.0031 does not support the longer usernames and passwords introduced in K.14.59. Use caution when upgrading or downgrading between software versions that do not support these features.

Before downgrading to a software version that does not include this feature, use one of the following procedures:

- Using the **password** CLI command or the Web browser interface, change usernames or passwords to be no more than 16 characters in length, and without any special characters. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).
- Clear the values using the **no password all** CLI command. This clears all the passwords. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).
- Clear password values by using the "Clear" button on the switch. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).

**Note** These procedures should be used only when downgrading from a software version that supports long usernames and passwords to a version that does not.

If a switch with long usernames/passwords is inadvertently booted into K.15.01.0031, you will not be able to gain access to the switch. To regain access to the switch:

1. Get access to the serial console on the switch.
2. Reboot the switch.
3. Interrupt the boot process when you see the following text:
   `Boot Profiles:`

```
   0. Monitor ROM Console
   1. Primary Software Image
   2. Secondary Software Image

   Select profile (secondary):
```

4. Boot the software image that does support long usernames and passwords. For example, if your Primary image is K.15.01.0031 installed and your Secondary image is K.14.*xx*, boot your Secondary image.
5. After the switch is booted, perform one of the three procedures described above.

**Caution** If you inadvertently booted into K.15.01.0031 with a long username/password, **do not** attempt to change the password or clear the password while running K.15.01.0031 software. Attempting to do so may corrupt the switch configuration and cause the switch to be inaccessible, resulting in a service call.

### IPv4 Loopback Address Not Required for IPv6 Address Configuration

On K.14.*xx* software, an IPv4 loopback address was required prior to configuring an IPv6 address. In K.15.01.0031 (or later), this is no longer a requirement.

However, before enabling OSPFv3 on K.15.01.0031 (or later), do one of the following:

- Configure a unique 32-bit router ID.
- Configure a unique IPv4 loopback address.

OSPFv3 requires a 32-bit router ID for operation. The 32-bit router ID can be derived from an IPv4 loopback address or it can be specifically set.

## Version K.15.02.0004 Clarifications

### Rate-Limiting on the Entire Packet

As of software version K.15.02.0004, ICMP rate-limiting and Classifier-based rate-limiting operates on the entire packet length instead of just the IP payload part of the packet. As a result, the effective metering rate is now the same as the configured rate. The rate-limiting applies to these modules.

| HP Device | Product Number | Minimum Supported Software Version |
|---|---|---|
| HP 24-port 10/100/1000 PoE+ v2 zl Module | J9534A | K.15.02.0004 |
| HP 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module | J9535A | K.15.02.0004 |
| HP 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl Module | J9536A | K.15.02.0004 |
| HP 24-port SFP v2 zl Module | J9537A | K.15.02.0004 |
| HP 8-port 10-GbE SFP+ v2 zl Module | J9538A | K.15.02.0004 |
| HP 24-port 10/100 PoE+ v2 zl Module | J9547A | K.15.02.0004 |
| HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module | J9548A | K.15.02.0004 |
| HP 20-port Gig-T / 4-port SFP v2 zl Module | J9549A | K.15.02.0004 |

| HP Device | Product Number | Minimum Supported Software Version |
|---|---|---|
| HP 24-port Gig-T v2 zl Module | J9550A | K.15.02.0004 |
| HP 12-port Gig-T / 12-port SFP v2 zl Module | J9637A | K.15.02.0004 |
| HP 8-port 10GBase-T v2 zl Module | J9546A | K.15.04.0002 |

## Change to Default Setting for Detecting and Powering Pre-802.3af Devices

- **PoE (PR_0000060319)** – The default setting for the **pre-std-detect** PoE parameter changed. In earlier software the default setting is "on". In K.15.02 and later software, the new default setting is "off".

## Compatibility Mode for v2 zl and zl Modules

**Note** In the following context, v2 zl modules are the second version of the current zl modules. Both v2 zl and zl modules are supported in the 5400zl and 8200zl series chassis switches.

Compatibility Mode allows the inter-operation of v2 zl modules with zl modules in a chassis switch. When in Compatibility Mode, the switch accepts either v2 zl or zl modules. The default is Compatibility Mode enabled. If Compatibility Mode is disabled by executing the **no allow-v1-modules command**, the switch will only power up v2 zl modules.

***Syntax***: [no] allow-v1-modules

*Enables Compatibility Mode for inter-operation of v2 zl and zl modules in the same chassis.*

*The* **no** *form of the command disables Compatibility Mode. Only the v2 zl modules will be powered up.*

*Default: Enabled.*

The following table shows how the v2 zl and zl modules behave in various combinations and situations when Compatibility Mode is enabled and when it is disabled.

| Modules | Compatibility Mode Enabled | Compatibility Mode Disabled |
|---|---|---|
| v2 zl modules only | Can insert zl module and the module will come up. Any v2 zl modules are limited to the zl configuration capacities. | v2 zl modules are at full capacity.<br>ZL modules are not allowed to power up. |
| Mixed v2 zl and zl modules | Can insert zl module and the module will come up. Any v2 zl modules are limited to the zl configuration capacities.<br>But if compatibility mode is disabled, the zl modules go down. | ZL modules are not allowed to power up. |
| ZL modules only | Same as exists already.<br>If a v2 zl module is inserted, then it operates in the same mode as the zl module, but with performance increases. | The Management Module is the only module that powers up. |
| | In Compatibility Mode, no v2 zl features are allowed whether the modules are all v2 zl or not. | If Compatibility Mode is disabled, and then enabled, the startup config is erased and the chassis will reboot. |

```
Switch(config)# allow-v1-modules
This will erase the configuration and reboot the switch.
Continue [y/n]?
```

**Figure 1. Example of Enabling Compatibility Mode**

```
Switch(config)# no allow-v1-modules
All V1 modules will be disabled. Continue [y/n]?
```

**Figure 2. Example of Disabling Compatibility Mode**

## Authorized IP Managers Precedence

Page 15-2 in the Access Security Guide dated June 2010 (and earlier versions) for switches running version K software incorrectly states that the Authorized IP Managers feature takes precedence over Port-Based Access Control (802.1X) and Port Security. The 802.1X and Port Security features are *network* authentication methods, and do not apply to authenticating clients to manage the switch itself. The first sentence in the second paragraph on page 15-2 should read as follows:

> "Also, when configured in the switch, the Authorized IP Managers feature takes precedence over local passwords, TACACS+, and RADIUS."

## Minimum Guaranteed Bandwidth Issue

When 10 Mbps ports on an 8200zl or 5400zl switch are configured in QoS for eight outbound queues (the default), and the guaranteed minimum bandwidth is set for 5 Mbps or less for a given queue, then packets in the lower-priority queues may be discarded on ports that are oversubscribed for extended periods of time. If the oversubscription cannot be corrected, HP recommends reconfiguring the switch to operate with four outbound queues. The command to do this is:

```
HPswitch(config)# qos queue-config 4-queues
```

This issue applies to 8200zl and 5400zl switch operating with any of the following modules installed.

| HP Device | Product Number | Minimum Supported Software Version |
|---|---|---|
| HP 24-port 10/100/1000 PoE+v2 zl Module | J9534A | K.15.02.0004 |
| HP 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module | J9535A | K.15.02.0004 |
| HP 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl Module | J9536A | K.15.02.0004 |
| HP 24-port 10/100 PoE+ v2 zl Module | J9547A | K.15.02.0004 |
| HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module | J9548A | K.15.02.0004 |
| HP 20-port Gig-T / 4-port SFP v2 zl Module | J9549A | K.15.02.0004 |
| HP 24-port Gig-T v2 zl Module | J9550A | K.15.02.0004 |
| HP 12-port Gig-T / 12-port SFP v2 zl Module | J9637A | K.15.02.0004 |

# Version K.15.03.0005 Clarifications

## Loss of Event Log on Upgrade/Downgrade

As a result of the new method of storing the event log in switch memory, event log entries created in K.15.01 or K.15.02 software versions will be erased when upgrading to K.15.03 or later software. Also, event log entries created in K.15.03 and later software will be erased when back-revving to K.15.02 and earlier software versions.

## RADIUS Server Authentication Issue

Because of an inconsistency between the Windows XP 802.1x supplicant timeout value and the switch default timeout value, which is 5, when adding a backup RADIUS server, set the radius-server timeout value to 4 on the switch. Otherwise, the switch may not failover properly to the backup RADIUS server.

# Version K.15.07.0002 Clarifications

## Distributed Trunking Cannot Coexist with MAC-based Mirroring

Beginning with software version K.15.07, the switch will not allow both Distributed Trunking and MAC-based Mirroring to function simultaneously. The switch will respond as follows:

- If the user attempts to configure both, an error message will appear.
- When a switch is updated from older software to K.15.07, if the older config file has both Distributed Trunking and MAC-based Mirroring, the switch will automatically remove the MAC-based Mirroring lines from the config file, and will give an explanatory error message.
- If a switch is running K.15.07 and an existing config file that has both Distributed Trunking and MAC-based Mirroring is loaded onto the switch, the switch will automatically remove the MAC-based Mirroring lines from the config file, and will give an explanatory error message.

## Enhancement Inadvertently Listed

The "Event Log Severity Change" enhancement that was inadvertently listed in K.15.07.0002 Release Notes is not included in K.15.07.0002 software. That entry was removed from these release notes.

# Known Issues

**Note** Version K.15.01.0031 is a major software release, and was developed from Version K.14.41.

Features, enhancements, software fixes and known issues in K.15.01.0031 and later versions will differ from K.14.42 and later versions.

Known Issues are listed in chronological order of the software version, oldest to newest. For Known Issues in prior versions (K.14.*xx* or earlier), see the Release Notes provided with those versions.

## Version K.15.01.0031 Known Issues

- **OSPF (PR_0000054952)** — [RESOLVED in K.15.01.0032] HP Switch does not accept Type 7 default route in a NSSA when announced by Cisco.
- **VRRP (PR_0000055742)** — [RESOLVED in K.15.01.0032] VRRP Fast Failover fails for HA when advertisement interval is less than 1.
- **File Transfer (PR_0000048178)** — [RESOLVED in K.15.01.0032] If a switch is rebooted through software (CLI, Web, or SNMP) after starting to transfer a new software image to the switch using Secure Copy or SSH File Transfer Protocol, it may abort the image transfer in progress, and reboot to the existing version of the switch software.
- **802.1X (PR_0000054821)** — [RESOLVED in K.15.01.0032] Client with valid credentials is not able to reach authorized-vid when mixed mode and unauthorized-vid are set.

  **Expected Results**: The client with invalid credentials should be sent to the unauthorized VLAN and the client with the valid credentials should be sent to the authorized VLAN and be able to ping that VLAN.

  **Current Results**: The client with the valid credentials is correctly authenticated but it is not able to ping the auth-vid.
- **Crash (PR_0000055882)** — [RESOLVED in K.15.01.0032] IPv4 loopback address which followed an IPv6 EUI-64 address in configuration would cause a crash.
- **OSPF (PR_0000046029)** — [RESOLVED in K.15.02.0004] OSPF Virtual Links cause route flapping.
- **DAC (PR_0000050635)** — [RESOLVED in K.15.02.0004] DAC port flaps after reboot.
- **SFLOW (PR_0000041583)** — [RESOLVED in K.15.02.0004] Not sending vlan tag in sFlow data.

## Version K.15.02.0004 Known Issues

- **PoE (PR_0000060884)** — When using TFTP to copy a pre-K.15 configuration file onto a switch running K.15 software, if the value of **pre-std-detect** was “disabled” in the pre-K.15 config file, the value of **pre-std-detect** will be “enabled” after the file transfer. Workaround: manually disable **pre-std-detect** after the file transfer.
- **Services Module (PR_0000053005)** — In some cases the Services Module will initially fail to boot, but will then recover. During the initial boot failure, the switch Fault LED and the slot LED on the System Support Module will be lit, as well as the module status LED on the Services Module. After the module boots successfully, the Services Module LEDs will correctly indicate that it is functioning properly, but the switch Fault LED and slot LED on the System Support Module will incorrectly remain lit.

- **SFTP (PR_0000060656)** — When connecting to a switch via SFTP, if the user enters the command **ls /cfg**, the switch may appear unresponsive for a period of time. The console will recover, but it might be unresponsive for one minute or more.
- **UDLD (PR_0000058636)** — [RESOLVED in K.15.03.0003] UDLD can take up to 5 seconds to bring a port online, which may cause issues with VRRP.

## Version K.15.03.0005 Known Issues

- **Event Log (PR_0000060511)** — When the switch experiences a brief power outage, the event log might give erroneous indications regarding the cause and the results. Specifically, the switch might report that a) the switch rebooted due to the reset button being pressed, and b) the switch booted from secondary flash because primary flash is corrupt. Both these indications are false. The output of **show version** confirms that the switch booted from primary flash and is running the software from primary flash.

## Version K.15.05.0001 Known Issues

- **MAC-Based VLANs (PR_0000071068)** — When a client moves from one port on a v2 zl module to another port on the same v2 zl module, there is a delay before the client becomes authenticated on the new port. Workaround: reduce the logoff-period from the default of 300 to 180 seconds, to minimize the delay.
- **Passwords (CR_0000103309)** —[RESOLVED in K.15.08.0007] If the switch is configured with a manager and/or operator password, a username must be configured in addition to the password. This is a new requirement beginning with K.15.05 software; when connecting to the switch a user will be prompted for the username. Workaround: Before updating software, be sure to configure a username, or the switch will not be accessible after updating.

## Version K.15.08.0007 Known Issues

- **Switch Hang (CR_0000106245)** — [RESOLVED in K.15.08.00008] The switch might fail to boot fully, requiring a power-cycle to recover.

## Version K.15.09.0003 Known Issues

- **CLI (PR_0000071398, CR_0000076389)** - Previous software versions allowed configuration of VLAN IP addresses in overlapping subnets, which can cause mis-routing of packets and IP communication failure. With this fix, the switch no longer allows overlapping subnet configurations. The switch takes these actions when booting into K.15.09 or later software, if the config file includes overlapping subnets:
  - The event log gives an error message similar to `ip: VLAN8: IP initialization failed for vlan 8`
  - The output of **show ip** correctly indicates that the overlapping IP does not exist on the VLANs that have error messages in the event log
  - The output of **show run** incorrectly indicates that the overlapping IP is configured. The information is retained in the config file to allow a user to boot up and function as configured with earlier software that allows overlapping subnets.
  - If the user attempts to remove the overlapping subnet from the VLAN, the switch gives an error message similar to `The IP address 10.10.8.1/24 is not configured on this VLAN`, because from the switch's perspective the overlapping IP address does not exist.
    - Use the **show ip** command to see what addresses exist from the switch's perspective.

– The user can remove the phantom IP address from the config file only by removing all IP addresses from the VLAN in question, with the command **no ip address**. Be sure to document the other valid IP addresses on that VLAN, so they can be reinstated after the phantom IP address is removed.

### Operating Notes:

1. The overlap is determined by order of configuration.
2. For a multinetted VLAN (with several IP addresses assigned), only the IP addresses that are overlapping subnets are removed. Other IP addresses on the VLAN are retained and function properly, so in that situation the event log error message `IP initialization failed` is misleading.

# Enhancements

**Note** Version K.15.01.0031 is a major software release, and was developed from Version K.14.41.

Features, enhancements, software fixes and known issues in K.15.01.0031 and later versions will differ from K.14.42 and later versions.

This section lists only the software versions that contain enhancements. Enhancements are listed in chronological order, from oldest to newest software version. Unless otherwise noted, each new software version includes all the enhancements added in previous versions.

## Version K.15.01.0031 Enhancements

### Cached Re-authentication

- **Enhancement (PR_0000011015)** — Cached Re-authentication (Hold State if Radius Server Unavailable). For more information, see the "RADIUS" chapter in the *Access Security Guide* for your switch.

### Flapping Transceiver Mitigation

- **Enhancement (PR_0000017201)** — The switch Fault Finder function has been extended to cover an improperly behaving fiber transceiver, or other condition which results in a link "flapping" rapidly between link-up and link-down states. For more information, see the "Troubleshooting" appendix in the *Management and Configuration Guide* for your switch.

### Reduced Down Time When C-RP Not Reachable

- **Enhancement (PR_0000040783)** — This enhancement reduces the down time when unicast routing indicates a Candidate Rendezvous Point (C-RP) is not reachable. For more information, see the "PIM-SM (Sparse Mode)" chapter in the *Multicast Routing Guide* for your switch.

### Enhanced AAA Accounting

- **Enhancement (PR_0000041022)** — Enhancement to AAA accounting. For more information, see the "RADIUS" chapter in the *Access Security Guide* for your switch.

### Debug Capability for PIM Packet Events

- **Enhancement (PR_0000041395)** — Debug capability for PIM packet events is added. For more information, use the CLI help for syntax details, and see the "Troubleshooting" appendix in the *Management and Configuration Guide* for your switch.

### VRRP Ping Virtual IP of Backup

- **Enhancement (PR_0000041472)** — VRRP Ping Virtual IP of Backup. For more information, see the chapter "Virtual Router Redundancy Protocol (VRRP)" in the *Multicast and Routing Guide* for your switch.

### OOBM Port Enabled for IPv6 Host

- **Enhancement (PR_0000045438)** — The Out Of Band Management (OOBM) port on the HP Switch 6600 Series is now enabled for IPv6 host functionality. For more information, see the appendix "Network Out-of-Band Management (OOBM) for the 6600 Switch" in the *Management and Configuration Guide*.

### Module Reload (5400zl and 8200zl switches)

- **Enhancement (PR_0000045749)** — Module reload enhancement for 5400zl and 8200zl switches. For more information, see the chapter "Switch Memory and Configuration" in the *Basic Operation Guide* for your switch.

## Version K.15.01.0032 Enhancements

### Username and Password Size Increase

- **Enhancement (PR_0000018479)** — Longer usernames and passwords are now allowed, and some special characters may be used. For more information, see the chapter "Configuring Username and Password Security" in the *Access Security Guide* for your switch.

## Version K.15.02.0004 Enhancements

### Multicast ARP Support

- **Enhancement (PR_0000018427)** — Multicast ARP support enhancement to enable acceptance of MAC addresses in the IP multicast range. For more information, see the chapter "Multimedia Traffic Control with IGMP" in the *Multicast Routing Guide* for your switch.

### Display Configuration of Selected Interface

- **Enhancement (PR_0000044183)** — Display interface configuration enhancement. For more information, see the chapter "Switch Memory and Configuration" in the *Basic Operation Guide* for your switch.

### Post-logon Banner Enhancement

- **Enhancement (PR_0000045649)** — Post-logon banner enhancement. For more information, see the chapter "Getting Started" in the *Basic Operation Guide* for your switch.

### Support for the Tilde (~) Character in TACACS+ and RADIUS Keys

- **Enhancement (PR_0000045707)** — The tilde character is now allowed in TACACS+ and RADIUS encryption keys. For more information, see the chapters "Web and MAC Authentication" and "Configuring Port-Based and User-Based Access Control (802.1X)" in the *Access Security Guide* for your switch. For more information about TACACS+, see the chapter 'TACACS+ Authentication" in the *Access Security Guide* for your switch. For more information about RADIUS keys, see the chapter "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide* for your switch.

### Web Auth Deny Message

- **Enhancement (PR_0000045711)** — Web authentication message enhancement to allow administrators to configure custom messages that are displayed when authentication with the RADIUS server fails. For more information, see the chapter "Web and MAC Authentication" in the *Access Security Guide* for your switch.

## Port Security Per-Port MAC Increase

- **Enhancement (PR_0000045752)** — Increases the number of user-configurable per-port MAC addresses from 32 to 64 addresses. The switch-wide per-port address limit is unchanged. For more information, see the chapter "Configuring and Monitoring Port Security" in the *Access Security Guide* for your switch.

## PoE with LLDP

- **Enhancement (PR_0000046912)** — Adds support for LLDP PoE+. For more information, see the chapter "Power Over Ethernet (PoE/PoE+) Operation" in the *Management and Configuration Guide* for your switch.

## Support for Additional Switches and Modules

- **Enhancement (PR_0000048021)** — Support was added for the following products.

  J9310A - HP 3500yl-24G-PoE+ Switch
  J9311A - HP 3500yl-48G-PoE+ Switch
  J9312A - HP 10-GbE 2-Port SFP+/2-Port CX4 yl Module.

## Interrupt-Driven Port-Down Notification

- **Enhancement (PR_0000050143)** — Adds the ability for Interrupt-Driven Port-Down Notification.
  Note: This enhancement was inadvertently omitted from the published K.15.02.0005 Release Notes.

## Increase MAC Auth Client Limit to 256

- **Enhancement (PR_0000052732)** — Enhancement to increase the MAC Authentication Client Limit to 256. For more information, see the chapter "Configuring Port-Based and User-Based Access Control (802.1X)" in the *Access Security Guide* for your switch.

## Categorize CLI Return Messages

- **Enhancement (PR_0000052801)** — Enhancement to add a prefix to CLI command return messages indicating the type of message. For more information, see the chapter "Using the Command Line Interface (CLI)" in the *Basic Operation Guide* for your switch.

## Energy Efficient Ethernet (EEE)

- **Enhancement (PR_0000055430)** — Adds support for Energy Efficient Ethernet (IEEE 802.3az). For more information, see the appendix "Power-Saving Features" in the *Management and Configuration Guide* for your switch.

## Support for the SFP+ ER Transceiver

- **Enhancement (PR_0000055751)** — Support was added for the following product.

  J9153A – 10-GbE SFP+ ER Transceiver (J9153A HP X132 10G SFP+ LC ER Transceiver)

## Sync of 802.1X Supplicants for Nonstop Switching

- **Enhancement (PR_0000057058)** — Adds this feature to Nonstop Switching: synchronization for 802.1X supplicants originating from the switch. For more information, see the chapter "Chassis Redundancy (8200zl Switches) in the *Management and Configuration Guide* for your switch.

### Support for the v2 zl Modules

- **Enhancement(PR_000057799)** — Support was added for the following products.

  J9534A - HP 24-port 10/100/1000 PoE+ v2 zl Module
  J9535A - HP 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module
  J9536A - HP 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl Module
  J9537A - HP 24-port SFP v2 zl Module
  J9538A - HP 8-port 10-GbE SFP+ v2 zl Module
  J9547A - HP 24-port 10/100 PoE+ v2 zl Module
  J9548A - HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module
  J9549A - HP 20-port Gig-T / 4-port SFP v2 zl Module
  J9550A - HP 24-port Gig-T v2 zl Module
  J9637A - HP 12-port Gig-T / 12-port SFP v2 zl Module

## Version K.15.03.0003 Enhancements

### Custom Default Configuration

- **Enhancement (PR_0000045685)** — Allows creation of a custom default configuration for the switch. For more information, see the chapter “Switch Memory and Configuration” in the *Basic Operation Guide* for your switch.

### SNMP Trap Upon Addition or Deletion of Port MAC Addresses

- **Enhancement (PR_0000045796)** — Adds the ability to enable SNMP traps when MAC addresses are added to or deleted from a port. For more information, see the chapter “Configuring for Network Management Applications” in the *Management and Configuration Guide* for your switch.

### SNMP Trap and Log Message When Startup Config Updated

- **Enhancement (PR_0000052266)** — Adds the ability to enable an SNMP trap when the switch's startup configuration is changed. A log message is always generated for such changes. For more information, see the chapter “Configuring for Network Management Applications” in the *Management and Configuration Guide* for your switch.

### Show MAC with VLAN

- **Enhancement (PR_0000052738)** — Adds VLAN information to the output of the **show mac-address** commands. For more information, see the appendix “Monitoring and Analyzing Switch Operation” in the *Management and Configuration Guide* for your switch, and the chapter “Configuring and Monitoring Port Security” in the *Access Security Guide* for your switch.

### Outbound Queue Monitor

- **Enhancement (PR_0000054042)** — Adds the ability to monitor egress queues for dropped packets when QoS is configured. For more information, see the chapter “Quality of Service: Managing Bandwidth More Effectively” in the *Advanced Traffic Management Guide* for your switch.

### Show OSPF Neighbor Timers

- **Enhancement (PR_0000054055)** — This enhancement provides the ability to display OSPF neighbor timer information. For more information, see the chapter “IP Routing Features” in the *Multicast Routing Guide* for your switch.

### IP Enable/Disable for All VLANs

- **Enhancement (PR_0000054183)** — This enhancement provides the ability to disable the IP addresses on specified VLANs, without deleting the configured IP addresses or the other Layer 3 configuration. For more information, see the "Static Virtual LANs (VLANs)" chapter in the *Advanced Traffic Management Guide* for your switch.

### Logging for Routing ACLs

- **Enhancement (PR_0000055367)** — Adds the ability to log ACL **permit** entries in the same manner that ACL "deny" entries are currently logged. For more information, see the chapter "IPv4 Access Control Lists (ACLs)" in the *Access Security Guide* for your switch.

### Trunk Load Balancing Using L4 Ports

- **Enhancement (PR_0000058115)** — Allows the use of TCP/UDP source and destination port number for trunk load balancing. For more information, see the chapter "Port Trunking" in the *Management and Configuration Guide* for your switch.

### Wake-on-LAN Support Across VLANs

- **Enhancement (PR_0000058512)** — Adds Wake-on-LAN support across VLANs. For more information, see the "IP Routing Features" chapter in the *Multicast Routing Guide* for your switch.

### Syslog via TCP

- **Enhancement (PR_0000058564)** — Adds the ability to send syslog messages via TCP. For more information, see "Debug/Syslog Operation" in the "Troubleshooting" appendix of the *Management and Configuration Guide* for your switch.

### SNMP Trap on Running Configuration Changes

- **Enhancement (PR_0000058798)** — Adds the ability to enable an SNMP trap for any configuration change made in the switch's running configuration file. For more information, see the chapter "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

### Static Summary Route to RIP

- **Enhancement (PR_0000058804)** — Allows the redistribution into RIP of static black hole or reject routes. For more information, see the "IP Routing Features" chapter in the *Multicast Routing Guide* for your switch.

### Dynamic Port Access Auth via RADIUS

- **Enhancement (PR_0000060972)** — Enables configuration of RADIUS attributes for downstream supplicant devices. This allows a common port policy to be configured on all access ports by creating new RADIUS HP vendor-specific attributes (VSAs) that will dynamically override the authentication limits. For more information, see the chapter "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide* for your switch.

## Version K.15.04.0002 Enhancements

### DHCPv6 Client Authentication Options Added

- **Enhancement (PR_0000060667)** — Adds DHCPv6 client authentication options. For more information, see the "DHCPv6 Client Authentication" section in the *IPv6 Configuration Guide* for your switch.

### SSH Client

- **Enhancement (PR_0000060779)** — Allows the switch to act as an SSH client to connect to another HP switch. Also enhances SFTP to allow bidirectional secure copying of files between a switch and an SFTP server, initiated from the switch with the **copy** command. For more information, see the chapter "Configuring Secure Shell (SSH)" in the *Access Security Guide* for your switch. Additional information for IPv6 configuration can be found in the chapter "IPv6 Management Security Features" in the *IPv6 Configuration Guide* for your switch.

### Encoded Version Information Added to Config File

- **Enhancement (PR_0000061695)** — Adds encoded version information to the config file, (for example, Ver #01:00:01), to allow the switch to move between software versions that have different configuration options. The user should not modify this string. For more information on displaying the switch configuration, see the chapter "Switch Memory and Configuration" in the *Basic Operation Guide* for your switch.

### Fields Added to Authentication Requests

- **Enhancement (PR_0000063932)** — For improved interoperability with Cisco ACS, fields are now added in authentication requests for management telnet, ssh, and http service. For more information, see the chapter "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide* for your switch.

### Include RADIUS and TACACS Only Credentials

- **Enhancement (PR_0000064186)** — The **include-credentials** feature is enhanced to provide a **radius-tacacs-only** option to the command. For more information, see the chapter "Configuring Username and Password Security" in the *Access Security Guide* for your switch.

### OSPF Neighbor Shutdown Notification

- **Enhancement (PR_0000065022)** — Provides a way to gracefully shut down OSPF routing on HP switches without losing packets that are in transit. For more information, see the chapter "IP Routing Features" in the *Multicast and Routing Guide* for your switch.

### Accept CDP/LLDP Packets Tagged for VLAN 1

- **Enhancement (PR_0000065164)** — Allows incoming CDP and LLDP packets tagged for VLAN 1 to be processed even if VLAN 1 does not contain any ports. For more information, see the chapter "Configuring for Network Management Applications" in the *Management and Configuration Guide* for your switch.

### Define Cost of LSA Type 3 Summarized Prefix

- **Enhancement (PR_0000065218)** — Provides a way to define a fixed, user-assigned cost of an OSPF LSA type 3 summarized prefix. For more information, see the section "Configuring OSPFv3 on the Routing Switch" in the *IPv6 Configuration Guide* for your switch.

### Additional Support for zl Modules

- **Enhancement (PR_0000069103)** — Additional support added for zl modules. Adds support for the J9546A HP 8-port 10GBase-T v2 zl Module.

# Version K.15.05.0001 Enhancements

## OSPF, VRRP, and RIP Nonstop Routing

- **Enhancement (PR_0000051260)** — Adds Nonstop Routing for OSPF, VRRP, and RIP during a management module failover. See the "Chassis Redundancy" chapter in the *Management and Configuration Guide* for your switch.

## OSPFv2 Logging commands and command output

- **Enhancement (PR_0000052548)** — Adds improved logging, commands, and command output for OSPFv2 troubleshooting. See the "IP Routing Features" chapter in the *Multicast and Routing Guide* for your switch.

## VLAN Multicast Filter Global Configuration

- **Enhancement (PR_0000053047)** — Adds a global configuration option that allows each VLAN to have a multicast filter. See the "Multimedia Traffic Control with IP Multicast (IGMP)" chapter in the *Multicast and Routing Guide* for your switch.

## Distributed Trunking Switch-to-Switch

- **Enhancement (PR_0000063613)** — Adds support for switch-to-switch Distributed Trunking. See "Port Trunking" in the *Management and Configuration Guide*.

## MAC-Based VLANs

- **Enhancement (PR_0000064722)** — Adds support for MAC-Based VLANs on the v2 zl modules. See **"**MAC-Based VLANs" in the *Access Security Guide*.

## View Transceiver Diagnostic Optical Monitoring (DOM) Information

- **Enhancement (PR_0000066341)** — Adds the ability to view diagnostic monitoring information for transceivers with Diagnostic Optical Monitoring (DOM) support. See "Troubleshooting" in the *Management and Configuration Guide*.

## Override Reverse Path Forward (RPF) Lookup

- **Enhancement (PR_0000066432)** — Adds the ability to override the normal Reverse Path Forward (RPF) lookup mechanism so the router can accept multicast traffic on an interface other than that which would be normally selected. See "PIM-SM (Sparse Mode)" in the *Multicast and Routing Guide*.

## 10m and 15m Direct Attach Cables (DACs)

- **Enhancement (PR_0000067349)** - Adds support for the J9286B 10m and J9287B 15m Direct Attach Cables (DACs).

## Customized Commands for Local User Accounts

- **Enhancement (PR_0000069000)** — Provides additional control over user access to the switch by creating local user accounts that are authorized to use a customized set of commands. See "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide*.

## Spanning Tree Loop Guard

- **Enhancement (PR_0000069073)** — Adds the Spanning Tree loop guard feature, which prevents network loops when BPDUs are not received on a blocking port for various reasons ("BPDU starvation"). See "Multiple Spanning Tree Operation" in the *Advanced Traffic Management Guide* for your switch.

# Version K.15.05.0005 Enhancement

## Encrypt Credentials

- **Enhancement (PR_0000068734)** — Adds the ability to encrypt passwords and authentication keys in the config file. After enabling this feature, the resulting config file cannot be used by older software versions. Before enabling this feature, please refer to "Getting Further Software Management Information" on page 10. For more information about the feature, see the "Configuring Username and Password Security" chapter in the *Access Security Guide* for your switch.

# Version K.15.06.0006 Enhancements

## OSPF Stub Router Advertisement for OSPF v3

- **Enhancement (PR_0000071946)** — OSPF Stub Router Advertisement for OSPF v3 - renamed to better reflect the feature. For more information, see the "Introduction to OSPFv3" chapter in the *IPv6 Configuration Guide* for your switch.

## OSPF LSA Type 3 Summarized Prefix Cost

- **Enhancement (PR_0000071947)** — Define OSPF LSA Type 3 Summarized Prefix Cost for OSPF v3. For more information, see the "Introduction to OSPFv3" chapter in the *IPv6 Configuration Guide* for your switch.

## Transceiver Diagnostics

- **Enhancement (PR_0000070797)** — Display Transceiver Information to transceiver cable diagnostics. For more information, see the "Troubleshooting" appendix in the *Management and Configuration Guide* for your switch.

## MSTP Standards Compliant Based MIB

- **Enhancement (PR_0000060335)** — This enhancement implements full compliance with the IEEE standard for the SNMP MIB object **ieee8021MstpMib**. For more information, see the "Multiple Instance Spanning-Tree Operation" chapter in the *Advanced Traffic Management Guide* for your switch.

## MLDv2

- **Enhancement (PR_0000071588)** — IGMP v3 and MLD v2 capabilities were added to the switch. For more information, see the "Multicast Listener Discovery (MLDv1 and MLDv2)" chapter in the *IPv6 Configuration Guide* for your switch.

## 6in4 Tunneling

- **Enhancement (PR_0000072668)** — IPv6 over IPv4 tunneling is a way to establish point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers so that they can be carried over the IPv4 routing infrastructure. IPv6 over IPv4 tunneling provides a mechanism for utilizing the existing IPv4 routing infrastructure to carry IPv6 traffic between IPv6 networks. For information on configuring tunnels, see the "IPv6 Tunneling Over IPv4 Using Manually Configured Tunnels" chapter in the *IPv6 Configuration Guide*.

## OSPFv3 over 6in4 Tunnels

- **Enhancement (PR_0000072702)** — Both VLANS and tunnels can be assigned to areas and may be collectively referred to as an IP routing interface. For information on configuring tunnels, see the "IPv6 Tunneling Over IPv4 Using Manually Configured Tunnels" chapter in the *IPv6 Configuration Guide*.

## Policy Based Routing (PBR)

- **Enhancement (PR_0000072658)** — PBR provides the ability to manipulate a packet's path based on attributes of the packet. Traffic with the same destination can be routed over different paths, so that different types of traffic, such as VOIP or traffic with special security requirements, can be better managed. For more information, see the "Classifier-Based Software Configuration" chapter in the *Advanced Traffic Management Guide* for your switch.

## BGPv4

- **Enhancement (PR_0000073705)** — Border Gateway Protocol (BGP) support has been added. *Note: BGP authentication is not supported.* For more information, see the "BGP (Border Gateway Protocol)" chapter in the *Multicast and Routing Guide* for your switch.

## LACP Key

- **Enhancement (PR_0000069334)** — The **lacp key** option provides the ability to control dynamic trunk configuration. Ports with the same key will be aggregated as a single trunk. For more information see the "Port Trunking" chapter in the *Management and Configuration Guide* for your switch.

## LACP Debug Logging and Show Commands

- **Enhancement (PR_0000069334)** — LACP added to debug list. The **show lacp**, **show lacp peer**, and **show lacp counters** commands modified or added. For more information see the "Port Trunking" chapter and the "Troubleshooting" appendix in the *Management and Configuration Guide* for your switch.

## Displaying Information about LACP Trunk Load Balancing

- **Enhancement (PR_0000069334)** — The **show trunks load-balance interface** command displays the port on which the information will be forwarded out for the specified traffic flow with the specified source and destination address. For more information see the "Port Trunking" chapter and the "Troubleshooting" appendix in the *Management and Configuration Guide* for your switch.

## Uplink Failure Detection

- **Enhancement (PR_0000070161)** — Uplink Failure Detection (UFD) is a network path redundancy feature that works in conjunction with NIC teaming functionality. For more information, see the "Port Status and Configuration" chapter in the *Management and Configuration Guide* for your switch.

## PIM CLI enhancements

- **Enhancement (PR_0000068123)** — Enhanced the **router pim** command. For more information, see the "PIM-DM (Dense Mode)" and "PIM-SM (Sparse Mode)" chapters in the *Multicast and Routing Guide* for your switch.

## Support for Additional RPs and Multicast Groups

- **Enhancement (PR_0000070869)** — The administrator is now able to configure 8 static Rendezvous Points (RPs) and 8 multicast group ranges per static RP in PIM-SM mode. For more information, see the "PIM-SM" chapter in the *Multicast and Routing Guide* for your switch.

## Flight Data Recorder Log

- **Enhancement (PR_0000071572)** — Flight Data Recorder (FDR) logs information that is **"**interesting**"** at the time of the crash as well as when the switch is misbehaving, but not crashed. The crash-log and crash-data files now maintain data for the last 4 crashes instead of just the most recent. For more information about this feature, see the "File Transfers" and "Troubleshooting" appendices in the *Management and Configuration Guid*e for your switch.

# Version K.15.07.0002 Enhancements

## Show IP Route Summary

- **Enhancement (PR_0000065586, CR_0000072508)** — Displays the aggregate count of routes per routing protocol. See the *Multicast and Routing Guide*, "IP Routing" chapter.

## BGP Route Maps

- **Enhancement (PR_0000065723, CR_0000072572)** — Adds support for BGP route maps. See "BGP (Border Gateway Protocol)" in the *Multicast and Routing Guide*.

## Display Transceiver Command

- **Enhancement (PR_0000066341, CR_0000072917)** — Adds the ability to view diagnostic monitoring information for transceivers with Diagnostic Optical Monitoring (DOM) support. See "Troubleshooting" in the *Management and Configuration Guide*.

## OSPFv2 Range Metrics

- **Enhancement (PR_0000067641, CR_0000073680)** — Adds NSSA range metrics to OSPFv2. See the *Multicast and Routing Guide*, "IP Routing" chapter.

## Reporting Config Changes

- **Enhancement (PR_0000069196, CR_0000074531)** — This feature provides the ability to track and report information about switch management processes on a per-user, per-session basis. Syslog or RADIUS will be used for logging the information.

## sFlow IPv6

- **Enhancement (PR_0000069433, CR_0000074736)** — Adds support for sFlow using IPv6. See the *Management and Configuration Guide*, "Network Management" chapter.

## Router Advertisement (RA) Guard

- **Enhancement (PR_0000072298, CR_0000077209)** — The RA Guard feature restricts the ports (or trunks) that can accept IPv6 Router Advertisements (RAs). Additionally, ICMPv6 router redirects are blocked on the configured ports.

## SPF Throttling

- **Enhancement (PR_0000072987, CR_0000077793)** — SPF scheduling (throttling) allows the switch to delay SPF calculations when the network is unstable or there is a change in topology. See the *IPv6 Configuration Guide*, "OSPFv3 Routing" chapter, or the *Multicast and Routing Guide*, "IP Routing" chapter.

## Set sFlow Agent Address

- **Enhancement (PR_0000073083, CR_0000077874)** — This feature adds **sflow** as an option to the existing **ip source-interface** command, which provides the ability to specify the sFlow source agent address that is included in the packets sent from the switch to the sFlow collection nodes.

### MAC Limit Notify

- **Enhancement (PR_0000073085, CR_0000077875)** — The MAC Address Count feature provides a way to notify the switch management system when the number of MAC addresses learned on a switch port exceeds the permitted configurable number.

### DHCP Client DNS Support

- **Enhancement (PR_0000073284, CR_0000078031)** — Allows the configuration of the Domain Name Server (DNS) with DHCP. See the *Management and Configuration Guide*, Appendix C "Troubleshooting".

### BGP MD5 Authentication

- **Enhancement (PR_0000073738, CR_0000078395)** — Adds support for BGP MD5 authentication. See "BGP (Border Gateway Protocol)" in the *Multicast and Routing Guide*.

### Mesh ID

- **Enhancement (PR_0000093199, CR_0000093199)** — Adds the ability to configure a mesh ID. See the *Advanced Traffic Configuration Guide*, "Switch Meshing" chapter.

### BGP Route Filtering and Peer Restart Time Display

- **Enhancement (PR_0000102845, CR_0000102845)** — Adds support for filtering BGP routes by adding the option **bgp** to **show ip route**, and for displaying the BGP peer's graceful restart time with **show ip route bgp neighbor**. See "BGP (Border Gateway Protocol)" in the *Multicast and Routing Guide*.

## Version K.15.08.0007 Enhancements

### Comware CLI Commands in ProVision Software

- **Enhancement (CR_0000106070)** — This is the first of several phases that allows a Comware CLI proficient user to use their Comware CLI knowledge to generate equivalent ProVision software CLI commands to manage and configure ProVision software switches. This preliminary offering adds 21 simple Comware Display commands directly to the ProVision CLI, with additional troubleshooting and management commands planned for future software versions. See the *Comware CLI Commands in ProVision Software* manual for more details.

### Structured Config File Display

- **Enhancement (CR_0000106090)** — The structured option is an additional parameter for the **show running-config** and **show config** commands. Using the structured option, the command output is grouped together in a more logical manner. For more information, see the chapter "Switch Memory and Configuration" in the *Basic Operation Guide* for your switch.

### Grouped Config File Display

- **Enhancement (PR_0000071901)** — When executing the **show config** or **show running-config** commands, interfaces that have configuration settings are displayed together in order, only once, containing all the configuration commands for that interface. For more information, see the chapter "Switch Memory and Configuration" in the *Basic Operation Guide* for your switch.

# Version K.15.09.0003 Enhancements

## Concurrent Meshing and Routing

- **Enhancement (PR_0000068493, CR_0000074060**) - Meshing and routing now can be configured simultaneously. A packet can be routed into a mesh, or be switched through a mesh and then routed. Two routers can be connected by mesh links, which offers additional network topologies between routers and switches. Concurrent meshing and routing makes it possible to implement meshing throughout a broadcast domain without the need for additional switches or the use of another Layer 2 technology such as Spanning Tree to connect meshing domains with routing switches.

## RPVST+

- **Enhancement (PR_0000070948, CR_0000075993)** - RPVST+ is a proprietary spanning tree implementation that extends RSTP (802.1w) to run a separate spanning tree for each VLAN on the switch, and ensures that only one active, loop-free path exists between any two nodes on a given VLAN.

## Terminal Line Width and Length

- **Enhancement (CR_0000074537)** - For console/serial link and inbound telnet sessions, the switch output:
  - Uses whatever width is set by the terminal program. If width is not specified, 80 characters is the default.
  - Automatically wraps on word boundaries (such as spaces) for non-columnar output
  - Automatically wraps on column boundaries for columnar output
  - HP recommends that you do not set your terminal width **(terminal width <y>)** above 150 columns.

## MSTP Standards Compliant Based MIB (part 2)

- **Enhancement (CR_0000105360)** - This enhancement is a follow-on to PR_0000060335, which implements full compliance with the IEEE standard for the SNMP MIB object ieee8021MstpMib. This CR_0000105360 adds Single Instance STP information to the MIB.

## Flight Data Recorder Phase 2

- **Enhancement (CR_0000106140)** - The Flight Data Recorder provides a way to capture and preserve data that is related to a crash event. Phase 2 adds the capture and preservation of protocol and subsystem-specific information.

## CDPv2 Transmit Capability

- **Enhancement (CR_0000107011)** - When a Cisco VoIP phone boots up (or sometimes periodically), it queries the switch and advertises information about itself using CDPv2. The switch receives the VoIP VLAN Query TLV (type 0x0f) from the phone and then immediately sends the voice VLAN ID in a reply packet to the phone using the VLAN Reply TLV (type 0x0e). The phone then begins tagging all packets with the advertised voice VLAN ID.

## Comware CLI Commands in ProVision Software (Phase 2)

- **Enhancement (CR_0000114497)** - This is the second of several phases that allows a Comware CLI proficient user to use their Comware CLI knowledge to effectively manage and configure ProVision software switches. This phase adds 112 additional Comware display commands to the ProVision software CLI.

# Version K.15.10.0003 Enhancements

## MIB to Check Load of Module Slots

- **Enhancement (PR_0000073100, CR_0000077888)** - This feature provides SNMP read access to the CPU utilization of the modules. Currently the only method to retrieve the module CPU utilization is the CLI command **show cpu slot <slot | all>**. A new MIB table is created to facilitate the reading of information related to the module and its CPU utilization statistics.

## AAA Authorization on HTTPS

- **Enhancement (CR_0000103497)** - When using Commands authorization, the Web Agent windows may show or hide fields, or allow or deny configuration steps, based on the access or deny list (VSA filtering) for the authenticated user. For more information, see the chapter "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide* for your switch.

## IPv6 DNS via RA Options

- **Enhancement (CR_0000107183)** - IPv6 Router Advertisements allow IPv6 routers to advertise a list of recursive DNS Server (RDNSS) addresses and a DNS Search List (DNSSL) to IPv6 hosts. The new command options are **ipv6 nd suppress-ra-dns**, which is executed in the global config context, and **ipv6 nd ra suppress-dns**, which is executed in the VLAN context. For more information, see the chapter "IPv6 Router Advertisements" in the *IPv6 Configuration Guide* for your switch.

## Reinterpret CDP Info When Using IP Phones

- **Enhancement (CR_0000108063)** - Prevents MAC addresses from being learned on the specified ports when the VLAN is untagged and the destination MAC address is 01000c-CCCCCC (CDP), 0180c2-00000e (LLDP), or 0180c2-000003 (EAPOL). The feature is configured per-port by using the **ignore-untagged-mac <port-list>** command. For more information, see the chapter "Configuring for Network Management" in the *Management and Configuration Guide* for your switch.

## OpenFlow

- **Enhancement (CR_0000109154)** - OpenFlow is a programmable open-standard network protocol that uses flexible matching rules to classify and manage network traffic into flows. For more information, see the *OpenFlow Configuration Guide*.

## Comware CLI Commands in ProVision Software (Phase 3)

- **Enhancement (CR_0000115963)** - This is the third of four phases that allows a Comware CLI proficient user to use their Comware CLI knowledge to effectively manage and configure ProVision software switches. This phase adds 97 additional Comware display commands to the ProVision software CLI. With this addition there are now 230 Comware display commands in the ProVision software CLI.

# Software Fixes

**Note** Version K.15.01.0031 is a major software release, and was developed from Version K.14.41.

Features, enhancements, software fixes and known issues in K.15.01.0031 and later versions will differ from K.14.42 and later versions.

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

For software fixes in prior versions (K.14.*xx* or earlier), see the Release Notes provided with those versions.

## Version K.15.01.0031 Fixes

Status: Released and fully supported, and posted on the Web.
The following problems were resolved in software version K.15.01.0031.

- **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.
- **ACL/QoS (PR_0000045616)** — ACL/QOS Error return definitions as measured by the hardware layer are out-of-synch with SNMP values.
- **ACLs (PR_0000045003)** — Updated IPv6 rules for IDM ACLs.
- **Authentication (PR_0000043924)** — The switch responds with invalid PEAP packets when the RADIUS server request includes optional EAP TLVs, resulting in authentication failure.
- **Banner MOTD (PR_0000042871)** — The message returned by the CLI in response to the banner MOTD configuration command erroneously states that a banner of up to 3071 characters is supported; the actual maximum number of characters is 3070.
- **CLI (PR_0000009814)** — When an attempt is made to configure a mirror or monitor port for a 10-GbE transceiver not present in the switch, the error message is vague (`invalid value`). This fix provides a more meaningful error message.
- **CLI (PR_0000044704)** — The switch does not properly adjust terminal size display, if the user telnets to the switch and then changes the terminal size. This can cause the username to display when the password is requested, instead of a blank field.
- **CLI (PR_0000045556)** — Mesh ports cannot be configured to mirror or monitor. For example, when issuing the CLI command **int mesh monitor**, the switch reports: `Unknown port type`.
- **CLI (PR_0000047545)** — The CLI command **no telnet-server** is not saved in the config file.
- **CLI (PR_0000049955)** — The output of **show tech route** does not include all the information it is intended to provide.
- **CLI (PR_0000050078)** — When a PoE power supply is hot-swapped into a Switch 5400zl or 8200zl, the output of the CLI command **show system power** always lists the power supply as being 120 V, 875 W, even if it is a different voltage/wattage power supply.

- **CLI (PR_0000050088)** — If the user removes an interface module from the switch configuration (for example with the command, **no module 1**), an SNMP link-change trap configuration for ports on that module is truncated instead of removed from the configuration. For example, the configuration **no snmp-server enable traps link-change A1-A2** is truncated to **no snmp-server enable traps link-change**, which is an invalid configuration. If the user saves that configuration to a server, the config file cannot be successfully downloaded to the switch because of the incomplete command.
- **CLI Help (PR_0000046320)** — AAA command in-line help lists the options even after an option has already been typed into that command.

  ```
  Switch(config)# aaa authentication port-access chap-radius server-group pat cached-reauth?

  none           Do not use backup authentication methods.
  authorized     Allow access without authentication.
  cached-reauth  Grant access in case of reauthentication retaining the current
                 session attributes.
  <cr>
  ```

  The options should not be displayed, since an option (in this case, **cached-reauth**) has already been typed in the command line.
- **Command Authorization (PR_0000043525)** — HP-Command-String authorization does not work as expected.
- **Config (PR_0000040782)** — When an HP Gigabit 1000Base-T Mini-GBIC (J8177C) is configured with the **speed-duplex auto-100** setting, that configuration is lost from both running and startup configurations after a switch reload.
- **Config (PR_0000043984)** — The switch allows an inherent configuration conflict; the **rate-limit** and **service-policy** parameters should not be allowed concurrently on an interface.
- **Config (PR_0000046578)** — An IP BOOTP gateway configured on subnet zero is not displayed in the startup or running configuration file. The gateway is used correctly by the switch; this is a configuration display issue only.
- **Console Connectivity (PR_0000042248)** — The console port on a switch may get into a state where it appears to be unresponsive.
- **COS (PR_0000046599)** — The switch reports incorrect Class Of Service (COS) information in the output of the command **show port-access auth <port>** when the default COS (value 255) is in effect.
- **Crash (PR_0000018180)** — The switch may reboot unexpectedly during PIM-SM configuration and display a message similar to the following.

  ```
  Software exception at pim_sm_ctrl.c:376 -- in 'mPimsmCtrl'
  ```
- **Crash (PR_0000040241)** — The switch may reboot unexpectedly with a message similar to the following (message may vary).

  ```
  Software exception at hwBp.c:156 -- in 'mBSRCtrl', task ID = 0x7f06db0
  -> MemWatch Trigger: Offending task 'mPimsmCtrl'. Offending IP=0x845580
  ```
- **Crash (PR_0000041445)** — When Web Authentication is in use, the switch may experience conditions that cause it to reboot unexpectedly with a crash message similar to the following.

  ```
  Software exception at buffers.c:2231 -- in 'tHttpd', task ID = 0x80d25b0
  ```
- **Crash (PR_0000043167)** — When using TFTP with "octet" mode to upload the switch's configuration file, the switch may reboot unexpectedly with a message similar to the following.

  ```
  Software exception at hwBp.c:156 -- in 'eDevIdle', task ID = 0xabeb240
  -> MemWatch Trigger: Offending task 'tTftpDmn'. Offending IP=0x1cb174
  ```
- **Crash (PR_0000043217)** — If a VLAN containing a candidate RP is deleted, the switch will reboot unexpectedly, recording a crash message similar to the following.

```
Software exception at vls_util.c:133 -- in 'mBSRCtrl'
```

- **Crash (PR_0000044298)** — When RADIUS accounting is enabled, entering a command with too many characters entered at the CLI will crash the switch and record an error similar to the following.

```
Access Violation - Restricted Memory
Exception number: 0xdead0000
HW Addr=0x00000000 IP=0x00002680 Task='mftTask' Task ID=0xa941c80
fp: 0x30442030 sp:0x042333b
```

- **Crash (PR_0000046506)** — Execution of the CLI command **console local-terminal none** may cause the switch to reboot unexpectedly, logging a message similar to the following. Note that this problem was found and fixed on a special debug version of software; symptoms in released software, if any, may vary.

```
Software exception at parser.c:2373 -- in 'mSess1', task ID = 0xa931000 -> ASSERT: failed
```

- **Crash (PR_0000046643)** — With DHCP Snooping enabled on a VLAN, if a client requests a DHCP address and receives it from a trusted port, these changes can cause the switch to reboot unexpectedly:

  1) the client port is disabled

  2) the trusted port configuration is changed to be untrusted

  3) the client port is re-enabled and the client requests a DHCP address, but the response comes from the now-untrusted port

  The switch logs a message similar to the following.

```
Software exception at pmgr_util.c:1283 -- in 'mIpPktRecv', task ID = 0xa972cc0
```

- **Crash (PR_0000051910)** — SSH login to the switch might fail, and the switch may reboot unexpectedly with a message similar to the following.

```
NMI event SW:IP=0x00f64f88 MSR:0x02029200 LR:0x00f654dc cr:0x20000000
sp:0x05337598 xer:0x00000000 Task='tTelnetOut2' Task ID=0xa903000
```

- **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 (e.g. **dhcp-snooping trust Dyn1**), and this fix enforces that limitation at the CLI with an error message.
- **DHCP Snooping (PR_0000046831)** — The switch forwards DHCP Discovery packets out untrusted ports.
- **DHCP Snooping (PR_0000048426)** — With DHCP Snooping enabled, a client DHCP request is forwarded out untrusted ports.
- **Enhancement (PR_0000011015)** — Cached Re-authentication (Hold State if Radius Server Unavailable). For more information, see “Enhancements” on page 27.
- **Enhancement (PR_0000017201)** — The switch Fault Finder function has been extended to cover an improperly behaving fiber transceiver, or other condition which results in a link “flapping” rapidly between link-up and link-down states. A new fault event “link-flap” has been created to detect these events. Additionally, a new action, “warn-and-disable,” has been created to report and disable the events. Together, these enhancements allow the errant condition to be detected, and the port in question optionally disabled. For more information, see “Flapping Transceiver Mitigation” on page 27.
- **Enhancement (PR_0000040783)** — This enhancement reduces the down time when unicast routing indicates a Candidate Rendezvous Point (C-RP) is not reachable. For more information, see ““Reduced Down Time When C-RP Not Reachable” on page 27.
- **Enhancement (PR_0000041022)** — Enhancement to AAA accounting. For more information, see the “RADIUS” chapter in the *Access Security Guide* for your switch.

- **Enhancement (PR_0000041395)** — Debug capability for PIM packet events is added. For more information, see "Enhancements" on page 27.
- **Enhancement (PR_0000041472)** — VRRP Ping Virtual IP of Backup. For more information, see the chapter "Virtual Router Redundancy Protocol (VRRP)" in the *Multicast and Routing Guide* for your switch.
- **Enhancement (PR_0000045438)** — The Out Of Band Management (OOBM) port on the HP Networking Switch 6600 Series is now enabled for IPv6 host functionality.
- **Enhancement (PR_0000045749)** — Module reload enhancement. For more information, see "Module Reload (5400zl and 8200zl switches)" on page 28.
- **Event Log (PR_0000043041)** — When the switch downgrades a port from Gigabit to 10/100 operation, the resulting event log "`FFI`" message is displayed twice.
- **Fault Finder (PR_0000045772)** — When the switch fault-finder feature is configured to disable a transceiver port in response to link-flapping, and the disable has occurred, fault-finder will no longer properly disable that port following transceiver hot-swap.
- **GVRP (PR_0000012224)** — Changing the GVRP unknown-vlan state from 'block' to 'learn' and vice versa stops all GVRP advertisements from that interface until the interface is disabled and then re-enabled.
- **GVRP (PR_0000040238)** — After a dynamically-learned VLAN is converted to a static port-based VLAN, and an interface is made a static member of that VLAN, disabling GVRP causes the port to lose the VLAN membership. The running-config, startup-config and the SNMP egress static member list for the VLAN show the port as member of the VLAN. All other data shows the port is no longer a member of the VLAN. VLAN communication over the affected interface is no longer possible until the one of the two following workarounds is executed. Workarounds: Either re-issue the tag and untag commands for VLAN port assignment, or reload the system.
- **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).
- **IGMP (PR_0000018494)** — IGMP joins may cause multicast streams to flood, briefly, across the VLAN.
- **IP Communication (PR_0000043121)** — Execution and subsequent interruption of the CLI command **show tech route** during a vulnerability scan negatively affects IP communication.
- **IP Communication (PR_0000044004)** — Switches may experience a self-limiting resource leak in ICMP.
- **IPv6 (PR_0000045773)** — IPv6 duplicate address detection (DAD) does not work properly in some topologies.
- **LLDP (PR_0000048124)** — The LLDP Port VLAN ID TLV is incorrectly advertised as 0 for Trunked ports.
- **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.
- **Management (PR_0000016049)** — If a console or telnet session to the switch is used to execute a CLI command (for example, execution of the **show tech** command) and then the management session is abandoned before the task is completed (e.g., the window is closed), that session becomes unresponsive. If, at that point, another management session is established and the CLI command **kill** is executed to end the initial, now unresponsive session, the new management session will become unresponsive as well, until all sessions are in use and unresponsive.
- **Mini-GBIC (PR_0000044130)** — The HP Gigabit-SX-LC Mini-GBIC (J4858C) does not transmit after a switch reboot or hot-swap when it is used in a dual-personality port.
- **Module Crash (PR_0000043280)** — With IP routing and QinQ enabled, a switch module may reboot unexpectedly with a message similar to the following.

```
00374 chassis: Ports C: Lost Communications detected - Heart Beat Lost
```

- **MSTP/QinQ (PR_0000041219)** — When QinQ (Provider Bridging) is operating in mixed mode, switch identification of S-VLANs (Service VLANs) and C-VLANs (Customer VLANs) may be sometimes inaccurate. As a result, the switch allows S-VLANs to be assigned as members of MSTP instances and disallows some C-VLANs from being properly assigned to an MSTP instance.
- **Multicast (PR_0000041104)** — A software flaw was found which may have resulted in a variety of unexpected behaviors.
- **PC Phone/Authentication (PR_0000038652)** — When an IP phone is connected in tandem with a PC, the switch would not allow the PC user to be in an unauthenticated VLAN or authenticate using 802.1X, Web auth, or MAC authentication.
- **PIM (PR_0000012391)** — When OSPF, IGMP, and PIM are all configured, the switch reaches a sustained or increasing level of greater than 50% CPU utilization when a multicast stream with TTL=1 is received.
- **PIM (PR_0000018504)** — When a multicast stream is flowing through a PIM network using a better path (as determined by the DR) than the one through the rendezvous point, PIM does not adjust the multicast stream properly (it stops flowing) when PIM gets disabled on a VLAN along the data path.
- **PIM (PR_0000040412)** — When software is routing multicast packets, the packets are sent as CPU originated packets. As a result, features that rely on knowing the inbound source port (e.g., source port filtering) do not get applied.
- **PIM (PR_0000041887)** — When a PIM router is the elected Bootstrap Router (BSR), then fails a future BSR election, it keeps stale candidate Rendezvous Point (RP) information. If this device later becomes the elected BSR again, this stale information is then included in the BSM packets created by the BSR. This can cause long delays in failovers if the stale information includes RP's which are no longer reachable.
- **PIM (PR_0000043798)** — PIM debug output has the wrong bits set for (*,G) join-prune packets.
- **PIM (PR_0000050672)** — Fragmented PIM packets are not correctly routed by the switch.
- **PIM-SM (PR_0000012262)** — In a topology with a statically configured rendezvous point, a client's initial join will trigger receipt of the multicast stream. However, after leaving and re-joining the group, one of the following will happen.
  - If the multicast stream address is still present in the client's local router's multicast routing table, there is a delay of up to a minute after the IGMP join before the client receives the stream.
  - If the client's local router's multicast routing table has timed-out the multicast stream address, then the stream is never received by the client after it re-joins the group.
- **PIM-SM (PR_0000016110)** — When the DR_Priority option is configured to a value of zero (default priority is 1), the option is no longer included in the hello message as it should be.
- **PIM-SM (PR_0000040618)** — When the last known neighbor on an interface times out, PIM-SM fails to remove the flows which have that interface as the Reverse Path Forward (RPF) to the source. This causes the multicast streams to stop, instead of moving to the Reverse Path Tree (RPT) if possible.
- **PIM-SM (PR_0000040621)** — When information about a multicast group with any source (*,G) is received for downstream interfaces, the outbound list is only modified if it is a new *,G; it needs to be about to modify the outbound list for existing groups as well.
- **PIM-SM (PR_0000040825)** — Candidate-Rendezvous Point Advertisement (C-RP-Adv) messages are still sent out after the Candidate RP source-VLAN is down. This results in other PIM routers in the domain continuing to send Register messages to the unavailable RP.
- **PIM-SM (PR_0000041446)** — When a Bootstrap Router (BSR) receives a Candidate-RP Advertisement (C-RP-Adv) with a zero holdtime, it does not send a Bootstrap Message (BSM) with a zero holdtime; instead, it stops including the C-RP in subsequent bootstrap messages.

- **PIM-SM (PR_0000042163)** — Multicast traffic is lost for 20-30 seconds, approximately 5 minutes after a failed-over topology has recovered.
- **PIM-SM (PR_0000042263)** — PIM may send RPT joins or prunes to itself when it is the rendezvous point.
- **PIM-SM (PR_0000042433)** — When a multicast client joins and then leaves a multicast stream, there may be a delay of approximately 20 seconds before that client can join again.
- **PIM-SM (PR_0000042647)** — The PIM bootstrap router (BSR) has a memory leak when static rendezvous points are used.
- **PIM-SM (PR_0000042654)** — PIM may send a join or prune to a device that it inappropriately sees as an upstream neighbor.
- **PIM-SM (PR_0000043801)** — PIM is not sending compound (*,G) Prune (S,G) for SG's not joined.
- **PIM-SM (PR_0000045837)** — Following link failover and failback along the active data path, PIM-SM floods the UDP stream from the source to multiple RP's.
- **PoE (PR_0000045766)** — There are intermittent issues in the support of some pre-standard PoE phones; sometimes phones will boot and sometimes they don't. Grouping four or more phones together in consecutive ports may trigger this issue more often.
- **Port Access (PR_0000017541)** — The switch allows an inherent configuration conflict; port-based 802.1X should not be allowed concurrently with Web and MAC authentication.
- **Port Communication (PR_0000043048)** — The switch will not allow a port to link if the MDIX-MODE is set to MDI or MDIX (only the **auto-MDIX** setting will allow link).
- **Port Connectivity (PR_0000038601)** — The time between a port coming up and that port being online and passing traffic varies, and at times, may be extended to over a minute.
- **QoS (PR_0000042343)** — QoS on Ports may not behave correctly when trunks are involved, e.g., if QoS is configured on a port that is a member of a trunk, the CLI command **no qos** does not disable the feature as it should.
- **RADIUS (PR_0000045092)** — The Radius A/V pair option, 'NAS-IP-Address' does not get populated when the Out of Band Management (OOBM) port is the source of the packet.
- **RADIUS (PR_0000046154)** — MAC Based Radius Sessions go unauthenticated even if cached reauth is enabled when Radius Server Groups are set
- **RADIUS Accounting (PR_0000042522)** — The 'class' attribute is not included in the accounting-request to the RADIUS server; RFC 2865 states that this should occur.
- **Rate Limiting (PR_0000047195)** — HP ProCurve ONE environment protects the network from non-ONE applications by imposing rate limits on the ONE Services zl module ports. In some cases, a demonstration activation license for a ONE application is not interpreted correctly as a valid ONE activation license and the rate limits are imposed.
- **Redundant Management (PR_0000037617)** — Synchronization of redundant management modules on an 8200zl switch fails if there are more than 2 characters in the minor revision field of the switch system software version.
- **SNMP (PR_0000045869)** — When a large number of SNMPSET commands (on the order of 100 commands) are sent to the switch, at some point the switch runs out of room to store those entries. When the switch's memory limit is reached it gives this error message: `snmp: event 1997; events file too big; record not written.` This fix increases the available memory to allow the switch to accept up to 380 SNMPSET commands.
- **SNMP (PR_0000046735)** — Event log messages of type **"**Info**"** are sent as traps even after applying the configuration command **snmp-server host <IPaddress> <community> not-info**.

- **SNMP (PR_0000046906)** — Responses to SNMP queries on a switch configured with trunk groups are slow, which can lead to SNMP polling failures.
- **SNTP (PR_0000048717)** — The switch does not ensure the VLAN is up before sending SNTP requests, which can result in SNTP timeouts.
- **SSH (PR_0000014531)** — Rarely, after some period of time with normal SSH connectivity, the switch may become unresponsive to further SSH management.
- **SSH (PR_0000046860)** — After a client public key is copied to the switch via TFTP, if the user uses SSH to connect to the switch, when the SSH session is closed the switch reboots unexpectedly with a software exception message.
- **STP (PR_0000017189)** — When the switch is running in RSTP-mode (through the use of the CLI configuration command **spanning-tree force-version rstp-operation**) and MSTI settings are still present in the switch, a TCN is triggered when the MSTI settings are modified or removed.
- **TACACS (PR_0000047886)** — When a TACACS server is not available, the switch waits 40 seconds or more before the TACACS request is timed out and the configured secondary authentication method is tried. By default, the timeout should take 5 seconds.
- **Terminal Display (PR_0000008239)** — When a switch telnet session is opened from a Unix/Linux terminal, the line wrap of the terminal is not preserved after logout.
- **TFTP (PR_0000040441)** — When an attempt is made to download a configuration file from the TFTP server, there is an invalid error being logged if the config file does not exist on the TFTP server: `tftp: RCVD error:0, msg:.` Changes have been implemented so that the error message accurately indicates the cause of the file transfer failure.
- **TFTP (PR_0000046063)** — When the management VLAN is changed from the default (VLAN 1), the switch does not respond to TFTP requests.
- **Transceivers (PR_0000045170)** — The J8437A X2-SC LR Optic (transceiver) continues to transmit after the interface is disabled, which causes the far end to think the link is still up.
- **Transceivers (PR_0000045482)** — Some J9152A SFP+ LRM transceivers do not turn on the laser after the switch reboots. *Workaround*: remove, then re-insert the transceiver.
- **UDLD (PR_0000043071)** — UDLD transmits a burst of packets when any port on the switch goes down (1 packet is sent for each port that goes down), falsely triggering a failure state.
- **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.
- **UDLD (PR_0000050402)** — With UDLD enabled, a trunk that uses fiberoptic transceivers stops forwarding traffic after a switch reboot.
- **Unauthenticated VLAN (PR_0000010533)** — The switch allows an inherent configuration conflict; an unauthenticated VLAN (unauth-vid) can be configured concurrently for both 802.1X and Web/MAC authentication. This fix will not allow concurrent configuration of an unauth-vid for the **aaa port-access authenticator** and **aaa port-access web-based** or **aaa port-access mac-based** functions. Software versions that contain this fix will not allow this configuration conflict at the CLI. *Existing configurations will be altered by this fix*, and an error will be reported at the switch CLI and event log.

  **Best Practice Tip:** 802.1X should not have an unauthenticated VLAN setting when it works concurrently with Web-based or MAC-based authentication if the unauth-period in 802.1X is zero (the default value). Recall that the unauth-period is the time that 802.1X will wait for authentication completion before the client will be authorized on an unauthenticated VLAN. If 802.1X is associated with an unauthenticated VLAN when the unauth-period is zero, Web- or MAC-auth may not get the opportunity to initiate authentication at all if the first packet from the client is an 802.1X packet. Alternatively, if the first packet sent was not 802.1X, then Web- or MAC-auth could be initiated before 802.1X places the user in the

unauthenticated VLAN; when Web- or MAC-auth completes successfully, it will be awaiting traffic (to enable VLAN assignment) from the client but the traffic will be restricted to the unauthenticated VLAN, and thus the client will remain there.

If a MAC- or Web-based configuration on a port is associated with an unauth-VID, and an attempt is made to configure an unauth-VID for 802.1X (**port-access authenticator**), the switch with this fix will reject the configuration change with a message similar to one of the following.

- Message 1 (when an unauth-vid config is attempted on a port with an existing Web- or MAC-auth unauth-vid):

  ```
  Configuration change denied for port <number>. Only Web or MAC authenticator can have
  unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port.
  Please disable Web and MAC authentication on this port using the following commands:
  ```

  **no aaa port-access web-based <PORT-LIST>** or

  **no aaa port-access mac-based <PORT-LIST>**

  ```
  Then you can enable 802.1X authentication with unauthenticated VLAN. You can re-enable
  Web and/or MAC authentication after you remove the unauthenticated VLAN from 802.1X.
  Note that you can set unauthenticated VLAN for Web or MAC authentication instead.
  ```

- Message 2 (when an unauth-vid config is attempted on a port with an existing 802.1X unauth-vid):

  ```
  Configuration change denied for port <number>.Only Web or MAC authenticator can have
  unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port.
  Please remove the unauthenticated VLAN from 802.1X authentication on this port using
  the following command:
  ```

  **no aaa port-access authenticator <PORT-LIST> unauth-vid**

  Note that you can set unauthenticated VLAN for Web or MAC authentication instead.

- Message 3:

  ```
  Configuration change denied for port <number>. Only Web or MAC authenticator can have
  unauthenticated VLAN enabled if 802.1X authenticator is enabled on the same port.
  Please use unauthenticated VLAN for Web or MAC authentication instead.
  ```

  Event log message when the configuration is changed:

  ```
  mgr: Disabled unauthenticated VLAN on port <number> for the 802.1X.
  Unauthenticated VLAN cannot be simultaneously enabled on both 802.1X and Web or
  MAC authentication.
  ```

- **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.
- **VRRP (PR_0000018777)** — In a VRRP topology with two VRRP routers configured as Backup VRRP routers of the same priority, a simultaneous reboot of the two VRRP routers may lead to a situation where no VRRP router becomes the Master. This fix enhances VRRP functionality for skew time implementation as per RFC 3768.
- **VRRP (PR_0000049259)** — In some situations the VRRP Virtual IP does not respond to ping. This fix refines the enhancement introduced with PR_0000041472.

## Version K.15.01.0032 Fixes

Status: Never released.
The following problems were resolved in software version K.15.01.0032.

- **Authentication (PR_0000054821)** — With "mixed port access mode" enabled, a client with valid credentials is authenticated but not authorized on the authorized VLAN.
- **CLI (PR_0000056904)** — The output of the CLI command **show tech** does not include Standby Management Module (SMM) information.
- **Enhancement (PR_0000018479)** — Longer usernames and passwords are now allowed, and some special characters may be used. For more information, see page 28.
- **File Transfer (PR_0000048178)** — While loading switch software via Secure Copy (SCP) or TFTP, the switch can be rebooted by the user before the software file load completes.
- **File Transfer (PR_0000055817)** — During a software update to version K.15.xx, the part of the process that includes a System Support Module (SSM) update fails with the following error message.

```
Updating SSM ...Error on line 20: syntax error.
Program terminated.
```

- **IPv6 (PR_0000055882)** — After reboot, the switch's IPv6 EUI-64 addresses are changed from the configured values.
- **OSPF (PR_0000054952)** — Default routes in LSAs received from Area Border Routers are not accepted.
- **Spanning Tree (PR_0000056941)** — After a management module failover, ports on the switch might be erroneously blocked by Spanning Tree.
- **VRRP (PR_0000055742)** — If the VRRP advertisement interval is configured to be different than the default value of 1, failover from Active to Standby management module may take 15 seconds.

## Version K.15.01.0033 Fixes

Status: Released and fully supported, and posted on the Web.
The following problems were resolved in software version K.15.01.0033.

- **CLI (PR_0000058300)** — When the active and standby management modules are running different software versions (one boots from software in primary flash, the other boots from software in secondary flash), the output of the CLI command **show redundancy** incorrectly displays redundancy as `Nonstop switching` instead of `Warm-standby`.
- **OSPF (PR_0000057764)** — With OSPF routing and Spanning Tree enabled, if the Spanning Tree path cost is changed to force a specific link to block, the switch might reboot unexpectedly with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

```
OSPFv3 - Software exception at rt_table.c:4197 -- in 'eRouteCtrl',
task ID = 0xa968300-> Routing Stack: Assert Failed
```

## Version K.15.02.0004 Fixes

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.15.02.0004.

- **802.1X (PR_0000038874)** — When using 802.1X in client mode, the command **aaa port-access authenticator 1 client-limit 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.
- **802.1X (PR_0000047205)** — Cached reauthentication does not work with Windows XP running Service Pack 3.

- **Authentication (PR_0000054344)** — The request sent from switch to RADIUS server truncates the username to 16 characters, which causes authentication failure if the username is longer than 16 characters.
- **Authentication (PR_0000058602)** — A client using 802.1X, Web, or MAC authentication might lose access to the network immediately after being authenticated.
- **Banner MOTD (PR_0000053198)** — When using TACACS for telnet authentication, if a banner MOTD is longer than four lines, the first four lines of the banner are not visible on the screen.
- **CDP (PR_0000056202)** — When CDP is disabled with the CLI command **no cdp run**, the switch forwards CDP packets it receives.
- **CLI (PR_0000050756)** — When the user presses **"**<Ctrl>c**"** to cancel the output of a previously-issued command, in some cases the "<Ctrl>c" does not appear to have any effect, and the switch displays the remaining output of the previous command.
- **CLI (PR_0000050800)** — The output of the CLI command **show tech instrumentation** displays incorrect values for "port toggles".
- **CLI (PR_0000052748)** — The switch does not allow a VLAN number higher than 4 to be configured as the primary VLAN.
- **CLI (PR_0000059016)** — When the user types **logout** from a console session, the switch closes the session without the `Do you want to log out [y/n]?` and `Do you want to save current configuration [y/n/^C]?` prompts.
- **CPU Utilization (PR_0000059792, PR_0000061703)** — Certain situations with ECMP, a large number of routes (on the order of 3000), or use of the **clear arp** command, may result in high CPU utilization and decreased performance on the switch.
- **Crash (PR_0000039465)** — Rarely, a switch with DHCP Snooping configured may experience an unexpected reboot that triggers a crash message similar to the following.

```
TLB Miss: Virtual Addr=0x00000004 IP=0x800e3e30 Task='mDsnoop003'
Task ID=0x85dbb190 fp:0x00000000 sp:0x85dbae88 ra:0x80384c40 sr:0x1000fc01
```

- **Crash (PR_0000052464)** — A switch that has a large number of ACLs applied by the Identity Driven Manager (IDM) application might reboot unexpectedly with a message similar to the following.

```
Software exception at enDecode.c:54 -- in 'midmCtrl', task ID = 0xa946380
-> out of memory!
```

- **Crash (PR_0000054005)** — If an SFP+ transceiver or cable is present in the switch and the menu interface is used to make port or trunk configuration changes, the switch might reboot unexpectedly with a message similar to the following.

```
Access Violation - Restricted Memory
Exception number: 0xdead0000
HW Addr=0x3131393e IP=0x00002670 Task='mSess1' Task ID=0xa930640
fp: 0x05216200 sp:0x038ac7f0
```

- **Crash Messaging (PR_0000015799)** — Important data may be truncated from the crash message.
- **DHCP (PR_0000054749)** — When the switch acts as a DHCP relay agent, it erroneously removes the **"**end**"** option (code 255) from DHCP packets.
- **DHCP Snooping (PR_0000056774)** — When DHCP snooping is enabled, valid PXE boot packets that have yiaddr = 0.0.0.0 are dropped by the switch.
- **DIPLD (PR_0000052518)** — With Dynamic IP Lockdown enabled, there is no communication between clients on the switch.

- **Enhancement (PR_0000018427)** — Multicast ARP support enhancement. For more information, see "Multicast ARP Support" on page 28.
- **Enhancement (PR_0000044183)** — Display interface configuration enhancement. For more information, see "Display Configuration of Selected Interface" on page 28.
- **Enhancement (PR_0000045649)** — Post-logon banner enhancement. For more information, see "Post-logon Banner Enhancement" on page 28.
- **Enhancement (PR_0000045707)** — The tilde character is now allowed in TACACS+ and RADIUS encryption keys. For more information, see "Support for the Tilde (~) Character in TACACS+ and RADIUS Keys" on page 28.
- **Enhancement (PR_0000045711)** — Web authentication message enhancement. For more information, see "Web Auth Deny Message" on page 28.
- **Enhancement (PR_0000045752)** — User-configurable per-port MAC address enhancement. For more information, see "Port Security Per-Port MAC Increase" on page 29.
- **Enhancement (PR_0000046912)** — Adds support for LLDP PoE+. For more information, see "PoE with LLDP" on page 29.
- **Enhancement (PR_0000048021)** — Support was added for the following products.

  J9310A - HP 3500yl-24G-PoE+ Switch
  J9311A - HP 3500yl-48G-PoE+ Switch
  J9312A - HP 10-GbE 2-Port SFP+/2-Port CX4 yl Module.

- **Enhancement (PR_0000050143)** — Adds the ability for Interrupt-Driven Port-Down Notification.
  Note: This enhancement was inadvertently omitted from the published K.15.02.0005 Release Notes.
- **Enhancement (PR_0000052732)** — Enhancement to increase the MAC Authentication Client Limit to 256. For more information, please see "Increase MAC Auth Client Limit to 256" on page 29.
- **Enhancement (PR_0000052801)** — Categorize CLI Return Messages enhancement. For more information, please see "Categorize CLI Return Messages" on page 29.
- **Enhancement (PR_0000055430)** — Adds support for Energy Efficient Ethernet (IEEE 802.3az). For more information, please see "Energy Efficient Ethernet (EEE)" on page 29.
- **Enhancement (PR_0000055751)** — Support was added for the following product. J9153A 10-GbE SFP+ ER Transceiver (J9153A HP X132 10G SFP+ LC ER Transceiver)
- **Enhancement (PR_0000057058)** — Adds this feature to Nonstop Switching: synchronization for 802.1X supplicants originating from the switch.
- **Enhancement(PR_000057799)** — Support was added for the following products.

  J9534A - HP 24-port 10/100/1000 PoE+ v2 zl Module
  J9535A - HP 20-port 10/100/1000 PoE+ / 4-port SFP v2 zl Module
  J9536A - HP 20-port 10/100/1000 PoE+ / 2-port 10-GbE SFP+ v2 zl Module
  J9537A - HP 24-port SFP v2 zl Module
  J9538A - HP 8-port 10-GbE SFP+ v2 zl Module
  J9547A - HP 24-port 10/100 PoE+ v2 zl Module
  J9548A - HP 20-port Gig-T / 2-port 10-GbE SFP+ v2 zl Module
  J9549A - HP 20-port Gig-T / 4-port SFP v2 zl Module
  J9550A - HP 24-port Gig-T v2 zl Module
  J9637A - HP 12-port Gig-T / 12-port SFP v2 zl Module

- **Event Log (PR_0000050999)** — If the CLI command is issued to download software to the switch, and during that download an SNMP request to download software is sent to the switch, the resulting error message is garbled.

- **File Transfer (PR_0000039190)** — A configuration file that has a QoS policy applied to a VLAN (**vlan <vlan-id> service-policy <policy-name> in**) cannot be downloaded to the switch.
- **File Transfer (PR_0000054790)** — Switch software cannot be updated via HTTPS.
- **IGMP (PR_0000052737) —** With Forced Fast-Leave disabled (which is the default), upon receipt of a "leave" message from a client, the switch sends a Group Specific Query with a Max Response Time of zero seconds, which is not a valid value.
- **IP Communication (PR_0000053603)** — The switch responds to an ARP request received on one VLAN but sent from a different VLAN. This situation can occur when a client's port is moved from one VLAN to another, and the client sends an ARP request from an IP address on the original VLAN.
- **IP Communication (PR_0000053861)** — The switch is unable to telnet or ping to supernetted IP addresses, and supernetted IP addresses cannot be configured on the switch.
- **IPv6 (PR_0000056259)** — The switch does not use the longest matching prefix for default address selection, which violates rule 8 in section 5 of RFC 3484.
- **IPv6 (PR_0000056301)** — Autoconfigured addresses remain in effect after preferred and valid prefix lifetimes expire.
- **LLDP (PR_0000058583)** — After a switch port loses link, the output of **show power brief <port_number>** wrongly indicates that no PoE power is being delivered.
- **MSTP (PR_0000058462)** — Under certain circumstances, the switch might increment the Topology Change Count when it should not. The topology change is incorrectly detected on a link that is blocked at the far end.
- **Nonstop Switching (PR_0000050740)** — RADIUS accounting statistics are not maintained during a management module failover.
- **OSPF (PR_0000040435)** — If the switch is configured as an OSPF Area Border Router (ABR) with a Loopback 0 address assigned to area 0.0.0.0, the switch does not exchange inter-area routes after the last physical interface in area 0.0.0.0 goes down.
- **OSPF (PR_0000045110)** — With OSPF routing and OSPF traps enabled, the switch's available memory decreases over time.
- **OSPF (PR_0000046029)** — If there are routers in an OSPF area that do not support "demand circuits", virtual links (which are treated as demand circuits and should stop LSA aging) cause the LSAs to age out, causing SPF recalculation and periodic route flapping.
- **OSPF (PR_0000055768)** — After 255 topology changes, the next OSPF topology change resets the Shortest Path First (SPF) counter to 1 instead of incrementing to 256.
- **OSPF (PR_0000058797)** — With OSPF and VRRP enabled, a route to a specific host might be lost during a VRRP failover. The switch will display this event log message: `IpAddrMgr: Failed to add FIB entry - route matches existing next-hop router`.
- **PIM (PR_0000054424)** — When a multicast source is connected to a VLAN with multiple IP address ranges (a "multinetted VLAN"), and the multicast source is configured with an IP address in one of the secondary IP address ranges, the multicast streams are not forwarded by the switch.
- **PIM-SM (PR_0000050032)** — The switch logs erroneous `No pim neighbor on vid <VLAN-ID>, cannot send joinprune packet` messages. The event log messages are the only problem; PIM-SM functions properly.

- **PoE (PR_0000053516**) — If a faulty PoE+ power supply is installed in the zl Power Shelf, the switch does not properly indicate that the power supply is bad. Instead, the switch displays `0W /Connected` in the **show power-over-ethernet** output. With this fix, a) the command output displays `0W /Connected - Faulted`, b) an event log message is generated: `Ext Power Supply <power-supply-number> measured out of spec or is faulty. Please change or contact support.`, and c) the Power Supply Status LED flashes orange.
- **Port Connectivity (PR_0000050635)** — When 7-meter Direct Attach Cables (J9285B) connect two switches, if one of the switches is rebooted, the connected ports might begin to toggle offline/online repeatedly.
- **Rate Limiting (PR_0000045467)** — Ingress rate-limiting that is configured via RADIUS or Identity Driven Manager (IDM) is not applied to OSI Layer 2 traffic.
- **Routing (PR_0000053115)** — With the VLAN MAC Address Reconfiguration feature enabled, routed packets are forwarded at very slow rates if the switch's route table has a large number of entries.
- **sFlow (PR_0000012123)** — The switch does not allow sFlow to be configured on a mirror port.
- **sFlow (PR_0000041583)** — The switch does not send VLAN tag information in sFlow data.
- **Spanning Tree (PR_0000058714)** — After loading a configuration file with non-default Spanning Tree path costs defined for 10-Gigabit ports, the 10-Gigabit port path costs revert to their default value of 2000.
- **SSH (PR_0000052970)** — The output of a CLI **show** command may have truncated lines, when the **show** command is executed via an SSH login and the output is very large (on the order of 2 KB).
- **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.
- **TACACS (PR_0000052495)** — If the switch is configured to use TACACS for telnet access and the TACACS timeout is configured for a value greater than 75 seconds, the switch waits much longer than 75 seconds before timing out the TACACS request.
- **TELNET (PR_0000061481)** — When connecting to the switch via TELNET, if a router between the client and the switch has an MTU setting of less than 1500 bytes, the first attempt to TELNET fails.
- **TFTP (PR_0000046863)** — The switch experiences a loss of free memory each time a software image is downloaded via TFTP, unless there is a redundant management module installed.

## Version K.15.02.0005 Fixes

Status: Released and fully supported, and posted on the Web.
The following problems were resolved in software version K.15.02.0005.

- **OSPF (PR_0000063104)** — OSPF unicast packets are sent to the medium priority queue instead of the high priority queue.
- **SSH (PR_0000062414)** — When a configuration file is copied onto a switch and the switch reboots as a result of this copy, the SSH key information is deleted from the configuration file.

## Version K.15.03.0003 Fixes

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.15.03.0003.

- **802.1X (PR_0000005372)** — Some combinations of source and destination MAC addresses may cause 802.1X to stop functioning on a port; only a reboot will recover functionality.

- **ACLs (PR_0000059674)** — After updating switch software from K.13.58 or later (with a K.13 config file) to K.15 software, ACL rate-limit commands that are applied to multiple interfaces are duplicated for each interface in the config file. That is, a uniquely-numbered but identical policy is created for each interface, instead of applying a single policy to each interface. The policies function properly, but the config file is more difficult to interpret.
- **ACLs (PR_0000061483)** — The Access Control Entry (ACE) **permit tcp any <destination_IP> established** does not function properly.
- **Authentication (PR_0000058253)** — The switch's event log reports `auth: Invalid user name/password on SSH session`, even though the client is already authenticated.
- **BPDU Protection (PR_0000047748)** — This fix corrects the output of an SNMP query. Before the fix, the switch might incorrectly respond that BPDU protection is disabled on a port, when in fact it is enabled and functioning properly.
- **CLI (PR_0000015197)** — The CLI response to **sho int eth <port_number>** displays only the second half of the first byte of the MAC address. The switch response to **show mac** and other commands that list the MAC address accurately display the proper format of MAC addresses.
- **CLI (PR_0000061404)** — After configuring an SFP slot with the CLI command **speed-duplex 100-half** and saving the configuration, that setting is erased when the switch reboots.
- **Console (PR_0000001136)** — Rarely, the switch console may hang after a software image transfer to the switch. Workaround: **<Ctrl-C>** will restore the command prompt.
- **Counters (PR_0000062966)** — The Drops Tx counter is not reset when a port goes offline, which can cause erroneous FFI (Find, Fix, Inform) `High collision or drop rate` messages after the port comes back online.
- **Crash (PR_0000050103)** — The switch allows setMIB commands to create invalid configurations, which might cause the switch to reboot unexpectedly when the user issues the **show running-config** command, with a message similar to the following. Note that this problem was found and fixed on an internal development software build; symptoms in released software may vary.

  ```
  Software exception at cli_xlate.c:5340 -- in 'mSess1', task ID = > 0xa924e00
  ```

- **DHCP Snooping (PR_0000046276)** — With DHCP snooping enabled, a MAC-Authentication client whose session times out cannot reauthenticate.
- **Distributed Trunking (PR_0000048802)** — After powering down a switch participating in a distributed LACP trunk, the remaining switch does not take over the conversations previously running through the offline switch. Workaround: Do not power down a switch running Distributed Trunking. If a reload is required, first unplug the Distributed Trunk links from the switch, wait at least one minute, then unplug the Inter-Switch Connection (ISC), then reload or power down the switch.
- **Enhancement (PR_0000045685)** — Allows creation of a custom default configuration for the switch. For more information, see “Custom Default Configuration” on page 30.
- **Enhancement (PR_0000045796)** — Adds the ability to enable SNMP traps when MAC addresses are added to or deleted from a port. For more information, see “SNMP Trap Upon Addition or Deletion of Port MAC Addresses” on page 30.
- **Enhancement (PR_0000052266)** — Adds the ability to enable an SNMP trap when the switch's startup configuration is changed. For more information, see “SNMP Trap and Log Message When Startup Config Updated” on page 30.
- **Enhancement (PR_0000052738)** — Adds VLAN information to the output of the **show mac-address** commands. For more information, see “Show MAC with VLAN” on page 30.
- **Enhancement (PR_0000054042)** — Adds the ability to monitor egress queues for dropped packets when QoS is configured. For more information, see “Outbound Queue Monitor” on page 30.

- **Enhancement (PR_0000054055)** — This enhancement provides the ability to display OSPF neighbor timer information. For more information, see "Show OSPF Neighbor Timers" on page 30.
- **Enhancement (PR_0000054183)** — The user can now disable the IP addresses on specified VLANs, without deleting the configured IP addresses. For more information, see "IP Enable/Disable for All VLANs" on page 31.
- **Enhancement (PR_0000055367)** — Adds the ability to log ACL **permit** entries. For more information, see "Logging for Routing ACLs" on page 31.
- **Enhancement (PR_0000058115)** — Allows the use of TCP/UDP source and destination port number for trunk load balancing. For more information, see "Trunk Load Balancing Using L4 Ports" on page 31.
- **Enhancement (PR_0000058512)** — Adds Wake-on-LAN support across VLANs. For more information, see "Wake-on-LAN Support Across VLANs" on page 31.
- **Enhancement (PR_0000058564**) — Adds the ability to send syslog messages via TCP. For more information, see "Syslog via TCP" on page 31.
- **Enhancement (PR_0000058798)** — Adds the ability to enable an SNMP trap for any configuration change made in the switch's running configuration file. For more information, see "SNMP Trap on Running Configuration Changes" on page 31.
- **Enhancement (PR_0000058804)** — Allows the redistribution into RIP of static blackhole or reject routes. For more information, see "Static Summary Route to RIP" on page 31.
- **Enhancement (PR_0000060972)** — Enables configuration of RADIUS attributes for downstream supplicant devices. This allows a common port policy to be configured on all access ports by creating new RADIUS HP vendor-specific attributes (VSAs) that will dynamically override the authentication limits. For more information, see "Dynamic Port Access Auth via RADIUS" on page 31.
- **Event Log (PR_0000059300)** — Event log message #608 displays "`vlan 0`" instead of a valid failure type.
- **Guaranteed Minimum Bandwidth (PR_0000042500**) — The switch does not allow Guaranteed Minimum Bandwidth (GMB) to be configured on port L24. Also, a configuration file with GMB on port L24 fails to load onto the switch.
- **IP Communication (PR_0000042790)** — A very busy switch may cease all IP communication when the CLI command **show tech route** is executed. Messages similar to the following may be seen in the event log when this occurs.

```
W <date> <time> 00436 NETINET: 1 route entry creation(s) failed.
W <date> <time> 00075 system: Out of pkt buffers; miss count: 0
```

- **IP Connectivity (PR_0000046280)** — After updating software, the hostname is removed from the configuration and the switch does not respond to SSH requests.
- **LLDP-MED (PR_0000018681)** — LLDP-MED responses from a device connected to the switch are stored in the wrong order, which causes errors when the user uses **snmpwalk** to see the stored values on the switch.
- **Port Authentication (PR_0000043433)** — The switch allows the user to configure reauthentication on ports that are not yet configured for authentication. With this fix, an error message will be generated if the user attempts that invalid configuration.
- **Port Communication (PR_0000060305)** — The interrupt-driven port-down notification introduced in K.15.02 may, in rare situations, cause a port to block outgoing traffic after a switch reboot.
- **Port Communication (PR_0000061884)** — A PoE+ switch port configured with **speed-duplex auto-10-100** and connected to an Intel NIC 82566 with Wake on LAN enabled might stop responding after one or two hours. Workaround: configure the port with the **speed-duplex auto** setting.
- **Savepower (PR_0000056993)** — Savepower commands are not available on the 3500 series switches.

- **SNMP (PR_0000046848)** — SNMP traps are sent to the in-band VLAN, even if configured to send SNMP traps to the Out-of-Band Management (OOBM) interface. This fix adds an option in CLI to specify OOBM as the trap destination.
- **SNMP (PR_0000060189)** — The MIB object "dot3PauseOperMode" has incorrect information about the state of flow control on a port.
- **SNMP (PR_0000060257)** — The port type for 100-BX and 1000-BX transceivers is incorrectly identified when requested via SNMP.
- **SNTP Authentication (PR_0000048588)** — With SNTP authentication disabled, the switch sends extra, unnecessary authentication information in the SNTP request packet.
- **SSH (PR_0000045158)** — SSH login to the switch might fail.
- **Syslog (PR_0000012167)** — Syslog messages longer than 119 characters get truncated.
- **TELNET (PR_0000061045)** — After opening and then closing a Telnet session to another switch, the message `Telnet closed: Connection reset by peer` is displayed instead of `Telnet closed: Connection closed by host`.
- **UDLD (PR_0000058636)** — A port that is configured for UDLD may be in a UDLD blocking state for five seconds after the link comes up, which can cause issues with VRRP.
- **Web Authentication (PR_0000042284)** — When an EWA server is used for Web authentication, authentication is successful but custom graphics are not displayed.
- **Web Authentication (PR_0000048486)** — When an EWA server is used for Web authentication, the EWA login page is not presented properly with some versions of Safari Web browser.
- **Web Management (PR_0000054861)** — The Web "device view" of a switch shows the power supply status as green for all installed internal power supplies, even if a power supply is installed with no power cord connected.
- **Web Management (PR_0000060813)** — Using the Web interface, the close-up view of stack members might not display if the commander is configured for SSL-only access.

## Version K.15.03.0004 Fixes

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.15.03.0004.

- **CLI (PR_0000061969)** — The switch responds with `translator failed` messages when the user enters **copy config** and **show tech** commands. This is seen with very large configuration files.
- **Self Test (PR_0000064124)** — Rarely, the LEDs for one or more ports indicate "selftest failure" after switch reboot, although there is no message in the event log.
- **SNTP (PR_0000064369)** — When the switch updates its system time via SNTP, the event log entry does not include the IP address of the SNTP server, and the previous and updated times are not displayed.

## Version K.15.03.0005 Fixes

Status: Released and fully supported, and posted on the Web.
The following problem was resolved in software version K.15.03.0005.

- **OSPF (PR_0000065337)** — When routing information changes lead to OSPF recalculation, the switch can experience packet loss under heavy traffic loads.

## Version K.15.03.0006 Fixes

Status: Never released.
The following problems were resolved in software version K.15.03.0006.

- **CLI (PR_0000067688)** — The output of the **show system** command might display an incorrect value for Free Memory.
- **Crash (PR_0000066570)** — After a large number of startup configuration changes, the switch might reboot unexpectedly with a message similar to the following.

```
Unable to allocate message buffer
Software exception in ISR at btmDmaApi.c:370
```

- **Direct Attach Cables (PR_0000065839)** — Some Direct Attach Cables (DACs) might be identified as "unsupported" when inserted in a v2 zl module running software versions K.15.03.0003 through K.15.03.0005. This issue only affects DACs with part numbers 8121-1148, 8121-1149 and 8121-1155.
- **SNMP (PR_0000068087)** — Two of the OIDs related to SNTP are in the wrong sequence in switch software. The affected OIDs are `hpSntpInetServerIsOobm` and `hpSntpInetServerAuthKeyId`.

## Version K.15.03.0007 Fixes

Status: Released and fully supported, and posted on the Web.
The following problem was resolved in software version K.15.03.0007.

- **Transceivers (PR_0000066558)** — With one or more J8177B/C 1000Base-T Mini-GBICs (HP X121 1G SFP RJ45 T Transceivers) installed in a 6200yl switch running K.15.02 or K.15.03.0003 through K.15.03.0006 software, the J8177B/C in the highest-numbered slot will not link when the switch reboots. Workaround: hot-swap the transceiver that does not link.

## Version K.15.04.0002 Fixes

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.15.04.0002.

- **Authentication (PR_0000068384)** — When a PC is plugged into a VOIP phone and authenticated on that switch port, if the PC is moved to another VOIP phone without first logging out of Windows, authentication fails.
- **BootROM (PR_0000054240)** — This software version includes a BootROM update to BootROM version K.15.12.
- **CLI (PR_0000048578)** — The **<Ctrl-c>** break sequence does not work while the user is creating a custom login banner.
- **CLI (PR_0000053222)** — The CLI command **snmp-server trap-source** does not allow the user to configure the Out of Band Management (OOBM) IP address as the trap source.
- **CLI (PR_0000060966)** — Changing the terminal width to values larger than 100 might cause CLI messages to be truncated.
- **CLI (PR_0000064511)** — The switch might become unresponsive to management after issuing the CLI command **show connection-rate-filter all**.
- **CLI (PR_0000068580)** — The **copy crash-data** command copies the crash log (text) instead of the binary crash data.
- **Counters (PR_0000048733)** — The output of **show interfaces** has commas for large values in some, but not all fields. This fix makes the display consistent.

- **Crash (PR_0000055261)** — In some situations the switch might reboot unexpectedly with a message similar to the following.

```
SubSystem 0 went down: 06/22/10 09:24:00
NMI event SW:IP=0x00e953d8 MSR:0x02029200 LR:0x00eb25c8
cr: 0x24000400 sp:0x02e30aa8 xer:0x20000000
Task='InetServer' Task ID=0xaad5000
```

- **Crash (PR_0000064620)** — When a trunk type is changed from **trunk** to **LACP**, if the trunk is a higher-numbered trunk (e.g., trk11) and has an access group applied, the switch might reboot unexpectedly with a message similar to the following.

```
Execute Access Error - Restricted Memory
Exception number: 0xdead0300
HW Addr=0x70000000 IP=0x70000000 Task='mSnmpCtrl' Task ID=0x1a47e9c0
fp: 0x72756769 sp:0x
```

- **Crash (PR_0000066285)** — In rare situations where the loopback address is removed and then re-applied, and an **snmpwalk** is performed, a switch running OSPFv3 might reboot unexpectedly with a message similar to the following.

```
Software exception at ospf3_ls.c:10150 -- in 'eRouteCtrl', task ID = 0xa96ff00
-> Routing Stack: Assert Failed
```

- **Crash (PR_0000066961)** — With DHCP snooping enabled, the switch might reboot unexpectedly with a message similar to the following.

```
TLB Miss:  Virtual Addr=0x00000003 IP=0x804e5658 Task='eDrvPoll'
Task ID=0x85992560 fp:0x000000f0 sp:0x85991f18 ra:0x804e54cc sr:0x1000fc01
```

- **Crash Messaging (PR_0000054038)** — The binary crash log lists the wrong software version, if the switch rebooted into a different version than that from which it crashed.
- **DHCP Snooping (PR_0000067680)** — The DHCP snooping database is not uploaded to or downloaded from the external TFTP server if **no tftp server** is configured on the switch.
- **Enhancement (PR_0000060667)** — Adds DHCPv6 client authentication options. For more information, see the "DHCPv6 Client Authentication" section in the *IPv6 Configuration Guide*.
- **Enhancement (PR_0000060779)** — Allows the switch to act as an SSH client to connect to another HP switch. Also enhances SFTP to allow bidirectional secure copying of files between a switch and an SFTP server, initiated from the switch with the **copy** command. For more information, see "SSH Client" on page 32.
- **Enhancement (PR_0000061695)** — Adds encoded version information to the config file (e.g., Ver #01:00:01), to allow the switch to move between software versions that have different configuration options. The user should not modify this string.
- **Enhancement (PR_0000063932)** — For improved interoperability with Cisco ACS, the Calling-Station-Id RADIUS attribute and Remote Address TACACS+ fields are now sent in authentication requests for management telnet, ssh, and http service. This enhancement provides the authentication server with the remote IP Address of the connecting station, if available, to provide more granular access policies and auditing based on incoming source IP Address.
- **Enhancement (PR_0000064186)** — The **include-credentials** feature is enhanced to provide a **radius-tacacs-only** option to the command. For more information, see "Include RADIUS and TACACS Only Credentials" on page 32.
- **Enhancement (PR_0000065022)** — Provides a way to gracefully shut down OSPF routing on HP switches without losing packets that are in transit. For more information, see "OSPF Neighbor Shutdown Notification" on page 32.
- **Enhancement (PR_0000065164)** — Allows incoming CDP and LLDP packets tagged for VLAN 1 to be processed even if VLAN 1 does not contain any ports. For more information, see "Accept CDP/LLDP Packets Tagged for VLAN 1" on page 32.

- **Enhancement (PR_0000065218)** — Provides a way to define a fixed, user-assigned cost of an OSPF LSA type 3 summarized prefix. For more information, see "Define Cost of LSA Type 3 Summarized Prefix" on page 32.
- **Enhancement (PR_0000069103)** — Adds support for the J9546A HP 8-port 10GBase-T v2 zl Module.
- **Event Log (PR_0000064762)** — Event log message #609 displays **vid 0** instead of a valid VLAN ID.
- **Instrumentation Monitor (PR_0000065498)** — The system delay value might be incorrectly displayed as a negative number.
- **IPv6 (PR_0000063725)** — The hop count used for IPv6 DHCP relay does not adhere to RFC 3315 specifications.
- **LLDP-MED (PR_0000038954)** — After rebooting, a switch with more than 25 phones connected may not place all the phones in the correct VLAN.
- **MAC Authentication (PR_0000063756)** — The switch does not respond to or learn from incoming packets with the same source and destination MAC addresses, which causes MAC authentication to fail.
- **Module Crash (PR_0000064847)** — A switch module might reboot unexpectedly with a message similar to the following.

```
Software exception in ISR at buffers.c:3222
-> ASSERT0:  failed
```

- **PIM (PR_0000064763)** — PIM register packets are dropped by the switch if the checksum is calculated over the entire packet.
- **QoS (PR_0000064876)** — Software version K.15.01 allowed the invalid configuration of duplicate class entries in one QoS policy, which was not accepted by the switch when updating to software versions K.15.02 or K.15.03.
- **SSH (PR_0000060114)** — With a large terminal length setting, if the switch output is on the order of 100 lines or more, the switch will appear to hang until the user presses **<Enter>** on the console. Workarounds: Use the **no page** command, or use the default terminal length setting (24 lines).
- **SSH (PR_0000063910)** — After enabling SSH and removing TELNET service, the switch does not respond to SSH management via Opsware NCM.
- **Stacking (PR_0000062828)** — After an Operator password is configured on the stack commander, that switch stops responding to console commands.
- **TACACS (PR_0000064709)** — In some situations when TACACS is configured for telnet access, the user can connect with Operator privileges but cannot enable Manager mode.

## Version K.15.04.0003 Fixes

Status: Released and fully supported, and posted on the Web.
The following problem was resolved in software version K.15.04.0003.

- **Crash (PR_0000067432)** — Attempts to copy the ssh-client-known-hosts file to the switch might cause the switch to reboot unexpectedly with a message similar to the following.

```
Restr Mem Access
HW Addr=0x3139322a IP=0x113e2dbc Task='mftTask' Task ID=0x1de82b40
sp:0x13181310 lr:0x113e2dac
msr: 0x0000b032 xer: 0x00000000 cr: 0x40000400
```

# Version K.15.05.0001 Fixes

Status: Never released.
The following problems were resolved in software version K.15.05.0001.

- **BootROM (PR_0000069773)** — This software version includes a BootROM update to BootROM version K.15.13.
- **CLI (PR_0000068813)** — The commands **page** and **no page** are not available at the Operator privilege level.
- **CLI (PR_0000069319)** — The output of **show running-config change-history detail** gives incorrect user names, when TACACS or RADIUS is used for authentication.
- **CLI (PR_0000069667)** — The switch reports incorrect values of CPU utilization when the switch is idle.
- **CLI (PR_0000069677)** — The output of the command **show system power-consumption** might have some values truncated.
- **CLI (PR_0000071056)** — On a switch with only v2 zl modules (no other zl modules), the output of **show tech all** fails to include the output of many commands.
- **CPU Utilization (PR_0000065847)** — In certain rare situations the switch might report CPU utilization of 100% for sustained intervals.
- **DHCP (PR_0000064525)** — With meshing and DHCP Snooping enabled, some DHCP clients might not receive an IP address.
- **Enhancement (PR_0000051260)** — Adds Nonstop Routing for OSPF, VRRP, and RIP during a management module failover. See "Chassis Redundancy" in the *Management and Configuration Guide*.
- **Enhancement (PR_0000052548)** — Adds improved logging, commands, and command output for OSPFv2 troubleshooting. See "IP Routing" in the *Multicast and Routing Guide*.
- **Enhancement (PR_0000053047)** — Adds a global configuration option that allows each VLAN to have a multicast filter. See "Multimedia Traffic Control with IP Multicast (IGMP)" in the *Multicast and Routing Guide*.
- **Enhancement (PR_0000063613)** — Adds support for switch-to-switch Distributed Trunking. See "Port Trunking" in the *Management and Configuration Guide*.
- **Enhancement (PR_0000064722)** — Adds support for MAC-Based VLANs on the v2 zl modules. See **"**MAC-Based VLANs" in the *Access Security Guide*.
- **Enhancement (PR_0000066341)** — Adds the ability to view diagnostic monitoring information for transceivers with Diagnostic Optical Monitoring (DOM) support. See "Troubleshooting" in the *Management and Configuration Guide*.
- **Enhancement (PR_0000066432)** — Adds the ability to override the normal Reverse Path Forward (RPF) lookup mechanism so the router can accept multicast traffic on an interface other than that which would be normally selected. See "PIM-SM (Sparse Mode)" in the *Multicast and Routing Guide*.
- **Enhancement (PR_0000067349)** — Adds support for the J9286B 10m and J9287B 15m Direct Attach Cables (DACs).
- **Enhancement (PR_0000069000)** — Provides additional control over user access to the switch by creating local user accounts that are authorized to use a customized set of commands. See "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide*.
- **Enhancement (PR_0000069073)** — Adds the Spanning Tree loop guard feature, which prevents network loops when BPDUs are not received on a blocking port for various reasons ("BPDU starvation"). See "Multiple Spanning Tree Operation" in the *Advanced Traffic Management Guide*.

- **File Transfer (PR_0000063877)** — Using the CLI command **copy flash flash < primary | secondary >** from an SSH session might cause the SSH session to disconnect. However, the file transfer completes successfully.
- **IPv6 (PR_0000068744)** — The output of **show ipv6 routers** lists router preference as medium. This field was removed.
- **LLDP-MED (PR_0000062113)** — The switch uses the default QoS priority of 6 for the voice VLAN, no matter what priority is configured.
- **OSPF (PR_0000069646)** — The switch does not form an adjacency with an OSFPv3 neighbor if the neighbor is a Spirent router.
- **PIM-DM (PR_0000059788)** — In an OSPF ECMP environment where two routers forward the multicast flows, some hosts might receive only half the multicast channels. Workaround: increment the OSFP cost on one of the equal-cost links, to remove the equal-cost issue while retaining network redundancy.
- **PoE (PR_0000052701)** — If the switch boots up with a powered device (PD) connected, the switch wrongly reports `PD Denied power due to insufficient power allocation`.
- **Port Connectivity (PR_0000070355)** — When a v2 zl module port is forced to 100 Mbps full-duplex, the port toggles offline, online constantly.
- **Power (PR_0000066248)** — When the switch is exposed to AC power fluctuations that cause voltage drops, some modules might lose power and not recover.
- **RADIUS Accounting (PR_0000069459)** — When a client is authenticated on one VLAN and then moves and is authenticated on a different VLAN, RADIUS accounting still shows the client IP address from the first VLAN.
- **Rate Limiting (PR_0000070215)** — With rate limiting set at 100% (i.e. no limit), the switch drops a tiny fraction of line-rate traffic.
- **Routing (PR_0000066531)** — In rare situations with a large number of topology changes, the switch might reboot unexpectedly with a message similar to the following.

  ```
  Software exception at aspath.c:5058 -- in 'eRouteCtrl', task ID = 0xa96b4c0 -> Routing
  Stack: Assert Failed
  ```

- **SNMP (PR_0000064215)** — An SNMP query for the authorized VLAN ID or the unauthorized VLAN ID does not receive a correct value.
- **SNMP (PR_0000066564)** — An SNMP command to turn off logging of specific event log messages has no effect.
- **VRRP (PR_0000071139)** — With VRRP enabled, the backup router responds to proxy ARP requests. Also, the VRRP master responds to proxy ARP requests with its physical MAC address instead of the VRRP virtual MAC address.
- **Web Management (PR_0000061436)** — The switch does not show "live view" information in E-PCM.
- **Web Management (PR_0000064583)** — The Web user interface does not display "lightning bolt" icons on PoE ports.
- **Web Management (PR_0000067308)** — After disabling PoE on a port, the Web user interface displays `PoE: error` when the mouse hovers over that port.
- **Web Management (PR_0000069394)** — The Web user interface might truncate the list of which ports are in a VLAN.
- **Web Management (PR_0000069983)** — With IP virtual stacking enabled and accessing the stack via the Web user interface, the IP address displayed in the "status" field of the "Home" folder is incorrect. This is a display issue only.
- **Web Management (PR_0000070113)** — The Web user interface gives incorrect flow control status for a port.

## Version K.15.05.0002 Fixes

Status: Released and fully supported, but removed from the Web due to PR_0000072472.
No problems were resolved in software version K.15.05.0002.

## Version K.15.05.0003 Fixes

Status: Never released.
The following problems were resolved in software version K.15.05.0003.

- **CLI (PR_0000072036)** — When more than one VLAN is configured as **ipv6 ospf3 passive**, the outputs of **show running-config** and **show startup-config** do not display `ipv6 ospf3 passive` for all VLANs that are configured as such. The VLANs act properly, and the output of **show ipv6 ospf3 interface** confirms that the VLANs are configured as `passive`. However, if the config file is copied to an external storage device, it will not have that command on all appropriate VLANs and therefore is not a valid backup config file.
- **Distributed Trunking (PR_0000072028)** — After a switch configured for switch-to-switch Distributed Trunking is rebooted, the rebooted switch's MAC address table might be out of sync with the MAC address table on the Distributed Trunking peer switch.
- **PoE (PR_0000072106)** — The switch does not provide power to a Cisco VoIP 9951 keypad.

## Version K.15.05.0004 Fixes

Status: Never released.
The following problem was resolved in software version K.15.05.0004.

- **Crash (PR_0000072472)** — In some situations the switch might reboot unexpectedly with a message similar to the following.

```
Crash msg:  Invalid Instr
HW Addr=0x00000000 IP=0x0 Task='mSess2' Task ID=0xa91a700
sp:0x6446788 lr:0x12c4824
msr: 0x02029200 xer: 0x20000000 cr: 0x48000400
```

## Version K.15.05.0005 Fixes

Status: Never released.
The following problem was resolved in software version K.15.05.0005.

- **Enhancement (PR_0000068734)** — Adds the ability to encrypt passwords and authentication keys in the config file. After enabling this feature, the resulting config file cannot be used by older software versions. Before enabling this feature, please refer to "Getting Further Software Management Information" on page 10 . For more information about the feature, see the chapter "Configuring Username and Password Security" in the *Access Security Guide* for your switch.

## Version K.15.5.0006 Fixes

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.15.05.0006.

- **CLI (PR_0000073363)** — In some situations, using the CLI **kill** command causes the current telnet connection to become unresponsive.

- **SSL (PR_0000073315)** — In software versions K.15.05.0001 - K.15.05.0005, a switch configured for SSL might experience a decrease in available memory over time.

## Version K.15.05.0007 Fixes

Status: Never released.
The following problems were resolved in software version K.15.05.0007.

- **CLI (PR_0000072854)** — The switch allows invalid parameters when configuring SNMPv3, and the resulting config file cannot be loaded onto a switch.
- **Crash (PR_0000071233)** — In some situations, a switch running OSPFv3 might reboot unexpectedly with a message similar to the following.

```
Software exception at ospf3_rt.c:341 -- in 'eRouteCtrl', task ID =0xa9c5200
-> Routing Stack: Assert Failed
```

- **Crash (PR_0000072643)** — In some rare situations the switch might reboot unexpectedly with no information in the event log other than `System went down without saving crash information`.
- **Crash (PR_0000072806)** — In some rare situations with ACL **deny** logging configured, the switch might reboot unexpectedly with a message similar to the following.

```
Software exception in ISR at btmDmaApi.c:378
-> ASSERT:  No resources available!
```

- **GVRP (PR_0000072394)** — When GVRP is enabled in software versions K.15.05.0001 - K.15.05.0006, the config file includes duplicate entries for several parameters.
- **Redundant Management (PR_0000071409)** — With the **encrypt credentials** feature enabled, after rebooting an 8212zl switch with redundant management modules, the Standby Management Module (SMM) does not boot up.

## Version K.15.06.0006 Fixes

Status: Released and fully supported, and posted on the Web.
The following problems were resolved in software version K.15.06.0006.

- **802.1X (PR_0000073030)** — Dynamic ACL works only once if **accounting network** is enabled and Radius-ACL is unchanged.
- **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.
- **Authentication (PR_0000070913)** — Sometimes, after rebooting a client PC, the client might not be placed in the authenticated VLAN.
- **BootROM (PR_0000072561)** — This software version includes a BootROM update to BootROM version K.15.19.
- **CLI (PR_0000070114)** — The switch gives an error message when the user adds a port to an existing voice VLAN. Also, a VLAN already configured with a tagged port cannot later be configured as a voice VLAN.
- **CLI (PR_0000071092)** — Multiple voice VLANs no longer allowed. With this fix, multiple voice VLANs are allowed again.
- **Config (PR_0000071616)** — Losing TACACS server and SNTP configuration after firmware update from K.15.01.0033 to any K.15.xx.

- **CPU Utilization (PR_0000071986)** — PVST Protection on a disabled port causes high CPU utilization.
- **Crash (PR_0000071284) - 5400 (K.14.56, K.14.81)** — Initiation of multiple consecutive SSH sessions may trigger an unexpected reboot with a message similar to the following: `OS Exception Task ID 0xa907440, tSsh0, exited`.
- **Crash (PR_0000072451)** — The command **show mesh traceroute mac-address *<MAC>* vlan *<VID>*** causes crash.
- **Crash (PR_0000073737 & 78394)** — When using the **reload at** command the switch will crash or hang one minute prior to the scheduled reload time.
- **Enhancement (PR_0000060335)** — This enhancement implements full compliance with the IEEE standard for the SNMP MIB object **ieee8021MstpMib**. For more information, see the "Multiple Instance Spanning-Tree Operation" chapter in the *Advanced Traffic Management Guide* for your switch.
- **Enhancement (PR_0000068123)** — Enhanced the **router pim** command. For more information, see the **"**PIM-DM (Dense Mode)" and "PIM-SM (Sparse Mode)" chapters in the *Multicast and Routing Guide* for your switch.
- **Enhancement (PR_0000069334)** — Includes three LACP enhancements.
  **1) LACP Key.** The **lacp key** option provides the ability to control dynamic trunk configuration. Ports with the same key will be aggregated as a single trunk. For more information see the "Port Trunking" chapter in the *Management and Configuration Guide* for your switch.
  **2) LACP Debug Logging and Show Commands.** The **show lacp**, **show lacp peer**, and **show lacp counters** commands are modified or added. For more information see the "Port Trunking" chapter and the "Troubleshooting" appendix in the *Management and Configuration Guide* for your switch.
  **3) Displaying Information about LACP Trunk Load Balancing.** The **show trunks load-balance interface** command displays the port on which the information will be forwarded out for the specified traffic flow with the specified source and destination address. For more information see the "Port Trunking" chapter and the "Troubleshooting" appendix in the *Management and Configuration Guide* for your switch.
- **Enhancement (PR_0000070161)** — Uplink Failure Detection (UFD) is a network path redundancy feature that works in conjunction with NIC teaming functionality. For more information, see the "Port Status and Configuration" chapter in the *Management and Configuration Guide* for your switch.
- **Enhancement (PR_0000070797)** — Display Transceiver Information to transceiver cable diagnostics. For more information, see the "Troubleshooting" appendix in the *Management and Configuration Guide* for your switch.
- **Enhancement (PR_0000070869)** — The administrator is now able to configure 8 static Rendezvous Points (RPs) and 8 multicast group ranges per static RP in PIM-SM mode. For more information, see the "PIM-SM" chapter in the *Multicast and Routing Guide* for your switch.
- **Enhancement (PR_0000071572)** — Flight Data Recorder (FDR) logs information that is **"**interesting**"** at the time of the crash as well as when the switch is misbehaving, but not crashed. The crash-log and crash-data files now maintain data for the last 4 crashes instead of just the most recent. For more information about this feature, see the "File Transfers" and "Troubleshooting" appendices in the *Management and Configuration Guide* for your switch.
- **Enhancement (PR_0000071588)** — IGMP v3 and MLD v2 capabilities were added to the switch. For more information, see the "Multicast Listener Discovery (MLDv1 and MLDv2)" chapter in the *IPv6 Configuration Guide* for your switch.
- **Enhancement (PR_0000071946)** — OSPF Stub Router Advertisement for OSPF v3 - renamed to better reflect the feature. For more information, see the "Introduction to OSPFv3" chapter in the *IPv6 Configuration Guide* for your switch.
- **Enhancement (PR_0000071947)** — Define OSPF LSA Type 3 Summarized Prefix Cost for OSPF v3. For more information, see the "Introduction to OSPFv3" chapter in the *IPv6 Configuration Guide* for your switch.

- **Enhancement (PR_0000072658)** — Policy Based Routing (PBR) provides the ability to manipulate a packet's path based on attributes of the packet. Traffic with the same destination can be routed over different paths, so that different types of traffic, such as VOIP or traffic with special security requirements, can be better managed. For more information, see the "Classifier-Based Software Configuration" chapter in the *Advanced Traffic Management Guide* for your switch.
- **Enhancement (PR_0000072668)** — IPv6 over IPv4 tunneling is a way to establish point-to-point tunnels by encapsulating IPv6 packets within IPv4 headers so that they can be carried over the IPv4 routing infrastructure. IPv6 over IPv4 tunneling provides a mechanism for utilizing the existing IPv4 routing infrastructure to carry IPv6 traffic between IPv6 networks. For information on configuring tunnels, see the "IPv6 Tunneling Over IPv4 Using Manually Configured Tunnels" chapter in the *IPv6 Configuration Guide* for your switch.
- **Enhancement (PR_0000072702)** — Both VLANS and tunnels can be assigned to areas and may be collectively referred to as an IP routing interface. For information on configuring tunnels, see the "IPv6 Tunneling Over IPv4 Using Manually Configured Tunnels" chapter in the *IPv6 Configuration Guide* for your switch.
- **Enhancement (PR_0000073705)** — Border Gateway Protocol (BGP) support has been added. *Note: BGP authentication is not supported.* For more information, see the "BGP (Border Gateway Protocol)" chapter in the *Multicast and Routing Guide* for your switch.
- **Event Log (PR_0000065597)** — A port failure that is identified by LEDs might not be noted in the event log, or the event log might indicate that the wrong port failed self test.
- **IP Communication (PR_0000071115)** — ICMP request getting `Destination net unreachable` instead of `Host unreachable`.
- **Logging (PR_0000071821)** — Switch using K.15.05 does not report informational log entry for SCP file transfers.
- **Loop Protection (PR_0000072139)** — Loop-protect stops working on the ports connected to an unmanaged switch.
- **Management (PR_0000071316)** — PCM Live view not working with K.14.83 when switch is configured to use HTTPS and banner.
- **Module Crash (PR_0000067805)** — In some unusual situations the module might reboot unexpectedly with a message similar to one of the following: `Msg loss detected - no ack for seq # 6111`, or `Re-Synchronization of module - reboot of module required`.
- **Proxy-ARP (PR_0000071924)** — The arp cache is not updated with the source client entry with the initial arp when Proxy arp is in use.
- **SFTP (PR_0000070592)** — SCP and SFTP transfer using openssh fails.
- **SNMP (PR_0000071613)** — SNMP data in `entPhysicalName` shows incorrect output.
- **SNMP (PR_0000072270)** — MIB object `ifHighSpeed` does not return current bandwidth of trunk, just the max available bandwidth.
- **SNMP (PR_0000070551)** — MIB problem: An SNMP query for a GVRP port that is administratively disabled from GVRP (CLI command **unknown-vlans disable**) shows the integer value `3` but not the text value `disabled`.
- **TFTP (PR_0000072631)** — A tftp transfer of the config file fails if it has **ospf dead** and **hello interval** timers configured.
- **Transceiver Configuration (PR_0000072290)** - SFP/SFP+ -- Fiber -- Beginning with K.15.05.0002, an SFP with a forced duplex mode does not link on the SFP+ side.
- **VRRP (PR_0000072285)** — **VR up_time** incorrectly displays a negative uptime value.
- **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 K.15.06.0007 Fixes

Status: Released and fully supported, but not posted on the Web.
The following problems were resolved in software version K.15.06.0007.

- **ARP (CR_0000102875)** — ARP replies from the switch to an NLB (Network Load Balancing) server are wrongly sent to the NLB server's physical address instead of its virtual address. This issue began with software version K.15.04.0002.
- **Authentication (CR_0000103285)** — On a switch containing v2 zl modules configured for MAC or Web authentication with a PC and IP phone connected to the same switch port, if the PC authenticates before the IP phone and the PC needs to re-authenticate later, the re-authentication fails.
- **CLI (CR_0000077695)** — The switch does not allow the use of a dash or an underscore (**"-"** or **"_"**) in an unauth-redirect URL.
- **CLI (CR_0000078167)** — On a switch with only v2 zl modules (no other zl modules), if one of the modules is faulty, the output of **show tech all** fails to include the output of many commands. This improves the original fix (PR_0000071056) in K.15.05.0001.
- **Crash (CR_0000103146)** — A switch configured for Distributed Trunking might reboot unexpectedly with a message similar to the following.

  ```
  Software exception at svc_sem.c:3094 -- in 'mDTCtrl', task ID = 0xa9fefc0
  ```

- **Crash (CR_0000103293)** — After the event log displays a stream of messages stating `...unresponsive to sustained traffic...`, the switch might reboot unexpectedly with a message similar to the following.

  ```
  Software exception in ISR at btmDmaApi.c:378
  -> ASSERT:  No resources available!
  ```

- **Crash (CR_0000103369)** — A switch configured with the command **web-management ssl** might reboot unexpectedly with a message similar to the following.

  ```
  Software exception at http_init.c:543 -- in 'tHttpd', task ID = 0xa984d80
  ```

- **Distributed Trunking (CR_0000102556)** — A switch configured for switch-to-switch Distributed Trunking and stacking might experience high CPU utilization and Spanning Tree instability.
- **Distributed Trunking (CR_0000102777)** — If a Distributed Trunking switch is configured with **peer-keepalive timeout 3** (the minimum value), after the switch reboots the config file has the timeout = 0 (zero).
- **Distributed Trunking (CR_0000103240)** — With Distributed Trunking enabled, applying the command **clear mac-address** to the VLAN of the InterSwitch-Connect (ISC) on one switch can cause the peer switch to drop packets that should be forwarded across the ISC.
- **Distributed Trunking (CR_0000103575)** — If the Distributed Trunking (DT) secondary switch is rebooted shortly before the DT primary switch, broadcast traffic might be forwarded in a loop through the trunk.
- **Distributed Trunking (CR_0000103623)** — A network loop can cause the MAC tables on the Distributed Trunking switches to get out of sync, resulting in connectivity issues.
- **Event Log (CR_0000103805)** — Messages are added to the event log too quickly, which can cause system resource issues after 49.7 days of system uptime.
- **ICMP (CR_0000103755)** — The switch does not send ICMP `Destination host unreachable` messages.
- **Module Crash (CR_0000069838)** — In some situations a switch module might reboot unexpectedly with messages similar to the following.

```
chassis: Slot X Read Error - Restricted Memory
Exception number: 0xdead0100
HW Addr=0x00000035 IP=0x000c48a8 Task='
chassis: Slot X Download Complete
chassis: Slot X Downloading
chassis: (87) Ports X: Blade Crash detected -Available
```

- **Nonstop Switching (CR_0000103195)** — When the active and standby management modules are running different software versions (one boots from software in primary flash, the other boots from software in secondary flash), in some situations the switch incorrectly remains in Nonstop switching mode instead of changing to warm-standby redundancy mode.
- **SNMP (CR_0000103637)** — The switch writes an incorrect value into the cdpCacheDevicePort OID, which can cause incorrect topology mappings.
- **SNMP (CR_0000103769)** — This fix improves the Distributed Trunking MIB object structure in switch software.

## Version K.15.06.0008 Fixes

Status: Released and fully supported, and posted on the Web.
The following problem was resolved in software version K.15.06.0008.

- **Authentication (CR_0000104351)** — A client that fails authentication and is placed in the unauth-VID cannot communicate on the network.

## Version K.15.07.0002 Fixes

Status: Released and fully supported, and posted on the Web.
The following problems were resolved in software version K.15.07.0002.

- **ARP (PR_0000102875, CR_0000102875)** — ARP replies from the switch to an NLB (Network Load Balancing) server are wrongly sent to the NLB server's physical address instead of its virtual address. This issue began with software version K.15.04.0002.
- **Authentication (PR_0000103285, CR_0000103285)** — On a switch containing v2 zl modules configured for MAC or Web authentication with a PC and IP phone connected to the same switch port, if the PC authenticates before the IP phone and the PC needs to re-authenticate later, the re-authentication fails.
- **BootROM (PR_0000105412, CR_0000105412)** — This software version includes a BootROM update to BootROM version K.15.27.
- **CLI (PR_0000064558, CR_0000072036)** — The switch displays the originally-configured RADIUS timeout in the output of **show port-access mac-based config auth-server**, even if RADIUS assigns a different timeout.
- **CLI (PR_0000072449, CR_0000077339)** — Some options are not available for the CLI command **ip route**.
- **CLI (PR_0000073442, CR_0000078167)** — On a switch with only v2 zl modules (no other zl modules), if one of the modules is faulty, the output of **show tech all** fails to include the output of many commands. This improves the original fix (PR_0000071056) in K.15.05.0001.
- **CLI (PR_0000103529, CR_0000103529)** — On an 8206zl switch, the output of the **show modules details** command gives incorrect versions of GP1 and GP2 for the System Support Module. This does not impact switch operation.
- **CLI (PR_0000104222, CR_0000104222)** — Output of the CLI command **show interface transceiver detail** gives an incorrect value for Transfer Distance.

- **CLI (PR_0000104428, CR_0000104428)** — The output of **show tech all** does not include all information it should, unless a premium license is installed.
- **Crash (PR_0000072806, CR_0000077641)** — In some rare situations with ACL **deny** logging configured, the switch might reboot unexpectedly with a message similar to the following.

```
Software exception in ISR at btmDmaApi.c:378
-> ASSERT:  No resources available!
```

- **Crash (PR_0000103293, CR_0000103293)** — After the event log displays a stream of messages stating "`...unresponsive to sustained traffic...`", the switch might reboot unexpectedly with a message similar to the following.

```
Software exception in ISR at btmDmaApi.c:378
-> ASSERT:  No resources available!
```

- **Crash (PR_0000103369, CR_0000103369)** — A switch configured with the command **web-management ssl** might reboot unexpectedly with a message similar to the following.

```
Software exception at http_init.c:543 -- in 'tHttpd', task ID = 0xa984d80
```

- **Crash (PR_0000103863, CR_0000103863)** — After undergoing certain configuration changes, it is possible for the switch to reboot unexpectedly with a message similar to the following.

```
Invalid Instr
HW Addr=0x00000000 IP=0x0 Task='mSess2' Task ID=0xa91a700
sp:0x6446788 lr:0x12c4824
msr: 0x02029200 xer: 0x20000000 cr: 0x48000400
```

- **Distributed Trunking (PR_0000102556, CR_0000102556)** — A switch configured for switch-to-switch Distributed Trunking and stacking might experience high CPU utilization and Spanning Tree instability.
- **Distributed Trunking (PR_0000102776, CR_0000102776)** — When the Distributed Trunking (DT) primary switch is rebooted the DT secondary switch erroneously brings down DT links.
- **Distributed Trunking (PR_0000102777, CR_0000102777)** — If a Distributed Trunking switch is configured with **peer-keepalive timeout 3** (the minimum value), after the switch reboots the config file has the timeout = 0 (zero).
- **Distributed Trunking (PR_0000103240, CR_0000103240)** — With Distributed Trunking enabled, applying the command **clear mac-address** to the VLAN of the InterSwitch-Connect (ISC) on one switch can cause the peer switch to drop packets that should be forwarded across the ISC.
- **Distributed Trunking (PR_0000103575, CR_0000103575)** — If the Distributed Trunking (DT) secondary switch is rebooted shortly before the DT primary switch, broadcast traffic might be forwarded in a loop through the trunk.
- **Distributed Trunking (PR_0000103623, CR_0000103623)** — A network loop can cause the MAC tables on the Distributed Trunking switches to get out of sync, resulting in connectivity issues.
- **Enhancement (PR_0000065586, CR_0000072508)** — Displays the aggregate count of routes per routing protocol. See the *Multicast and Routing Guide*, "IP Routing" chapter.
- **Enhancement (PR_0000065723, CR_0000072572)** — Adds support for BGP route maps. See "BGP (Border Gateway Protocol)" in the *Multicast and Routing Guide*.
- **Enhancement (PR_0000066341, CR_0000072917)** — Adds the ability to view diagnostic monitoring information for transceivers with Diagnostic Optical Monitoring (DOM) support. See "Troubleshooting" in the *Management and Configuration Guide*.
- **Enhancement (PR_0000067641, CR_0000073680)** — Adds NSSA range metrics to OSPFv2. See the *Multicast and Routing Guide*, "IP Routing" chapter.

- **Enhancement (PR_0000069196, CR_0000074531)** — This feature provides the ability to track and report information about switch management processes on a per-user, per-session basis. Syslog or RADIUS will be used for logging the information.
- **Enhancement (PR_0000069433, CR_0000074736)** — Adds support for sFlow using IPv6. See the *Management and Configuration Guide*, "Network Management" chapter.
- **Enhancement (PR_0000072298, CR_0000077209)** — The RA Guard feature restricts the ports (or trunks) that can accept IPv6 Router Advertisements (RAs). Additionally, ICMPv6 router redirects are blocked on the configured ports.
- **Enhancement (PR_0000072987, CR_0000077793)** — SPF scheduling (throttling) allows the switch to delay SPF calculations when the network is unstable or there is a change in topology. See the *IPv6 Configuration Guide*, "OSPFv3 Routing" chapter, or the *Multicast and Routing Guide*, "IP Routing" chapter.
- **Enhancement (PR_0000073083, CR_0000077874)** — This feature adds **sflow** as an option to the existing **ip source-interface** command, which provides the ability to specify the sFlow source agent address that is included in the packets sent from the switch to the sFlow collection nodes.
- **Enhancement (PR_0000073085, CR_0000077875)** — The MAC Address Count feature provides a way to notify the switch management system when the number of MAC addresses learned on a switch port exceeds the permitted configurable number.
- **Enhancement (PR_0000073284, CR_0000078031)** — Allows the configuration of the Domain Name Server (DNS) with DHCP. See the *Management and Configuration Guide*, "Troubleshooting" chapter.
- **Enhancement (PR_0000073738, CR_0000078395)** — Adds support for BGP MD5 authentication. See "BGP (Border Gateway Protocol)" in the *Multicast and Routing Guide*.
- **Enhancement (PR_0000093199, CR_0000093199)** — Adds the ability to configure a mesh ID. See the A*dvanced Traffic Configuration Guide*, "Switch Meshing" chapter.
- **Enhancement (PR_0000102845, CR_0000102845)** — Adds support for filtering BGP routes by adding the option **bgp** to **show ip route**, and for displaying the BGP peer's graceful restart time with **show ip route bgp neighbor**. See "BGP (Border Gateway Protocol)" in the *Multicast and Routing Guide*.
- **IGMP (PR_0000071591, CR_0000076574)** — Forced Fast-Leave IGMP does not work correctly for ports with MACs learned on multiple VLANs, unless each of those VLANs is configured for Forced Fast-Leave
- **IGMP (PR_0000103101, CR_0000103101)** — The switch forwards **"**joins**"** to all queriers instead of only to the querier for the VLAN on which the join was received. This can result in intermittent flow failures.
- **Module Crash (PR_0000059251, CR_0000069838)** — In some situations a switch module might reboot unexpectedly with messages similar to the following.

```
chassis: Slot X Read Error - Restricted Memory
Exception number: 0xdead0100
HW Addr=0x00000035 IP=0x000c48a8 Task='
chassis: Slot X Download Complete
chassis: Slot X Downloading
chassis: (87) Ports X: Blade Crash detected -Available
```

- **Nonstop Switching (PR_0000103195, CR_0000103195)** — When the active and standby management modules are running different software versions (one boots from software in primary flash, the other boots from software in secondary flash), in some situations the switch incorrectly remains in Nonstop switching mode instead of changing to warm-standby redundancy mode.
- **OSPF (PR_0000073445, CR_0000078168)** — When a VLAN is configured with the command **ip ospf cost**, the switch resets the OSPF interface, which causes adjacencies to go down.

- **RADIUS (PR_0000044139, CR_0000064558)** — The switch does not display the reauth timeout period received from a RADIUS server.
- **SNMP (PR_0000072099, CR_0000077036)** — The MIB object hpSwitchStpStatAdminStatus.0 gives the wrong value (2, disabled) even when STP is enabled.
- **SNMP (PR_0000072459, CR_0000077346)** — RMON event traps are sent even with **trap-level none** in the configuration.
- **SNMP (PR_0000103637, CR_0000103637)** — The switch writes an incorrect value into the cdpCacheDevicePort OID, which can cause incorrect topology mappings.
- **Syslog (PR_0000065540, CR_0000072482)** — There is a long delay before the switch event log messages are sent to the syslog server.
- **VRRP (PR_0000073641, CR_0000078318)** — VRRP does not function properly when these conditions exist: a) The priority of the Master is > 242, and b) **no preempt-mode** is configured, and c) There is a failover so the original backup becomes Master, and d) The track port is disabled on the new Master. With those conditions the original Master should take over but does not.

## Version K.15.08.0007 Fixes

Status: Released and fully supported, and posted on the web.
The following problems were resolved in software version K.15.08.0007.

- **ACLs (CR_0000106068)** — The switch does not allow the user to configure an ACL on static trunks, responding with the error message `Unable to apply the policy`.
- **ACLs (CR_0000106467)** — An Access Control Entry (ACE) that includes a remark cannot be fully deleted from an ACL; the switch responds with the error `Commit failed`, although the ACE no longer appears in the config file. However, an attempt to add that ACE back into the ACL has no effect. There is no error message, but the ACE does not appear in the config file.
- **Authentication (CR_0000105275)** — When a switch port is configured for two different types of authentication, if either authentication type is configured with a specific **logoff-period** that is different than the MAC address aging time, the authenticated clients might reauthenticate at random times.
- **BootROM (CR_0000109701)** — This software version includes a BootROM update to BootROM version K.15.28.
- **CLI (PR_0000071005)** — A DSCP class name entered by the user is displayed as the binary value in **show** command outputs. For example, the CLI entry **qos dscp cs6** is displayed as `qos dscp 110000`. This is a display issue only, the command functions properly.
- **Config (CR_0000104888)** — The **IPv6 nd ra prefix** command requires configuration of valid lifetime and preferred lifetime values before the user can add the parameters **off-link** and **no-autoconfig**. If the configured lifetime settings are the default values (valid = **2592000** and preferred = **604800**), the **off-link** and **no-autoconfig** parameters are not listed in the config file. When the switch is rebooted, the parameters function properly even though they are not listed in the config file. However, if the config file is saved to a TFTP server, then loaded onto a switch, the configuration will not operate as expected because the parameters are missing.
- **Crash (CR_0000103863)** — After undergoing certain configuration changes, it is possible for the switch to reboot unexpectedly with a message similar to the following.

```
Invalid Instr
HW Addr=0x00000000 IP=0x0 Task='mSess2' Task ID=0xa91a700
sp:0x6446788 lr:0x12c4824
msr: 0x02029200 xer: 0x20000000 cr: 0x48000400
```

- **Crash (CR_0000106131)** — When CPU utilization is very high (> 90%) and PIM routing is enabled with a large number of flows (on the order of several thousand), executing a command such as **show ip mroute** might cause the switch to reboot unexpectedly with a message similar to the following.

  ```
  NMI event SW:IP=0x010d0e60 MSR:0x02029200 LR:0x00d03984
  cr: 0x48000800 sp:0x04ff6fe0 xer:0x00000000
  Task='mPimsmCtrl' Task ID=0xa955000
  ```

- **Crash (CR_0000106847)** — With Distributed Trunking enabled, when IGMP is disabled on a VLAN, the switch's buffer pool decreases. Ultimately this can cause the switch to reboot unexpectedly with a message similar to the following.

  ```
  Software exception in ISR at btmDmaApi.c:378
  -> ASSERT: No resources available!
  ```

- **Crash (CR_0000107764)** — With VRRP enabled, a switch might crash again during bootup after a crash.

- **Crash (CR_0000108146)** — Related to **IGMP CR_0000107962** (also fixed in K.15.08.0007), after a large amount of querier elections the switch might reboot unexpectedly with a message similar to the following.

  ```
  NMI event SW:IP=0x001ce064 MSR:0x02029200 LR:0x001ce064
  cr: 0x28000400 sp:0x0478b5f0 xer:0x00000000
  Task='mIgmpCtrl' Task ID=0xa94a000
  ```

- **DHCP Snooping (CR_0000108666)** — When a PXE protocol DHCP-offer packet is sent from a boot server through a trusted port, the switch drops the packet.

- **Distributed Trunking (CR_0000106804)** — With Distributed Trunking enabled and a large number of MAC addresses learned by the switch (on the order of several thousand addresses), the switch experiences a gradual loss of free memory.

- **Distributed Trunking (CR_0000108567)** — In a switch-to-switch Distributed Trunking setup, one switch has a distributed trunk link to two other switches, and there is an InterSwitch-Connect (ISC) between those two other switches. If the distributed trunk link to one of those other switches is disabled, traffic from that other switch is not automatically forwarded across the ISC.

- **Enhancement (PR_0000071901)** — When executing the **show config** or **show running-config** commands, interfaces that have configuration settings are displayed together in order, only once, containing all the configuration commands for that interface. For more information, see the chapter “Switch Memory and Configuration” in the *Basic Operation Guide* for your switch.

- **Enhancement (CR_0000106070)** — This is the first of several phases that allows a Comware CLI proficient user to use their Comware CLI knowledge to generate equivalent ProVision software CLI commands to manage and configure ProVision software switches. This preliminary offering adds 21 simple Comware Display commands directly to the ProVision CLI, with additional troubleshooting and management commands planned for future software versions. See the *Comware CLI Commands in ProVision Software* manual for more details.

- **Enhancement (CR_0000106090)** — The structured option is an additional parameter for the **show running-config** and **show config** commands. Using the structured option, the command output is grouped together in a more logical manner. For more information, see the chapter “Switch Memory and Configuration” in the *Basic Operation Guide* for your switch.

- **GVRP (CR_0000103865)** — In some situations in an MSTP environment, a switch might become unresponsive to management traffic over the network after GVRP is enabled.

- **IGMP (CR_0000107962)** — If an IGMP query is received on the same switch that sent the query, the switch begins a querier election when it should not.

- **Meshing (CR_0000103714)** — ARP replies are not always forwarded through the mesh, resulting in loss of communication to affected end nodes.

- **Meshing (CR_0000106937)** — With meshing enabled and IGMP not enabled, the switch sends incorrect IGMP information to mesh partners, which might result in a daily error message similar to:

  ```
  ldbal: Inconsistent IGMP config with 0016b9-010101
  ```

- **MLDv2 (CR_0000107373)** — Enabling MLDv2 causes a gradual loss of packet buffers, eventually resulting in loss of management access to the switch.

- **Module Crash (CR_0000105186)** — On a switch configured with more than 1024 VLANs, it is possible for a v2 zl module to reboot unexpectedly with a message similar to the following.

  ```
  Slot A subsystem went down:
  Software exception in ISR at interrupts_ahs.c:4473
  ```

- **Module Crash (CR_0000105418)** — Related to **Module Crash CR_0000105186** (also fixed in K.15.08.0007): If a v2 zl module reboots unexpectedly due to CR_0000105186, a different v2 zl module with clients connected might reboot unexpectedly with a message similar to the following.

  ```
  ID: fa7b8969
  Slot A subsystem went down: 01/01/90 00:00:15 K.15.06.0006 62
  ASIC Parity 1516 0x0000040a = 0x00000000:00000000
  ```

- **OSPF (PR_0000073307)** — OSPF MD5 authentication does not work properly, which can lead to OSPF instability.

- **Passwords (CR_0000103309)** — If the switch is configured with a manager and/or operator password, a username must be configured in addition to the password. This is a new requirement beginning with K.15.05 software; when connecting to the switch a user will be prompted for the username. In the situation where usernames are not configured, upon software update this fix automatically adds usernames **operator** for operator-level access and **manager** for manager-level access.

- **Passwords (CR_0000107422)** — A password that is configured and saved with the "setup" screen is removed from the switch if the user invokes the CLI **setup** command again.

- **PIM (CR_0000108226)** — Multicast streams consisting of only fragmented frames are not routed by PIM.

- **Port Security (CR_0000105205)** — With a large number of ports configured for port security (on the order of 100 ports), after rebooting the switch, some clients such as IP phones might not be reachable on the network.

- **SNMP (CR_0000104175)** — The MIB object **ifDescr** is blank for an SFP slot that does not have a transceiver inserted.

- **SNMP (CR_0000106289)** — The **atTable** (address translation table) OID does not properly display the switch's network-to-physical address (ARP cache) information.

- **Spanning Tree (CR_0000106250)** — Spanning Tree BPDUs are not properly forwarded across a trunk that uses SFP+ interfaces, if the trunk ports are disabled when the switch is booted. This results in Spanning Tree instability such as multiple root switches, BPDU starvation, and Spanning Tree link flapping.

- **SSL (CR_0000108869)** — The switch accepts SSL sessions with export ciphers that use fewer than 128 bits.

- **Static Routes (CR_0000104240)** — If a switch is running K.15.06 software and configured with static routes, after downgrading to older software, the static routes are wrongly removed from the configuration.

- **Switch Hang (CR_0000109565, CR_0000109696)** — The switch might fail to boot fully, requiring a power-cycle to recover.

- **TELNET (PR_0000071780)** — The switch allows more telnet sessions than it should. When the maximum number of telnet sessions is exceeded, the sessions cannot be removed with the **kill** command and the switch must be rebooted to allow new telnet sessions.

- **Transceivers (CR_0000106077)** — When querying a transceiver, the first time the command **show interface transceiver <port> detail** is executed, the output shows false alarms and errors. **Workaround:** Execute the command a second time to get valid results.
- **Web Management (PR_0000072858)** — The Web interface does not allow a user to have manager privileges, even if the user provides correct manager credentials.
- **Web Management (CR_0000103673)** — The switch does not allow configuration of a "friendly port name" via the Web interface, responding with a `configuration failed` error. **Workaround:** This failure only affects the first port the user tries to name. After receiving the failure message, the user can select a different port and name it. Then the user can select the original port and successfully name it.

## Version K.15.08.0008 Fixes

Status: Released and fully supported, and posted on the web.
The following problem was resolved in software version K.15.08.0008.

- **Switch Hang (CR_0000106245)** - The switch might fail to boot fully, requiring a power-cycle to recover.

## Version K.15.09.0003 Fixes

Status: Released and fully supported, but not posted on the web.
The following problems were resolved in software version K.15.09.0003.

- **CLI (PR_0000071398, CR_0000076389)** - Previous software versions allowed configuration of VLAN IP addresses in overlapping subnets, which can cause mis-routing of packets and IP communication failure. With this fix, attempting to configure overlapping subnets gives the error message `The IP address (or subnet) <IP_address/mask> already exists.`
- **CLI (CR_0000112797)** - A DSCP class name entered by the user is displayed as the binary value in **show** outputs. For example, the CLI entry **qos dscp cs6** is displayed as `qos dscp 110000`. This is a display issue only, the command functions properly. This fix improves the CLI fix in K.15.08.0007 (PR_0000071005).
- **CLI (CR_0000113359)** - Existing trap receiver entries might be overwritten by later entries. This has been observed when the first trap receiver is configured with two community names, and then a second trap receiver is configured with the same two community names.
- **Crash (CR_0000108864)** - It is possible for communication between the External Power Supply (EPS) and the switch to fail. When that happens the switch gives the event log message `chassis: Ext Power Supply 1 measured out of spec or is faulty. Please change or contact support`. If the EPS is power-cycled at that time, the switch might reboot unexpectedly with a message similar to the following. Note that the communication issue was already resolved.

```
NMI event SW:IP=0x0077ddcc MSR:0x02029200 LR:0x0077dd84
cr: 0x48000400 sp:0x0441e560 xer:0x00000000
Task='mPoeMstCtl' Task ID=0xaa1b000
```

- **Crash (CR_0000115705)** - When using SFTP to copy a core dump from the standby management module, if the standby does not exist or does not have a core dump file the switch will reboot unexpectedly with a message similar to the following.

```
Software exception at fileTransferSFTP.c:498 -- in 'mftTask', task I  = 0xa97c600
-> Cannot open source file
```

- **DHCP (CR_0000113976)** - DHCP addresses are not properly assigned when Web Authentication or MAC Authentication clients fail authentication and are redirected at a high rate.

- **Enhancement (PR_0000068493, CR_0000074060)** - Meshing and routing now can be configured simultaneously. A packet can be routed into a mesh, or be switched through a mesh and then routed. Two routers can be connected by mesh links, which offers additional network topologies between routers and switches. Concurrent meshing and routing makes it possible to implement meshing throughout a broadcast domain without the need for additional switches or the use of another Layer 2 technology such as Spanning Tree to connect meshing domains with routing switches.
- **Enhancement (PR_0000070948, CR_0000075993)** - RPVST+ is a proprietary spanning tree implementation that extends RSTP (802.1w) to run a separate spanning tree for each VLAN on the switch, and ensures that only one active, loop-free path exists between any two nodes on a given VLAN.
- **Enhancement (CR_0000074537)** - For console/serial link and inbound telnet sessions, the switch output:
  - Uses whatever width is set by the terminal program. If width is not specified, 80 characters is the default.
  - Automatically wraps on word boundaries (such as spaces) for non-columnar output.
  - Automatically wraps on column boundaries for columnar output.
  - HP recommends that you do not set your terminal width **(terminal width <y>)** above 150 columns.
- **Enhancement (CR_0000105360)** - This enhancement is a follow-on to PR_0000060335, which implements full compliance with the IEEE standard for the SNMP MIB object ieee8021MstpMib. This CR_0000105360 adds Single Instance STP information to the MIB.
- **Enhancement (CR_0000106140)** - The Flight Data Recorder provides a way to capture and preserve data that is related to a crash event. Phase 2 adds the capture and preservation of protocol and subsystem-specific information.
- **Enhancement (CR_0000107011)** - When a Cisco VoIP phone boots up (or sometimes periodically), it queries the switch and advertises information about itself using CDPv2. The switch receives the `VoIP VLAN Query TLV (type 0x0f)` from the phone and then immediately sends the voice VLAN ID in a reply packet to the phone using the `VLAN Reply TLV (type 0x0e)`. The phone then begins tagging all packets with the advertised voice VLAN ID.
- **Enhancement (CR_0000114497)** - This is the second of several phases that allows a Comware CLI proficient user to use their Comware CLI knowledge to effectively manage and configure ProVision software switches. This phase adds 112 additional Comware display commands to the ProVision software CLI.
- **IPv6 (CR_0000103036)** - The switch does not always send ICMPv6 `destination unreachable` messages when it should.
- **IPv6 (CR_0000112244)** - When IPv6 traffic is forwarded through a 6in4 tunnel, the encapsulated packet does not include the DSCP value in the IPv4 header or the traffic class field in the IPv6 header, and QoS prioritization does not work properly.
- **MAC-Based VLANs (CR_0000114940)** - With mixed mode configured, after one client is authenticated on a port, other clients on the same port that are placed in the guest VLAN cannot communicate on the network.
- **PIM-DM (CR_0000107542)** - Sometimes new multicast streams are not added to the multicast routing table, and are not forwarded to clients.
- **PoE (CR_0000110353)** - When input power to the switch drops from 220 to 110 Volts, the switch recognizes this and adjusts available PoE power from 900 to 300 Watts. But when input power returns to 220 Volts, the switch does not adjust available PoE power back to 900 Watts. This issue affects both v1 and v2 zl PoE+ modules on 5400zl and 8200zl switches.
- **Port Communication (CR_0000114548)** - When port 14 of a v2 zl module is configured for tagged packets only, untagged packets including STP BPDUs are not received by that port. Workaround: configure an untagged VLAN on port 14.
- **Routing (PR_0000073028, CR_0000077827)** - When NIC teaming is used on a server and each NIC is connected to a different switch, it is possible that routed traffic to or from the server is not forwarded.

- **SNMP (CR_0000108820)** - When a switch has multiple VLANs with ARP cache entries on each VLAN, an SNMP get-next of the ipNetToPhysicalPhysAddress OID fails to report the values on the last VLAN index, giving the error `No such variable`.
- **Switch Hang (CR_0000114815)** - If any of the parameters in the command **snmpv3 targetaddress** includes a space, when the config is saved and the switch is rebooted the switch will hang and fail to boot fully.
- **Transceivers (CR_0000113788)** - When a transceiver is inserted into an SFP slot of a powered-up switch, the switch might wrongly change the enabled/disabled configurations of higher-numbered SFP slots.
- **VRRP (CR_0000113863)** - After a reboot, the VRRP Master configured with a preempt delay timer sends a gratuitous ARP from the switch's physical MAC address instead of the VRRP virtual MAC address. This causes routing to fail until the preempt delay timer expires.

## Version K.15.09.0004 Fixes

Status: Released and fully supported, and posted on the web.
The following problems were resolved in software version K.15.09.0004.

- **CLI (CR_0000115515)** - The switch does not allow configuration changes via the CLI, responding with the error message `inconsistent value`. This has been observed when the configuration includes **snmpv3 targetaddress TARGETADDRESS** with a **TARGETADDRESS** string longer than 24 characters, and the switch is updated to K.15 software.
- **Config (CR_0000117518)** - A switch configured with a username and password and with **include-credentials** cannot be accessed after updating software, because the username is wrongly removed from the config file during the software update.
- **Crash (CR_0000115929)** - With very large key sizes, the command **show crypto host-cert** might cause the switch to reboot unexpectedly with a message similar to the following.

```
Invalid Instr
HW Addr=0x00000000 IP=0x0 Task='mSess2' Task ID=0xa97ad40
sp:0x4acecc8 lr:0x57e468
msr: 0x02029200 xer: 0x20000000 cr: 0x28000400
```

- **Crash (CR_0000116647)** - It is possible for the switch to reboot unexpectedly with a message similar to the following.

```
Software exception in kernel context at ghsException.c:1101
-> Internal system error
```

- **Module Crash (CR_0000113992)** - In a rare situation, a switch module or port bank might reboot unexpectedly with a message similar to the following.

```
chassis: Slot H Read Error Restr Mem Access HW Addr=0xffaaaaf0
IP=0x1a10d64 Task='mIpAdMUpCt' Task ID=0x1b1e2300
Bus Error Data=0x00000000 Status=0x00000400
```

- **Module Crash (CR_0000116226)** - In a rare situation, a switch module or port bank might reboot unexpectedly with a message similar to the following. This improves the original Module Crash fix (CR_0000113992), also in K.15.09.0004.

```
chassis: Slot H Read Error Restr Mem Access HW Addr=0xe5911000
IP=0x1a10da8 Task='mIpAdMUpCt' Task ID=0x1b1e4c80
Bus Error Data=0x00000000 Status=0x00000400
```

- **Power (CR_0000112424)** - When the switch is exposed to AC power fluctuations and the voltage drops too low, the switch reboots and generates an incorrect error message saying the switch crashed. With this fix, the error message is changed to `Switch rebooting due to temporary loss of power or low voltage`.

- **SSL (CR_0000115933)** - Under certain conditions, the VLAN -> VLAN Mgmt page on the switch cannot be accessed via an SSL connection to the web user interface.
- **Web Management (CR_0000108339)** - The switch's web user interface cannot be accessed via the fully-qualified domain name in some situations. Workaround: Use the IP address to access the switch's web user interface.

## Version K.15.10.0003 Fixes

Status: Released and fully supported, and posted on the web.
The following problems were resolved in software version K.15.10.0003.

- **CLI (CR_0000113359)** - Existing trap receiver entries might be overwritten by later entries. This has been observed when the first trap receiver is configured with two community names, and then a second trap receiver is configured with the same two community names.
- **Crash (PR_0000071797, PR_0000076756)** - The switch might reboot unexpectedly when the following configuration options are applied.
  - The switch is configured to send events to a trap receiver, including `SNMP security access violation` events.
  - The switch receives a very high rate of SNMP queries.
  - The incoming queries use an incorrect SNMP community name.

  The switch will log a crash message similar to one the following.

```
TLB Miss: Virtual Addr=0x00000000 IP=0x805e1d14 Task='mSess1'
Task ID=0x81f14800 fp:0x00000000 sp:0x81f14598 ra:0x8015df58 sr:0x1000fc01

TLB Miss: Virtual Addr=0x00000000 IP=0x8061cd4c Task='tDevPollTx'
Task ID=0x81afa920 fp:0x00000060 sp:0x81afa7d0 ra:0x805e1c60 sr:0x1000fc01

TLB Miss: Virtual Addr=0x00000000 IP=0x800c3cf4 Task='mSnmpCtrl'
Task ID=0x81e4fa10 fp:0x00000000 sp:0x81e4f670 ra:0x800b741c sr:0x1000fc01
```

- **Crash (CR_0000103293)** - After the event log displays a stream of messages stating `...unresponsive to sustained traffic...`, the switch might reboot unexpectedly with a message similar to the following.

```
Software exception in ISR at btmDmaApi.c:378
-> ASSERT:  No resources available!
```

- **Crash (CR_0000116647)** - It is possible for the switch to reboot unexpectedly with a message similar to the following.

```
Software exception in kernel context at ghsException.c:1101
-> Internal system error
```

- **Crash (CR_0000116912)** - With OSPF routing and MSTP enabled, it is possible for the switch to reboot unexpectedly with a message similar to the following.

```
Software exception at rt_table.c:4453 -- in 'eRouteCtrl', task ID = 0xa95e140
-> Routing Stack: Assert Failed
```

- **Crash (CR_0000118474)** - The switch experiences a gradual loss of free memory when clients that use a RADIUS-assigned ACL reauthenticate. This can cause the switch to reboot unexpectedly.
- **Display Issue (CR_0000118422)** - A MAC address that begins with a non-zero value is displayed incorrectly in CLI and Web interface output.

- **Distributed Trunking (CR_0000103240)** - With Distributed Trunking enabled, applying the command **clear mac-address** to the VLAN of the InterSwitch-Connect (ISC) on one switch can cause the peer switch to drop packets that should be forwarded across the ISC.
- **Distributed Trunking (CR_0000115557)** - Multicast hosts might be temporarily dropped from the multicast stream, in a topology with Distributed Trunking where a Group-Specific Host Membership Query should be forwarded across the Inter-Switch Connection (ISC).
- **Distributed Trunking (CR_0000118526)** - In a switch-to-switch Distributed Trunking topology with IGMP enabled, multicast streams learned on one Distributed Trunking switch might not be known to the other Distributed Trunking switch. The result is multicast streams that cannot be joined by clients on one switch.
- **Distributed Trunking (CR_0000118663)** - The standby management module (SMM) periodically reports `Out of pkt buffers`, on a switch with redundant management configured for Nonstop Switching and Distributed Trunking. This can lead to an unexpected reboot of the SMM.
- **Enhancement (PR_0000073100, CR_0000077888)** - This feature provides SNMP read access to the CPU utilization of the modules. Currently the only method to retrieve the module CPU utilization is the CLI command **show cpu slot <slot | all>**. A new MIB table is created to facilitate the reading of information related to the module and its CPU utilization statistics.
- **Enhancement (CR_0000103497)** - When using Commands authorization, the Web Agent windows may show or hide fields, or allow or deny configuration steps, based on the access or deny list (VSA filtering) for the authenticated user. For more information, see the chapter "RADIUS Authentication, Authorization, and Accounting" in the *Access Security Guide* for your switch.
- **Enhancement (CR_0000107183)** - IPv6 Router Advertisements allow IPv6 routers to advertise a list of recursive DNS Server (RDNSS) addresses and a DNS Search List (DNSSL) to IPv6 hosts. The new command options are **ipv6 nd suppress-ra-dns**, which is executed in the global config context, and **ipv6 nd ra suppress-dns**, which is executed in the VLAN context. For more information, see the chapter "IPv6 Router Advertisements" in the *IPv6 Configuration Guide* for your switch.
- **Enhancement (CR_0000108063)** - Prevents MAC addresses from being learned on the specified ports when the VLAN is untagged and the destination MAC address is 01000c-CCCCCC (CDP), 0180c2-00000e (LLDP), or 0180c2-000003 (EAPOL). The feature is configured per-port by using the **ignore-untagged-mac <port-list>** command. For more information, see the chapter "Configuring for Network Management" in the *Management and Configuration Guide* for your switch.
- **Enhancement (CR_0000109154)** - OpenFlow is a programmable open-standard network protocol that uses flexible matching rules to classify and manage network traffic into flows. For more information, see the *OpenFlow Configuration Guide*.
- **Enhancement (CR_0000115963)** - This is the third of four phases that allows a Comware CLI proficient user to use their Comware CLI knowledge to effectively manage and configure ProVision software switches. This phase adds 97 additional Comware display commands to the ProVision software CLI. With this addition there are now 230 Comware display commands in the ProVision software CLI.
- **File Transfer (CR_0000106249)** - A configuration file that has loop protection enabled on a trunk cannot be downloaded to the switch, if the trunk does not exist in the currently-running configuration.
- **IPv6 (CR_0000112244)** - When IPv6 traffic is forwarded through a 6in4 tunnel, the encapsulated packet does not include the DSCP value in the IPv4 header or the traffic class field in the IPv6 header, and QoS prioritization does not work properly.
- **Module Crash (CR_0000110845)** - With MSTP enabled on the switch, a port configured for MAC authentication and loop protection does not detect a loop on a downstream switch. This can lead to CPU utilization of 90-100%, and the switch module or port bank might reboot unexpectedly with a message similar to the following.

```
Software exception in ISR at ngDmaRx.c:1660
```

- **Module Crash (CR_0000116784)** - If a MAC address moves between three Distributed Trunks repeatedly, the switch modules where the MAC address is seen experience a gradual loss of free memory that can lead to a module crash.
- **MSTP (CR_0000117421)** - A trunk has the default MSTP port priority = 4. If the trunk is configured with a port priority = 8 (which is the default for non-trunk gigabit ports), after saving the configuration and rebooting the switch, that port priority is wrongly changed to 4.
- **OSPF (CR_0000117192)** - When an OSPF neighbor is in the INIT state and the router receives a one way hello from that neighbor, the event log generates a message that the switch received an invalid one way hello. OSPF routing functions properly but this message should not be generated. This fix removes that erroneous message.
- **Port Security (CR_0000114545)** - With port security enabled, the first packet received on the port is not forwarded by the switch. This can cause DHCP failures for clients that send only one DHCP Discover packet.
- **Routing (CR_0000112796)** - In an unusual situation, the switch might erroneously forward local traffic to a router for a short period of time.
- **sFlow (CR_0000110640)** - When sFlow sends a sample that was routed, the switch does not have information to display the port on which the packet was received. With this fix, the sFlow sample will show zero as the received interface index instead of 0x3fffffff.
- **SNMP (CR_0000118604)** - The entPhysicalVendorType OID for the J9309A (HP 4-port 10GbE SFP+ zl Module) is incorrect.
- **Switch Hang (CR_0000114815)** - If any of the parameters in the command **snmpv3 targetaddress** includes a space, when the config is saved and the switch is rebooted the switch will hang and fail to boot fully.
- **Web Management (CR_0000108339)** - The switch's web user interface cannot be accessed via the fully-qualified domain name in some situations. Workaround: Use the IP address to access the switch's web user interface.
- **Web Management (CR_0000111720)** - The PCM Live View of a switch does not refresh automatically, and clicking on a port in the Live View window causes a browser script error.

## Version K.15.10.0004 Fixes

Status: Never released.
No problems were resolved in software version K.15.10.0004.

## Version K.15.10.0005 Fixes

Status: Released and fully supported, but not posted on the web.
The following problems were resolved in software version K.15.10.0005.

- **ACLs (CR_0000119956)** - Removing an ACL entry (ACE) that is a comment (a "remark") causes undesired changes to the ACL.
- **BGP (CR_0000122109)** - When configuring a BGP neighbor, the switch does not accept IP addresses that would be broadcast or network addresses in a classful addressing scheme. For example, the switch does not allow the neighbor addresses 15.255.255.255 or 15.0.0.0.
- **Display Issue (CR_0000121028)** - Some MAC addresses are displayed incorrectly in the output of CLI commands **show lldp info remote-device** and **display lldp neighbor-information list**.
- **Link (CR_0000120753)** - Remote link partner does not lose link when the local gigabit ethernet port on a v2 zl module is disabled.

- **Routing (CR_0000120907)** - A switch that has a default gateway or less-specific route configured does not allow users to connect to the switch's IP loopback address. The packets are routed instead of being accepted by the switch.
- **TFTP (CR_0000119184)** - The switch experiences a loss of free memory each time command output is copied to a TFTP server. When memory is no longer available, the TFTP will fail with a message similar to the following.

```
TFTP download in progress.
Failed to allocate a new TFTP client.
00000K Request failed.
```

## Version K.15.10.0006 Fixes

Status: Released and fully supported, but not posted on the web.
The following problems were resolved in software version K.15.10.0006.

- **802.1X (CR_0000122837)** - Clients have issues with authentication when 802.1X and MAC Authentication are both configured on a port.
- **Distributed Trunking (CR_0000120627)** - Some traffic is lost when a member of a Distributed Trunk pair is rebooted.
- **IPv6 (CR_0000122825)** - IPv6 packets with a mask of /65 to /127 are routed to the default route instead of the intended destination.
- **Module Crash (CR_0000115913)** - Modules in slots A-F (top 6 slots) crash and Modules G-L sometimes crash and reboot instead of going down; when the number of power supplies is decreased from 2 to 1 on an 8212 switch.
- **PIM-DM (CR_0000122264)** - Some PIM-DM multicast streams fail when a default route is configured on the switch.
- **Spanning Tree (CR_0000110052)** - In a topology with multiple MSTP regions and multiple same-cost links connecting the regions, the CST root port might change to a CST alternate port, and MSTP instances might be blocked on region boundary ports.
- **SSH (CR_0000122795)** - SSH session disconnects when the SSH key re-exchange takes place.

## Version K.15.10.0007 Fixes

Status: Never released.
The following problems were resolved in software version K.15.10.0007.

- **Authentication (CR_0000122439)** - With multiple certificates installed on the switch, PEAP-MSCHAPv2 authentication fails when using Windows Server 2008 R2 Network Policy Server (NPS).
- **BootROM (CR_0000124997)** - This software version includes a BootROM update to BootROM version K.15.30.
- **Crash (CR_0000122225)** - The switch might reboot unexpectedly when using VRRP with a message similar to `Software exception in ISR at btmDmaApi.c:378`.
- **Crash (CR_0000124336)** - When a redundancy switchover or a failover occurs on an 8200zl switch and the Active Management Module runs a K.15.08 or earlier software version and the Standby Management Module runs a K.15.09 or later software version, the Standby Management Module will reboot unexpectedly as it is transitioning to Active status with the error message:
`Software exception at chassisInfo.c:423 -- in 'swInitTask', task ID = 0xaa0d6c0 -> Switch does not have a mac address`.
- **Crash (CR_0000124443)** - Rarely, when ports go offline, then back online while voice VLAN requests are being sent, the switch might reboot unexpectedly with a message similar to:
`Software exception at sw_sem.c:1036 -- in 'mSnmpCtrl' -> Deadlock found!`.

- **IGMP (CR_0000105902)** - IGMPv2 LEAVE processing functionality no longer works for a multicast group after receipt of IGMPv1 group specific membership query (GSMQ) packet when operating in IGMPv2 mode, even when **ip igmp forcedfastleave 1-24** is enabled.
- **Power (CR_0000117394)** - With J9306A power supplies that have serial numbers beginning with "TH" in power slots 1 and 2, the bottom 6 interface slots fail to power up, resulting in `tombstone` errors on interface slots G through L.
- **SNMP (CR_0000124375)** - A switch configured to send syslog messages to a server also sends incorrect SNMP traps, causing `unknown trap` messages in the syslog server.
- **Stacking (CR_0000124971)** - After rebooting the switch, stack members show an error code of `rejected`, and do not join the commander.
- **TFTP (CR_0000124276)** - After multiple TFTP file transfers from the switch, additional file transfers might fail with the error message `Translator failed` or `RFS Error Reboot`.

## Version K.15.10.0008 Fixes

Status: Released and fully supported, but not posted on the web.
The following problems were resolved in software version K.15.10.0008.

- **Authentication (CR_0000114307)** - The switch does not allow users to login when the configured authentication method is **peap-mschapv2**.
- **Crash (CR_0000126636)** - It is possible for the switch to reboot unexpectedly, under conditions of very high traffic volumes and high CPU utilization.
- **Power (CR_0000126058)** - With J9306A power supplies that have serial numbers beginning with "TH" in power slots 1 and 2, the bottom 6 interface slots fail to power up, resulting in `tombstone` errors on interface slots G through L. This improves the original Power fix (CR_0000117394), in K.15.10.0007 software.

## Version K.15.10.0009 Fixes

Status: Released and fully supported, and posted on the web.
The following problems were resolved in software version K.15.10.0009.

- **ACLs (CR_0000122535)** - When configuring an ipv4 or ipv6 prefix-list, it is not possible to add an entry to permit/deny **any**.
- **CLI (CR_0000125980)** - After configuring **debug ip pbr**, the output of **show debug** does not include pbr in the list of enabled debug types.
- **CLI (CR_0000127335)** - Using the CLI command **show tech all** can cause the system to reboot unexpectedly.
- **Crash (CR_0000120116)** - With OSPF configured, 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.`
- **Crash (CR_0000126799)** - Under unusual stress conditions, the switch might reboot unexpectedly with a message similar to
  `Software exception at fileTransfer.c:1144 -- in 'tHttpd', task ID = 0xa9389c0 -> Could not open file.`

- **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 will not function properly when subsequently loaded on a switch.
- **Distributed Trunking (CR_0000124473)** - The switch does not allow DHCP server responses to cross the Inter-Switch Connection (ISC).
- **Distributed Trunking (CR_0000125623)** - After rebooting a switch participating in a distributed LACP trunk, a distributed trunk port that is disconnected will not link after it is connected.
- **Distributed Trunking (CR_0000127096)** - When the Inter-Switch Connection (ISC) is brought down, clients connected via Distributed Trunk links cannot be reached from one of the Distributed Trunking switches.
- **Include Credentials (CR_0000127700)** - With include credentials enabled, a config file that is saved to a TFTP server does not contain the SNMPv3 credentials.
- **LEDs (CR_0000115489)** - After a PoE error is resolved, the switch turns off the PoE LED but continues to flash the Fault LED.
- **OSPF (CR_0000122980)** - OSPF3 ECMP routes are not displayed in the IPv6 route table.
- **Policy Based Routing (CR_0000125847)** - After configuring a policy and applying it to a VLAN, the IP next-hop is unreachable until the switch is rebooted.
- **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.
- **Routing (CR_0000128007)** - ARP replies from a Microsoft Network Load Balancing (NLB) cluster operating in multicast mode cause the switch to use software routing. This affects v2 zl modules and 3800 switches.
- **sFlow (CR_0000128567)** - The switch uses the IP address of the source VLAN as the sFlow packet source, instead of the configured **source-interface**.
- **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.
- **SNMP (CR_0000125513)** - The value stored in MIB object ospfNbrState (OID 1.3.6.1.2.1.14.10.1.6) is incorrect.
- **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.
- **Transceivers (CR_0000126801)** - After booting a 3800 switch or a K-software switch with a v2 zl module, a J9054B/C 100-FX SFP-LC transceiver that was already inserted (or is inserted during the boot process) will not link with the remote end.
- **Web Management (CR_0000125239)** - After logging into the switch Web user interface, closing the tab on some Web browsers does not log the user out of the Web session.

## Version K.15.10.0010 Fixes

Status: Released, but no longer recommended due to CR_0000127868.
The following problems were resolved in software version K.15.10.0010.

- **Fastboot (CR_0000127452)** - With fastboot enabled, TCP traffic experiences poor performance through ports 4, 5, and 6 of the J9538A 8-port 10GbE SFP+ v2 zl Module.

- **IGMP (CR_0000127628)** - In a topology where the host connects to a querier, the querier connects to a non-querier switch, the non-querier switch connects to a router, and the multicast source is beyond the router, the host might not receive the multicast stream. This happens because a "join" from the host that is received by the querier is not forwarded by the non-querier switch.
- **IGMP (CR_0000127974)** - If a switch receives a PIM packet while it is in the querier election state, the switch gives up the querier role and does not forward multicast traffic.
- **Transceivers (CR_0000129775)** - The switch does not turn off the laser when a port is administratively disabled, which might result in the link partner still seeing link. This has been observed with X2-SC SR Optics (J8436A) that have MYxxxxxxxx serial numbers.

## Version K.15.10.0011 Fixes

Status: Released and fully supported, but not posted on the web.
The following problem was resolved in software version K.15.10.0011.

- **Uplink Failure Detection (CR_0000127868)** - On a switch that is configured for uplink failure detection where the link to monitor (LtM) or link to disable (LtD) is an LACP trunk, after reboot the link to monitor is listed as down in the output of **show uplink-failure-detection**, and the link to disable is taken down by the switch.

## Version K.15.10.0012 Fixes

Status: Released, but no longer recommended due to CR_0000133023 and CR_0000134243.
The following problems were resolved in software version K.15.10.0012.

- **Config (CR_0000127108)** - After downgrading from a newer software version to a 15.10 software version, the output of **show run** lists an incorrect software build version in the `Created on release` statement.
- **Config (CR_0000129797)** - A config file that has the entry **ipv6 ospf3 passive** on a tunnel cannot be downloaded to the switch.
- **GVRP (CR_0000129917)** - When the switch receives its own GVRP frames, it learns from them instead of dropping the frames.
- **GVRP (CR_0000130090)** - After rebooting the switch, the configuration **unknown-vlans disable** does not work on trunks.
- **Link (CR_0000128466)** - After booting a switch with a port configured for 100-full, if that port is changed to 10-half it will not link with a remote device that runs at 10-half.
- **QoS (CR_0000123663)** - VRRP IPv4 DSCP is tagged as 0 and cannot be changed by remarking.
- **SFTP (CR_0000130830)** - The switch does not allow users to copy files such as core dumps to a server via SFTP, responding with the message `System Error`.

## Version K.15.10.0013 Fixes

Status: Never released.
The following problems were resolved in software version K.15.10.0013.

- **Crash (CR_0000126777)** - With a combination of interface state changes along with IPV6 address configuration changes, it is possible for the switch to reboot unexpectedly with a message similar to `SubSystem 0 went down: 01/24/13 13:31:29, Invalid Instr HW Addr=0x000004a8 IP=0x4a8, Task='mIpCtrl' Task ID=0xa9ca140 sp:0x470aab0 lr:0x723f4c, msr: 0x02029200 xer: 0x20000000 cr: 0x48000400.`

- **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.
- **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.
- **PIM (CR_0000128681)** - After a large number of multicast streams are added and old streams time out, the switch might get into a state where it is unable to add new multicast streams, responding with a message similar to `IpAddrMgr: Failed to allocate new SW IP multicast group, table full FIB entry`.

## Version K.15.10.0014 Fixes

Status: Never released.
The following problems were resolved in software version K.15.10.0014.

- **Banner MOTD (CR_0000132198)** - The login banner is not displayed if the user logs into the switch via the standby or member switch instead of the active or commander switch.
- **CLI (CR_0000128124)** - The output of **show monitor** and **show monitor <mirror_destination_number>** displays information for only mirror destination #1.
- **Crash (CR_0000127791)** - With OSPF configured, 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).
- **Distributed Trunking (CR_0000132286)** - When a MAC address moves from a Distributed Trunk port to a non-Distributed-Trunk port, the switch MAC tables sometimes show that MAC address on the wrong port.
- **Distributed Trunking (CR_0000132900)** - With a switch configured for both Distributed Trunking and MSTP, a MAC address learned on a VLAN that is not part of the Inter-Switch Connection (ISC) might not appear in the MAC table, or might appear on the wrong port. This issue has been observed when all the Distributed Trunk ports are down on the switch that learns the MAC address.
- **Distributed Trunking (CR_0000133318)** - Distributed trunk links might go down after a redundancy failover of an 8200zl switch running in Nonstop Switching mode.
- **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.
- **LEDs (CR_0000133898)** - PoE faults cause the DIM Status LED to blink instead of the PoE Status LED.
- **Management (CR_0000134091)** - Disabling write access to an SNMP community via the Web user interface might cause the switch to become unresponsive to command input. The switch must be rebooted to regain management access.
- **MSTP (CR_0000129044)** - In a high-availability environment, ports might be incorrectly blocked by STP.
- **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 on which password is changed.
- **Passwords (CR_0000134675)** - The switch does not automatically create a default username of "manager" or "operator" when a password is configured for those levels of access.

- **PIM (CR_0000130353)** - The switch might send duplicate multicast packets when sFlow is enabled and the multicast packets are routed by software.
- **Self Test (CR_0000134243)** - The J9547A 24-port 10/100 PoE+ v2 zl Module fails power-on self test (POST), with a message similar to `ID: ae2c6f0d, Slot F subsystem went down: 01/01/90 00:01:30 K.15.11.0008 532, HSL0 Fatal ff8000c2: Task=mChassAgnt Task ID=0x1b1f3640 IP=0x1c77308`.
- **SNMP (CR_0000123582)** - Including the **detail** parameter in the command **show ipv6 ospf3 link-state area-scope detail** might cause infinite output. This affects the **show tech all** command, which includes the **detail** parameter.
- **SSL (CR_0000133153)** - If the SSL option is enabled, and an external EWA server is configured, the switch incorrectly uses an https (secure) redirect page when accessing a plain text URL.
- **TFTP (CR_0000129475)** - A switch config that has certain lines in the config file cannot be downloaded to the switch via TFTP. For example, attempting to download a config file with the valid statement **distributed-trunking peer-keepalive udp-port 6400** results in the error message `UDP port 6400 is already in use`.
- **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`.
- **Transceivers (CR_0000133023)** - 100-Megabit transceivers might have one or more of these symptoms: 1) Link LED is lit but link is down, 2) No Link after the transceiver is hot-swapped, 3) Transceiver fails self test.

## Version K.15.10.0015 Fixes

Status: Released and fully supported, but not posted on the web.
The following problems were resolved in software version K.15.10.0015.

- **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.
- **Distributed Trunking (CR_0000135388)** - When a MAC address moves from a Distributed Trunk port to a non-Distributed-Trunk port, the switch MAC tables sometimes show that MAC address on the wrong port. This fix improves the original Distributed Trunking fix (CR_0000132286).

## Version K.15.10.0016 Fixes

Status: Released and fully supported, and posted on the web.
The following problems were resolved in software version K.15.10.0016.

- **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.
- **IGMP (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.
- **IGMP (CR_0000136013)** - After the switch becomes querier, it does not update the table that defines the querier port, and continues to forward IGMP packets out the port that previously led to the querier.
- **Web Management (CR_0000135883)** - The "Rx Errors" column is missing from the Web user interface.

Technology for better business outcomes

To learn more, visit www.hp.com/networking/



July 2013

Manual Part Number
5998-3751