



Release Notes:

Version K.15.06.0008 Software

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

- This software is supported on the following switches

HP Switch 3500-24 (J9470A)
HP Switch 3500-24-PoE (J9471A)
HP Switch 3500-48 (J9472A)
HP Switch 3500-48-PoE (J9473A)
HP Switch 3500yl-24G-PWR Intelligent Edge (J8692A)
HP Switch 3500yl-48G-PWR Intelligent Edge (J8693A)
HP 3500yl-24G-PoE+ Switch (J9310A)
HP 3500yl-48G-PoE+ Switch (J9311A)
HP Switch 5406zl Intelligent Edge (J8697A)
E5406 zl Switch with Premium SW (J9642A)
HP Switch 5412zl Intelligent Edge (J8698A)
E5412 zl Switch with Premium SW (J9643A)
HP Switch 5406zl-48G Intelligent Edge (J8699A)
HP Switch 5412zl-96G Intelligent Edge (J8700A)
HP 5406zl-48G-PoE+ Switch (J9447A)
HP 5412zl-96G-PoE+ Switch (J9448A)
HP Switch 6200yl-24G-mGBIC (J8992A)
HP Switch 6600-24G (J9263A)
HP Switch 6600-24G-4XG (J9264A)
HP Switch 6600-24XG (J9265A)
HP Switch 6600-48G (J9451A)
HP Switch 6600-48G-4XG (J9452A)
HP Switch 8206zl (J9475A)
E8206 v2 zl Switch with Premium SW (J9640A)
HP Switch 8212zl (J8715A, J8715B)
E8212 v2 zl Switch with Premium SW (J9641A)

These release notes include information on the following:

- Getting further software management information ([page 2](#))
- Required BootROM updates ([page 6](#))
- Support Notes ([page 7](#))
- Clarifications for selected software features ([page 10](#))
- Known Issues ([page 16](#))
- A listing of software enhancements ([page 18](#))
- A listing of software fixes ([page 96](#))

© Copyright 2010-2011 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

Manual Part Number

5998-1186
November 2011

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

Premium License for Selected Switch Features	1
General Procedure	1
Getting Further Software Management Information	2
HP Switch, Routing Switch, and Router Products Software Keys	3
Operating System and Web Browser Compatibility Table	4
Minimum Software Versions	5
ROM Updates Required!	6

Support Notes

What's New	7
Summary of New Features	7
Additional Features	8

Clarifications

HP Security Policy and Release Notes	10
Version K.15.01.0031 Clarifications	10
Delays During Configuration Changes to Physical Ports	10
Nonstop Switching (5400zl and 8200zl Switches)	10
Password Length and Special Character Issues	11
IPv4 Loopback Address Not Required for IPv6 Address Configuration	12
Version K.15.02.0004 Clarifications	12
Rate-Limiting on the Entire Packet	12
Change to Default Setting for Detecting and Powering Pre-802.3af Devices	13
Compatibility Mode for v2 zl and zl Modules	13
Authorized IP Managers Precedence	14
Minimum Guaranteed Bandwidth Issue	14
Version K.15.03.0005 Clarifications	15
Loss of Event Log on Upgrade/Downgrade	15
RADIUS Server Authentication Issue	15

Known Issues

Version K.15.01.0031	16
Version K.15.02.0004	16
Version K.15.03.0005	17
Version K.15.05.0001	17

Enhancements

Version K.15.01.0031 Enhancements	18
Flapping Transceiver Mitigation	18
Module Reload (5400zl and 8200zl switches)	20

Version K.15.01.0032 Enhancements	22
Username and Password Size Increase	22
Version K.15.02.0004 Enhancements	23
Multicast ARP Support	23
Display Configuration of Selected Interface	24
Post-logon Banner Enhancement	30
Support for the Tilde (~) Character in TACACS+ and RADIUS Keys	32
Web Auth Deny Message	36
Port Security Per-Port MAC Increase	39
PoE with LLDP	39
Increase MAC Auth Client Limit to 256	42
Categorize CLI Return Messages	43
Energy Efficient Ethernet (EEE)	46
Version K.15.03.0003 Enhancements	50
Custom Default Configuration	50
SNMP Trap Upon Port Addition or Deletion of MAC Addresses	56
Log Message When Startup Config Updated	58
Show MAC with VLAN	60
Outbound Queue Monitor	61
Show OSPF Neighbor Timers	61
IP Enable/Disable for All VLANs	62
Logging for Routing ACLs	64
Trunk Load Balancing Using L4 Ports	68
Wake-on-LAN Support Across VLANs	69
Syslog via TCP	73
SNMP Trap on Running Configuration Changes	74
Static Summary Route to RIP	77
Dynamic Port Access Auth via RADIUS	78
Version K.15.04.0002 Enhancements	81
DHCPv6 Client Authentication Options Added	81
SSH Client	81
Encoded Version Information Added to Config File	86
Fields Added to Authentication Requests	86
Include RADIUS and TACACS Only Credentials	86
OSPF Neighbor Shutdown Notification	90
Accept CDP/LLDP Packets Tagged for VLAN 1	91
Define Cost of LSA Type 3 Summarized Prefix	91
Additional Support for zl Modules	92
Version K.15.05.0001 Enhancements	92
OSPF, VRRP, and RIP Nonstop Routing	92
OSPFv2 Logging commands and command output	92
VLAN Multicast Filter Global Configuration	93
Distributed Trunking Switch-to-Switch	93
MAC-Based VLANs	93
View Transceiver Diagnostic Optical Monitoring (DOM) Information	93

Override Reverse Path Forward (RPF) Lookup	93
10m and 15m Direct Attach Cables (DACs)	93
Customized Commands for Local User Accounts	93
Spanning Tree Loop Guard	93
Version K.15.05.0005 Enhancement	93
Encrypt Credentials	93
Version K.15.06.0006 Enhancements	94
OSPF Stub Router Advertisement for OSPF v3	94
OSPF LSA Type 3 Summarized Prefix Cost	94
Transceiver Diagnostics	94
MSTP Standards Compliant Based MIB	94
MLDv2	94
6in4 Tunneling	94
OSPFv3 over 6in4 Tunnels	94
Policy Based Routing (PBR)	94
BGPv4	94
LACP Key	95
LACP Debug Logging and Show Commands	95
Displaying Information about LACP Trunk Load Balancing	95
Uplink Failure Detection	95
PIM CLI enhancements	95
Support for Additional RPs and Multicast Groups	95
Flight Data Recorder Log	95

Software Fixes

Version K.15.01.0031	96
Version K.15.01.0032	104
Version K.15.01.0033	104
Version K.15.02.0004	105
Version K.15.02.0005	109
Version K.15.03.0003	109
Version K.15.03.0004	112
Version K.15.03.0005	112
Version K.15.03.0006	112
Version K.15.03.0007	112
Version K.15.04.0002	113
Version K.15.04.0003	115
Version K.15.05.0001	115
Version K.15.05.0002	117
Version K.15.05.0003	117
Version K.15.05.0004	117
Version K.15.05.0005	118

Version K.15.05.0006 118

Version K.15.05.0007 118

Version K.15.06.0006 119

Version K.15.06.0007 121

Version K.15.06.0008 122

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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> • 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 it 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 Networking 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, and 5372xl)
F	Switch 2500 Series (2512 and 2524), Switch 2312, and Switch 2324
G	Switch 4100gl Series (4104gl, 4108gl, and 4148gl)
H	Switch 2600 Series, Switch 2600-PWR Series: H.07.81 and earlier, or H.08.55 and greater, Switch 2600-8-PWR requires H.08.80 or greater. 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	Switch 3500yl Series (3500yl-24G-PWR and 3500yl-48G-PWR), Switch 6200yl-24G, 5400zl Series (5406zl, 5406zl-48G, 5412zl, 5412zl-96G), Switch 8212zl and Switch 6600 Series (6600-24G, 6600-24G-4XG, 6600-24XG).
KA	Switch E3800 Series (E3800-24G-PoE+-2SFP+, E3800-48G-PoE+-4SFP+, E3800-24G-2SFP+, E3800-48G-4SFP+, E3800-24SFP-2SFP+, E3800-24G-2X, E3800-48G-4XG, E3800-24G-PoE+-2XG, E3800-48G-PoE+-4XG)
L	Switch 4200vl Series (4204vl, 4208vl, 4202vl-72, and 4202vl-48G)
M	Switch 3400cl Series (3400-24G and 3400-48G): M.08.51 through M.08.97, or M.10.01 and greater; Series 6400cl (6400cl-6XG CX4, and 6410cl-6XG X2): M.08.51 through 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 1800 Series (Switch 1800-8G – PA.xx; Switch 1800-24G – PB.xx)
PK	Switch V1810-48G
Q	Switch 2510 Series (2510-24)
R	Switch 2610 Series (2610-24, 2610-24/12PWR, 2610-24-PWR, 2610-48 and 2610-48-PWR)
RA	Switch E2620 Series (E2620-24, E2620-24-PPoE+, E2620-24-PoE+, E2620-48, E2620-48-PoE+)
S	Switch 2520 Series (2520-8-PoE, 2520-24-PoE)
T	Switch 2900 Series (2900-24G and 2900-48G)
U	Switch 2510-48
VA/VB	Switch 1700 Series (Switch 1700-8 - VA and 1700-24 - VB)
W	Switch 2910al Series (2910al-24G, 2910al-24G-PoE+, 2910al-48G, and 2910al-48G-PoE+)
WA	ProCurve Access Point 530
WM	ProCurve Access Point 10ag
WS	ProCurve Wireless Edge Services xl Module and the ProCurve Redundant Wireless Services xl Module
WT	ProCurve Wireless Edge Services zl Module and the ProCurve Redundant Wireless Services zl Module
Y	Switch 2510G Series (2510G-24 and 2510G-48)
Z	ProCurve 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	Tested Web Browsers
Windows XP SP3	Internet Explorer 7, 8 Firefox 3.0, 3.5
Windows Vista SP2	Internet Explorer 7, 8 Firefox 3.0, 3.5
Windows Server 2003 SP2	Internet Explorer 7, 8 Firefox 3.0, 3.5
Windows Server 2008 SP2	Internet Explorer 7, 8 Firefox 3.0, 3.5
Windows 7	Internet Explorer 8 Firefox 3.0, 3.5
MAC OS	Firefox 3.0, 3.5

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 textbox, type J4858 (for 100-Mb and Gigabit information), or J8436 (for 10-Gigabit information). – Select any of the products that display in the dropdown list. – 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.15.06.0008 (BootROM K.15.19)

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. <ul style="list-style-type: none"> Allows layer 2 switching to continue during Management Module switchover. Transition from the Active Management Module to the Standby Management Module is quick and seamless, and does not require a reboot. Both Management Modules support identical features and configuration files
IPv6 Layer 3 support	<ul style="list-style-type: none"> K.13 provided IPv6 foundation services: <ul style="list-style-type: none"> IPv6 Host Dual stack (IPv4/IPv6) MLD snooping K.14 provided additional security and control: <ul style="list-style-type: none"> IPv6 ACL IPv6 QoS K.15 provides Layer 3 support services: <ul style="list-style-type: none"> OSPFv3 Static routing DHCPv6 Relay 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	<ul style="list-style-type: none"> VRRP enhancements, including: <ul style="list-style-type: none"> Simplified troubleshooting of VRRP configurations Physical IP is no longer identical with Virtual IP Route Maps enhancements for route management QoS and Mirroring Policies enhancements, allowing them to be applied dynamically show mesh, show class and show policy command enhancements
New software version designation	VVV.UU.BB.FFFFaaaaa software code designations, where: <ul style="list-style-type: none"> VVV is a switch platform identifier (for example, 'K'). UU is a major version number (for example, "15"), to specify significant changes in features or functions. 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'. 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. 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 subne t 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:

Clarifications

Version K.15.02.0004 Clarifications

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. 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. 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. If a v2 zl module is inserted, then it operates in the same mode as the zl module, but with performance increases. In Compatibility Mode, no v2zl features are allowed whether the modules are all v2 zl or not.	The Management Module is the only module that powers up. If Compatibility Mode is disabled, and then enabled, the startup config is erased and the chassis will reboot.

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

Figure 1. Example of Enabling Compatibility Mode

```
Switch(config)# no allow-vl-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.

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.*xxx* or earlier), see the Release Notes provided with those versions.

Version K.15.01.0031

- **OSPF (PR_0000054952)** — HP Switch does not accept Type 7 default route in a NSSA when announced by Cisco.
- **VRRP (PR_0000055742)** — VRRP Fast Failover fails for HA when advertisement interval is less than 1.
- **File Transfer (PR_0000048178)** — 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)** — 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)** — IPv4 loopback address which followed an IPv6 EUI-64 address in configuration would cause a crash.
- **OSPF (PR_0000046029)** — OSPF Virtual Links cause route flapping.
- **802.1X (PR_0000055580)** — Multiple auth users with different auth-vids placed on same vid
- **DAC (PR_0000050635)** — DAC port flaps after reboot.
- **SFLOW (PR_0000041583)** — Not sending vlan tag in sFlow data.

Version K.15.02.0004

- **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)** - UDLD can take up to 5 seconds to bring a port online, which may cause issues with VRRP.

Version K.15.03.0005

- **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

- **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.

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

- **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.
- **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”](#) below.

Flapping Transceiver Mitigation

In traditional HP switches, the state of a link is driven directly by the reported state of the port, which is required for rapid detection of link faults. However, the consequence of this is that a marginal transceiver, optical, or wire cabling, one which “flaps” up and down several times per second, can cause STP and other protocols to react poorly, resulting in a network outage. This enhancement expands the functionality of the existing Fault Finder function to include a “link-flap” event and a new action of "warn-and-disable". Together, these additions allow the errant condition to be detected, and the port in question can be optionally disabled.

Syntax: fault-finder <link-flap> sensitivity <low | medium | high> action <warn | warn-and-disable>

Default settings: Sensitivity = Medium; Action = Warn

Sensitivity thresholds are static. In a 10-second window, if more than the threshold number of link state transitions (up or down) is detected, the event is triggered. The 10-second window is statically determined, i.e. the counters are reset every 10 seconds, as opposed to being a sliding window. The counters are polled twice per second (every 500 milliseconds), and the event is triggered if the sensitivity threshold is crossed at that time.

The sensitivity thresholds are:

High = 3 transitions in 10 seconds
Medium = 6 transitions in 10 seconds
Low = 10 transitions in 10 seconds

Configuration of the link-flap event and corresponding action applies to all ports and port types (it is a global setting per FFI event type). Note that normal link transition protocols may prevent link state changes from occurring fast enough to trigger the event for some port types, configurations, and sensitivity settings.

When the link-flap threshold is met for a port configured for **warn** (for example, **fault-finder link-flap sensitivity medium action warn**), the following message will be seen in the switch event log.

```
02672 FFI: port <number>-Excessive link state transitions
```

When the link-flap threshold is met for a port configured for **warn-and-disable** (for example, **fault-finder linkflap sensitivity medium action warn-and-disable**), the following messages will be seen in the switch event log.

```
02672 FFI: port <number>-Excessive link state transitions
```

```
02673 FFI: port <number>-Port disabled by Fault-finder.
```

```
02674 FFI: port <number>-Administrator action required to re-enable.
```

The warn-and-disable action is available for all fault-finder events on an individual basis. It may be used, for example, to disable a port when excessive broadcasts are received. Because the fault-generated disabling of a port requires operator intervention to re-enable the port, such configuration should be used with care. For example, link-flap initiated disablement is not desired on ports that are at the client edge of the network, because link state changes there are frequent and expected.

Automatic disabling of a port when excessive broadcasts are detected is not recommended at the core or distribution layers, due to the potential to disable large parts of the network that may be uninvolved, and for the opportunity to create a denial-of-service attack.

Within the Web Management interface, double clicking an event on a port that was configured with warn-and-disable and has met the threshold to trigger the disable action, will bring up a dialog box with the event details. The event dialog box now contains a button at the bottom of the page, which can be used to re-enable the disabled port. The button will remain, even if the port has already been brought up through a prior exercise of it, or if the port was re-enabled via some other interface (e.g. the command line). Re-enabling an already enabled port has no effect. The button to acknowledge the event remains unchanged.

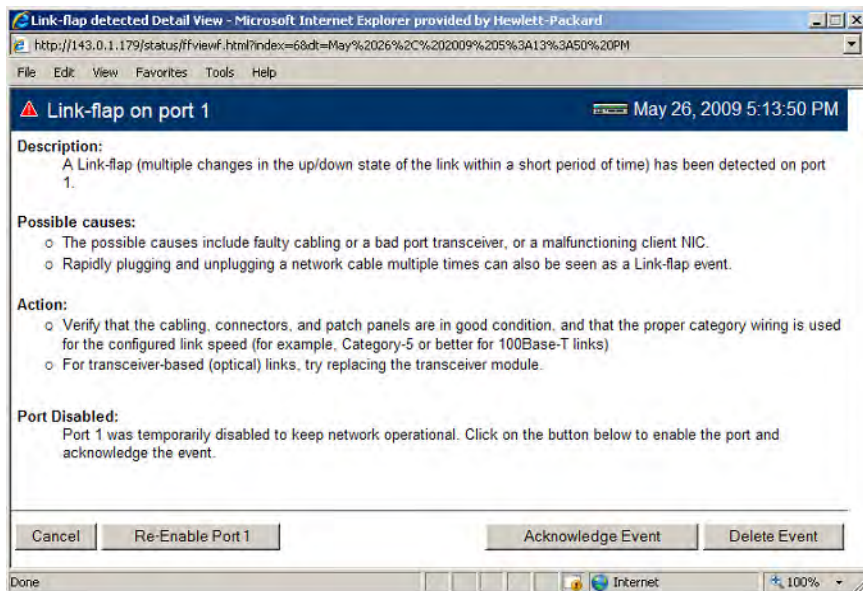


Figure 3. Link-flap on port 1 event detail dialog box

- **Enhancement (PR_0000040783)** — This enhancement reduces the down time when unicast routing indicates a Candidate Rendezvous Point (C-RP) is not reachable. Upon detecting a C-RP has become unreachable, the Bootstrap Router (BSR) sends a new Bootstrap Message (BSM) with a zero holdtime for the unreachable C-RP. All devices in the PIM domain should then remove this C-RP from their RP-set.
- **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. The command syntax is as follows:

```
Switch# debug ip pim packet <cr>
```

IP PIM debug output may be filtered further by specifying a source IP address, VLAN and group.

Use the CLI help for syntax details.

- **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 Switch 6600 Series is now enabled for IPv6 host functionality.
- **Enhancement (PR_0000045749)** — Module reload enhancement. For more information, see [“Module Reload \(5400zl and 8200zl switches\)”](#) below.

Module Reload (5400zl and 8200zl switches)

The Module reload feature allows you to reset a module by initiating a warm reboot of a specified module or modules. This saves time over rebooting the entire switch, which can take several minutes to complete and disrupts all users on the switch. The specified module has its power turned off, and then turned on again. This causes the module to reset to a known good state and reload its software.

Syntax: [no] reload [[after <[[DD:] HH:] MM>] | [at HH:MM [:SS] [MM/DD[/[YY]YY]]] | [module <slot-id range>]]

*When specified with the **module** parameter, initiates a reload of the module in the specified slot or slots by turning the slot power off, then on again. A valid slot or range of slots must be specified. The **at** and **after** parameters are not allowed with the **module** option. The **no** version of the command is not valid with the **module** option.*

*When the **reload** command is executed without any parameters, an immediate switch reload occurs.*

Note: This feature is not supported for ProCurve One modules.

at: Schedules a whole switch reload at a specified date and time. The time must not be more than 99 days in the future. Minimum required input is **HH:MM**. Cannot be used with the **module** option.

after: Schedules a whole switch reload after the specified length of time, which must not be more than 99 days in the future. Minimum required input is **MM**. Cannot be used with the **module** option

module: Powers the module on or off, forcing a software reload of the specified module or modules.

```
Switch(config)# reload module C
The 'reload module' command will shutdown the specified modules. Ports on
specified modules will no longer pass traffic. Any management traffic to
the switch which passes through the affected modules will be interrupted
(e.g. ssh, telnet, snmp). This command may take up to 2 minutes to power
down all specified modules. Please check the event log for current status
of module power down, power up cycle. Continue [y/n]?
```

Figure 4. Example of Reloading a Specified Module

Use the **show reload** command to display the reload information. This can include:

- A scheduled, pending reload of the entire switch
- A statement that no reload is scheduled

- The time of the last reload of each module on the system

```
Switch(config)# reload at 23:45
Reload scheduled at 23:45:47 6/16/2010
(in 0 days, 1 hours, 41 minutes)

Switch(config)# show reload at
Reload scheduled for 23:45:47 06/16/2010
(in 0 days, 1 hours, 40 minutes)

Switch(config)# show reload after
Reload scheduled for 23:45:47 6/16/2010
(in 0 days, 1 hours, 40 minutes)
```

Figure 5. Example of the Scheduled Reload At Information

```
Switch(config)# reload after 35
Reload scheduled in 0 days, 0 hours, 35 minutes

Switch(config)# show reload at
Reload scheduled in 0 days, 0 hours, 34 minutes

Switch(config)# show reload after
Reload scheduled in 0 days, 0 hours, 34 minutes
```

Figure 6. Example of the Scheduled Reload After Information

```
Switch(config)# show reload module

Module Reload information:

Module | Last reload date
-----+-----
C      | 10:50:51 01/13/2010
```

Figure 7. Example of the Module Reload Information

Version K.15.01.0032 Enhancements

- **Enhancement (PR_0000018479)** — Longer usernames and passwords are now allowed, and some special characters may be used.

Username and Password Size Increase

For security reasons, it is desirable to allow the configuration of longer usernames and passwords than is currently allowed on the switch. The limits on length will be extended to 64 characters for the following authentication methods:

- Front-end—WEB User Interface, SSH, and Telnet
- Back-end—RADIUS, TACACS+, and Local

General Rules for Usernames and Passwords

Usernames and passwords are case-sensitive. ASCII characters in the range of 33-126 are valid, including:

- A through Z uppercase characters
- a through z lower case characters
- 0 through 9 numeric characters
- Special characters ' ~ ! @ # \$ % ^ & * () - _ = + [] { } \ | ; : ' " , < > / ? (see Restrictions, below)

The SPACE character is allowed to form a username or password pass-phrase. The username must be in quotes, for example “The little brown fox”. A space is not allowed as part of a username without the quotes. A password that includes a space or spaces should not have quotes.

Restrictions for the Setmib Command

Usernames and passwords can be set using the CLI command **setmib**. They cannot be set using SNMP.

- Quotes are permitted for enclosing other characters, for example, a username or password of **abcd** can be enclosed in quotes “**abcd**” without the quotes becoming part of the username or password itself. Quotes can also be inserted between other characters of a username or password, for example, **ab**”**cd**. A pair of quotes enclosing characters followed by any additional characters is invalid, for example, “**abc**”**d**.
- Spaces are allowed in usernames and passwords. The username or password must be enclosed in quotes, for example, “**one two three**”. A blank space or spaces between quotes is allowed, for example, “ ”.

Additional Restrictions

Some authentication servers prevent the usage of special symbols such as the backslash (\) and quotes (“”). The switch allows the use of these symbols in configurable credentials, but using them may limit access for some users who may use different client software. Please refer to the vendor’s documentation for specific information about these restrictions.

Operating Notes on Upgrading or Downgrading Software Versions

When you update software from a version that does not support long passwords to a version that supports long passwords, the existing usernames and passwords continue to be there; no further action is required.

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

1. Reset the username and/or password to be no more than 16 characters in length, and without any special characters, using the CLI command **password** or the equivalent in the WebAgent. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).

```
Switch(config)# password manager
New password: *****
Please retype new password: *****
Switch(config)# write mem
```

Or

2. Execute the CLI command **no password all**. This clears all the passwords. Then execute a CLI **write memory** command (required if the **include-credentials** feature has ever been enabled).

```
Switch(config)# no password all
Password protections will be deleted, do you want to continue [y/n]? y
Switch(config)# write mem
```

Or

3. Clear the password 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).

If You Cannot Access the Switch Using the Previous Password

If you cannot access the switch after a software version downgrade, clear the password by using the "Clear" button on the switch to regain access. Then boot into a software version that supports long passwords, and perform steps 1, 2, or 3 in the preceding section.

Version K.15.02.0004 Enhancements

Version K.15.02.004 includes the following enhancements.

- **Enhancement (PR_0000018427)**—Multicast ARP support enhancement.

Multicast ARP Support

To support IP multicasting, the multicast address range of 01-00-5E-00-00-00 to 01-00-5E-7F-FF-FF is reserved for Ethernet MAC addresses. The command **ip arp-mcast-replies** enables acceptance of the MAC addresses in the IP multicast range

Syntax: [no] ip arp-mcast-replies

Enables or disables accepting multicast MAC addresses in the IP multicast address range in ARP requests and replies.

Default: Disabled.

```
Switch(config)# ip arp-mcast-replies
```

Figure 8. Example of Enabling the Acceptance of Multicast MACs in the IP Multicast Range

- **Enhancement (PR_0000044183)** —Display interface configuration enhancement.

Display Configuration of Selected Interface

The options provided in this feature allow you to display all the configurations on a specified interface or VLAN with a single command. You can use the options with the startup config command, **show config**, and the running config command, **show running-config**.

Running Configuration Output

You can display the running configuration using this command. An example of the output is shown in [Figure 9](#).

Syntax: show running-config [interface <port-list | loopback <0-7> | vlan <vlan-id-list>]

Displays running configuration information about the selected interface when one is specified. The interfaces can be ports, VLANs, or SVLANs.

Note

The **show running config interface/vlan/svlan** command output cannot be downloaded to the switch; it will not download correctly. Copying and pasting the displayed configuration information into the switch configuration is not supported. This feature only provides a display of all the configuration information for a selected interface or range of interfaces in a single view.

```
Switch(eth-A2-A4)# show running-config

Running configuration:

; J8698A Configuration Editor; Created on release #K.14.54C

hostname "Switch 5412z1"
interface A2
  disable
  name "test1"
  flow-control
  broadcast-limit 80
  speed-duplex 100-full
  unknown-vlans Block
  qos priority 4
  lacp Passive
  gvrp join-timer 30
  gvrp leave-timer 60
  gvrp leaveall-timer 700
exit
interface A3
  disable
  name "test1"
  flow-control
  broadcast-limit 80
  speed-duplex 100-full
  unknown-vlans Block
  qos priority 4
  lacp Passive
  gvrp join-timer 30
  gvrp leave-timer 60
  gvrp leaveall-timer 700
exit
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A4,C1-C24,F1-F24
  ip address dhcp-bootp
  exit
interface A2
  dhcp-snooping trust
  bandwidth-min output 20 10 10 10 20 10 10 10
  rate-limit bcast in percent 75
  ipv6 access-group "check" in
  exit
interface A3
  dhcp-snooping trust
  bandwidth-min output 20 10 10 10 20 10 10 10
  rate-limit bcast in percent 75
  ipv6 access-group "check" in
  exit
```

Configuration information for interfaces A2 and A3 is shown in two different places in the config file.

Figure 9. Example of Running Configuration Output for Interfaces A2 - A4

Figure 10 shows an example of the running config for a range of interfaces. The configuration information for interfaces A2 and A3 is now displayed together.

```
Switch(config)# show running-config interface A2-A3
```

```
Running configuration:
```

```
interface A2
  disable
  name "test1"
  flow-control
  broadcast-limit 80
  speed-duplex 100-full
  unknown-vlans block
  qos priority 4
  gvrp join-timer 30 leave-timer 60 leaveall-timer 700
  dhcp-snooping trust
  lacp passive
  bandwidth-min output 20 10 10 10 20 10 10 10
  rate-limit bcast in percent 75
  ipv6 access-group "check" in
  untagged vlan 1
  exit
interface A3
  disable
  name "test1"
  flow-control
  broadcast-limit 80
  speed-duplex 100-full
  unknown-vlans block
  qos priority 4
  gvrp join-timer 30 leave-timer 60 leaveall-timer 700
  dhcp-snooping trust
  lacp passive
  bandwidth-min output 20 10 10 10 20 10 10 10
  rate-limit bcast in percent 75
  ipv6 access-group "check" in
  untagged vlan 1
  exit
```

All the information for interfaces A2 and A3 is shown together in the output.

Figure 10. Example of Running Config Output for a Specified Interface Range

Figure 11 shows an example of the running config file for a range of interfaces after some configuration changes have been made.

```
Switch(config)# no stack
Switch(config)# mesh 2-3
Command will take effect after saving configuration and reboot.

Switch(config)# write memory
Switch(config)# reload

Switch# show running-config interface 2-3

Running configuration:

interface 2
  untagged vlan 1
  mesh
  exit
interface 3
  flow-control
  untagged vlan 1
  mesh
  exit
```

Figure 11. Example of Running Config Output for a Range of Interfaces

Figure 12 is an example of the running config output showing VLAN information.


```
Switch(config)# show running-config

Running configuration:

; J8698A Configuration Editor; Created on release #K.14.54C

hostname "Switch 5412z1"
module 1 type J9309A
module 3 type J8702A
module 6 type J8702A
ip routing
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A4,C1-C24,F1-F24
  ip address dhcp-bootp
  exit
vlan 2
  name "test-vlan-2"
  ip helper-address 4.1.1.1
  ip helper-address 5.1.1.1
  ip address 1.1.1.1 255.255.255.0
  ipv6 address 2001::/64 anycast
  ipv6 enable
  exit
vlan 3
  name "VLAN3"
  ip helper-address 7.1.1.1
  ip forward-protocol udp 7.1.1.1 snmp
  ip forward-protocol udp 11.1.1.2 dns
  no ip address
  exit
vlan 4
  name "VLAN4"
  ip address 5.1.1.1 255.255.255.0
  ip bootp-gateway 5.1.1.1
  exit
logging 10.0.102.90
logging system-module ospf
ip route 5.1.1.0 255.255.255.0 vlan 4 distance 3
```

VLAN 4 configuration information is not together in the config file output.

Figure 12. Example of Running Config Output Showing VLAN Information

In [Figure 13](#), the configuration information for VLAN 4 is now displayed in one place.

```
Switch(config)# show running-config vlan 3-4

Running configuration:

vlan 3
  name "VLAN3"
  ip helper-address 7.1.1.1
  ip forward-protocol udp 7.1.1.1 snmp
  ip forward-protocol udp 11.1.1.2 dns
  no ip address
  exit
vlan 4
  name "VLAN4"
  ip address 5.1.1.1 255.255.255.0
  ip bootp-gateway 5.1.1.1
  ip route 5.1.1.0 255.255.255.0 distance 3
  exit
```

VLAN 4 configuration information is displayed together in the output.

Figure 13. Example of Running Config Output for a Range of VLANs

[Figure 14](#) shows an example of the running config for a range of VLANs after configuration changes have been made to selected VLANs.

```
Switch(config)# dhcp-snooping
Switch(config)# vlan 14
Switch(vlan-14)# exit
Switch(config)# vlan 15
Switch(vlan-15)# exit
Switch(config)# vlan 23
Switch(vlan-23)# exit
Switch(config)# dhcp-snooping vlan 14-15
Switch(config)# static-mac 00:11:22:33:44:55 vlan 23 interface A3
Switch(config)# spanning-tree instance 2 vlan 15

Switch(config)# show running-config vlan 14-15

Running configuration:

vlan 14
  name "VLAN14"
  no ip address
  dhcp-snooping
  exit
vlan 15
  name "VLAN15"
  no ip address
  dhcp-snooping
  spanning-tree instance 2
  exit
```

Figure 14. Example of Output for Running Config for a Range of VLANs

Startup Configuration Output

You can display the startup configuration using this command. An example of the startup configuration output is shown in [Figure 15](#).

Syntax: show config [interface <port-list | loopback <0-7> | vlan <vlan-id-list>]

Displays startup configuration information about the selected interface when one is specified. The interfaces can be ports, VLANs, or SVLANs.

```
Switch(config)# show config

Startup configuration:

; J8698A Configuration Editor; Created on release #K.14.54C

hostname "Switch 5412z1"
module 1 type J9309A
module 3 type J8702A
module 6 type J8702A
vlan 1
    name "DEFAULT_VLAN"
    untagged A1-A4,C1-C9,C15-C24,F1-F24
    ip address dhcp-bootp
    no untagged C10-C14
    exit
vlan 5
    name "VLAN5"
    untagged C10-C14
    ip address 5.1.1.1 255.255.255.128
    exit
interface loopback 5
    ip address 7.1.1.1
    exit
interface loopback 7
    ip address 12.1.1.1
    exit
snmp-server community "public" unrestricted
```

Figure 15. Example of Startup Configuration Output

Figure 16 shows an example of the startup config output for a selected VLAN.

```
Switch(vlan-5)# show config vlan 5

Startup configuration:

vlan 5
    name "VLAN5"
    untagged C10-C14
    ip address 5.1.1.1 255.255.255.128
    exit
```

Figure 16. Example of Startup Config Output for a Specific VLAN

Figure 17 shows an example of the startup config output for a range of interfaces for a specific VLAN.

```
Switch(vlan-5)# show config interface C10-C13

Startup configuration:

interface C10
    untagged vlan 5
    exit
interface C11
    untagged vlan 5
    exit
interface C12
    untagged vlan 5
    exit
interface C13
    untagged vlan 5
    exit
```

Figure 17. Example of Startup Config Output for a Range of Interfaces for a Specific VLAN

■ **Enhancement (PR_0000045649)**—Post-logon banner enhancement.

Post-logon Banner Enhancement

A text message that has been configured with the **banner motd** command displays with the authentication prompt when a user opens a console, telnet, SSH, or WebAgent session.

The **exec** option of the **banner** command allows a user-configurable message to be displayed after the user has been authenticated. If there is no password on the switch, the exec banner message displays immediately.

Syntax: [no] banner exec <ASCII-string>

Sets the exec banner text. Text can be multiple lines up to 3070 characters, and can consist of any printable character except the tilde (~) and the delimiting character.

<ASCII-string>: *The text must end with a delimiting character, which can be any single character except the tilde (~) character.*

*The **no** version of the command removes the banner exec text.*

```
Switch(config)# banner exec &  
Enter TEXT message. End with the character &  
This is Switch A in the language lab &
```

Figure 18. Example of the banner exec Command

To display the status and text for the exec banner configuration, use the **show banner exec** command.

```
Switch(config)# show banner exec  
  
Banner Information  
  
Banner Status: Enabled  
Configured Banner:  
  
This is Switch A in the language lab
```

Figure 19. Example Displaying Exec Banner Configuration

WebAgent Display of Exec Banner Message

If the MOTD banner message has been configured, it is displayed first. If the **exec** banner option has also been configured, the MOTD banner message is followed by a [Continue](#) link to the next page.

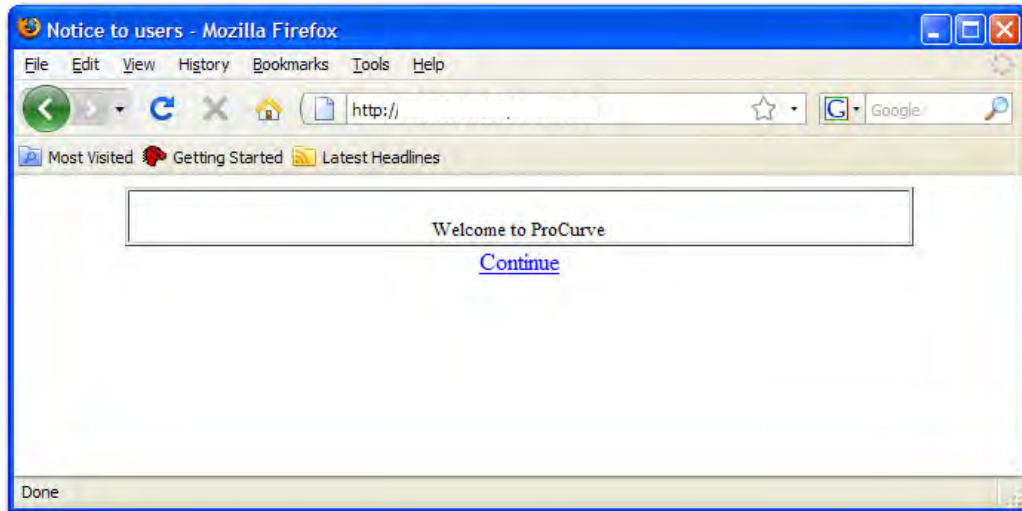


Figure 20. Example of MOTD Message in the WebAgent

Clicking on [Continue](#) displays the Username/Password dialog box if the switch has been configured with password security. If no password has been configured, the exec banner message displays immediately.

After being authenticated successfully when a password has been configured, the exec banner message displays. Click on the [Continue](#) link to proceed to the WebAgent Home Page.

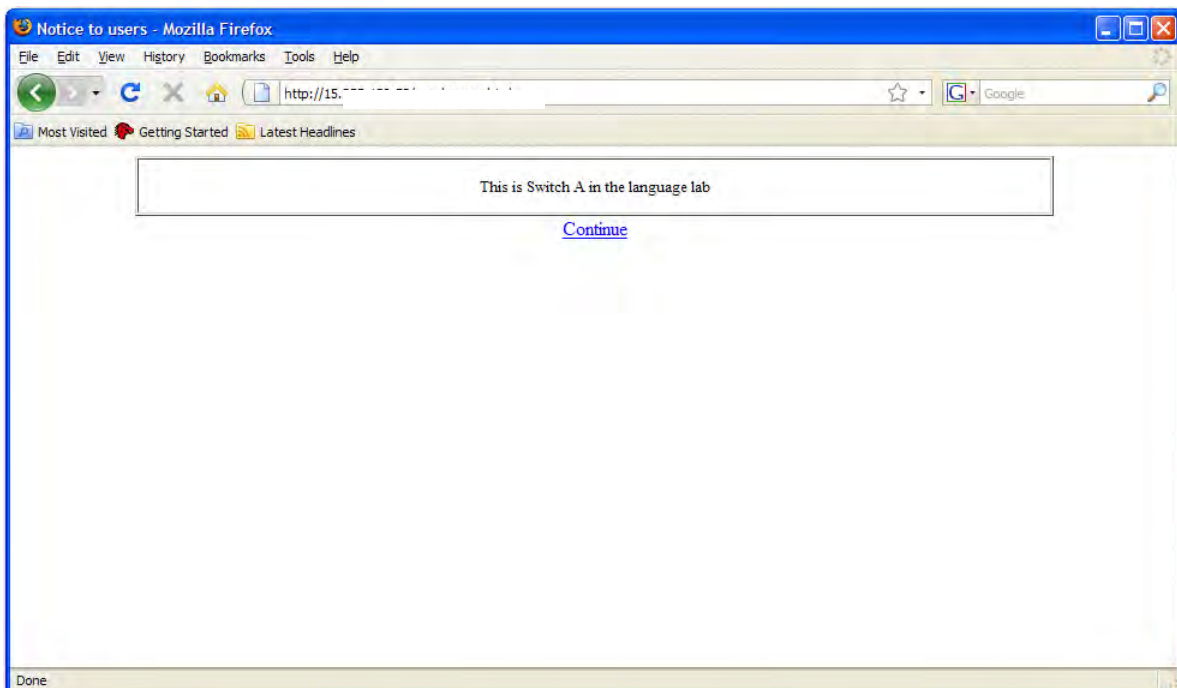


Figure 21. Example of Exec Banner Message

SNMP Support

The MIB variables required to support Exec banner are in the hpiefBasic.mib file.

Error Messages

Error Message	Description
Delimiter must be a single character	Use a single ASCII character for a delimiter at the end of the Exec Banner message
Tildes (~) are not allowed.	Do not use a tilde in the Exec Banner message.
String for Banner Exec is too long. Allowed length is 3070.	The Exec Banner message can be up to 3070 characters long.

- **Enhancement (PR_0000045707)**—The tilde character is now allowed in TACACS+ and RADIUS encryption keys.

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

This feature allows you to configure a TACACS+ or RADIUS encryption key that includes a tilde (~) as part of the key, for example, “hp~switch”. It is not backward compatible; the “~” character is lost if you use a software version that does not support the “~” character.

SNMP already supports the inclusion of the tilde character in a key.

Configuring TACACS+ Keys

Global Keys. If you need only one encryption key for the switch to use in all attempts to authenticate through a TACACS+ server, configure a global key.

To configure a global encryption key for TACACS+, enter this command.

Syntax: [no] tacacs-server key <key-string>

Configures an optional global encryption key. Keys configured in the switch must exactly match the encryption keys configured in the TACACS+ servers that the switch will attempt to use for authentication.

*The **no** form of the command removes the global encryption key.*

Switch(config)# tacacs-server key hp~switch											
Switch(config)# show tacacs											
Status and Counters - TACACS Information											
Timeout: 5											
Source IP Selection: Outgoing Interface											
Encryption Key: hp~switch											
Server	IP Addr	Opens	Closes	Aborts	Errors	Pkts Rx	Pkts Tx	OOBM			
-----	-----	-----	-----	-----	-----	-----	-----	-----			
10.10.10.2		0	0	0	0	0	0	0			

Figure 22. Example of Configuring a Global Encryption Key for TACACS+ with a ~ Character

Host-Specific Keys

If the switch is configured to access multiple TACACS+ servers having different encryption keys, you can configure the switch to use different encryption keys for different TACACS+ servers.

Syntax: [no] tacacs-server host <ip-addr> [key <key-string>]

Adds a TACACS+ server and optionally assigns a server-specific encryption key.

*The **no** form of the command removes a TACACS+ server assignment (including its server-specific encryption key, if any).*

```
Switch(config)# tacacs-server host 10.10.10.2 key hp~switch
```

Figure 23. Example of Configuring a Host-Specific Key

Use the **show running-config** command to display the key information.

```
Switch(config)# show running-config

Running configuration:

; J8692A Configuration Editor; Created on release #K.14.00x

hostname "Switch 3500yl-24G"
module 1 type J86xxA
vlan 1
    name "DEFAULT_VLAN"
    untagged 1-24
    ip address dhcp-bootp
    exit
banner motd "good morning
tacacs-server host 10.10.10.2 key "hp~switch"
snmp-server community "public" unrestricted
```

Shows the key configured for a specific host.

Figure 24. Example of the Running Configuration File Showing the Host-Specific Key for TACACS+ with the "~" Included

For more information about TACACS+, see the chapter "TACACS+ Authentication" in the *Access Security Guide* for your switch.

Configuring RADIUS Keys

Global Keys. To configure a global key for RADIUS authentication, enter this command.

Syntax: [no] radius-server key <global-key-string>

Specifies the global encryption key the switch uses with servers for which the switch does not have a server-specific key assignment. This key is optional if all RADIUS server addresses configured in the switch include a server-specific encryption key.

Default: Null

*The **no** form of the command removes the global encryption key.*

```
Switch(config)# radius-server key hp~switch

Switch(config)# show radius
Status and Counters - General RADIUS Information
Deadtime (min): 0
Timeout: 5
Retransmit Attempts: 3
Global Encryption Key: hp~switch
Dynamic Authorization UDP Port: 3799
Source IP Selection: Outgoing Interface

Auth Acct DM/Time

Server IP Addr Port Port CoA Window Encryption Key OOBM
-----
10.33.18.127 1812 1813 No 300 No
```

Global encryption key

Figure 25. Example of RADIUS Global Encryption Key with a ~ Character Included

Host-Specific Keys. To configure a host-specific key for RADIUS authentication, enter this command.

Syntax: [no] radius-server host <ip-address> key <key-string>

Optional. Specifies an encryption key for use during authentication (or accounting) sessions with the specified server. This key must match the encryption key used on the RADIUS server. Use this command only if the specified server requires a different encryption key than configured for the global encryption key.

Default: Null

*Use the **no** form of the command to remove the key for a specified server.*


```
Switch(config)# radius-server host 10.33.18.127 key hp~switch

Switch(config)# show radius

Status and Counters - General RADIUS Information

Deadtime(min) : 0
Timeout(secs) : 5
Retransmit Attempts : 5
Global Encryption Key :

Server IP Addr      Auth   Acct
-----
10.33.18.127      1812   1813   hp~switch
```

Figure 26. Example of Host-Specific Key for RADIUS Authentication

```
Switch(config)# show running

Running configuration:

; J8692A Configuration Editor; Created on release #K.14.00x

hostname "Switch 3500yl-24G"
module 1 type J86xxA
vlan 1
    name "DEFAULT_VLAN"
    untagged 1-24
    ip address dhcp-bootp
    exit
banner motd "good morning
radius-server host 10.33.18.127 key "hp~switch"
snmp-server community "public" unrestricted
```

Shows the key configured for a specific host.

Figure 27. Example of Running Configuration File Showing the Host-Specific Key for RADIUS Authentication

For more information about RADIUS keys, see the chapter “RADIUS Authentication, Authorization, and Accounting” in the *Access Security Guide* for your switch.

- **Enhancement (PR_0000045711)** —Web authentication message enhancement.

Web Auth Deny Message

This feature allows administrators to configure custom messages that are displayed when authentication with the RADIUS server fails. The messages are appended to the existing internal web page that displays during the authentication process. Messages can be configured using the CLI, or centrally using the RADIUS server, and can provide a description of the reason for the failure as well as possible steps to take to resolve the authentication issue. There is no change to the current web authentication functionality..

Syntax: [no] aaa port-access web-based access-denied-message <<access-denied-str> | radius-response>

Specifies the text message (ASCII string) shown on the web page after an unsuccessful login attempt. The message must be enclosed in quotes.

*The **no** form of the command means that no message is displayed upon failure to authenticate.*

Default: The internal web page is used. No message will be displayed upon authentication failure.

access-denied-str: *The text message that is appended to the end of the web page when there is an unsuccessful authentication request. The string can be up to 250 ASCII characters.*

radius-response: *Use the text message provided in the RADIUS server response to the authentication request.*

```
Switch(config)# aaa port-access web-based access-denied-message "Please contact
your system administrator to obtain authentication privileges."
```

Figure 28. Example of Configuring an Access Denied Message on the Switch

```
Switch(config)# show port-access web-based config

Port Access Web-based Configuration

DHCP Base Address       : 192.168.0.0
DHCP Subnet Mask        : 255.255.248.0
DHCP Lease Length       : 10 seconds
Allow RADIUS-assigned dynamic (GVRP) VLANs[No]: Yes
Access Denied Message   : Custom:
    Please contact your system administrator to obtain authentication privileges.
```

Port	Enabled	Client Limit	Client Moves	Logoff Period	Re-auth Period	Unauth VLAN ID	Auth VLAN ID	Ctrl Dir
A1	Yes	1	No	300	60	1	2	both
A2	Yes	18	No	999999999	999999999	0	0	both
A3	Yes	22	No	999999999	999999999	4096	4096	both

Figure 29. Example of Output showing the Custom Access Denied Message

The example in [Figure 30](#) shows the text of the Access Denied Message when the **radius-response** option is configured.

```
Switch(config)# show port-access web-based config
```

Port Access Web-based Configuration

DHCP Base Address : 192.168.0.0
 DHCP Subnet Mask : 255.255.248.0
 DHCP Lease Length : 10 seconds
 Allow RADIUS-assigned dynamic (GVRP) VLANs[No]: Yes
 Access Denied Message : Retrieved from Radius

Port	Enabled	Client Limit	Client Moves	Logoff Period	Re-auth Period	Unauth VLAN ID	Auth VLAN ID	Ctrl Dir
A1	Yes	1	No	300	60	1	2	both
A2	Yes	18	No	300	999999999	0	0	both
A3	Yes	22	No	300	999999999	4096	4096	both

Figure 30. Example of Access Denied Message when radius-response is Configured

Unauthenticated clients may be assigned to a specific static, untagged VLAN (**unauth-vid**), to provide access to specific (guest) network resources. If no VLAN is assigned to unauthenticated clients, the port is blocked and no network access is available.

Web Page Display of Access Denied Message

The web page in [Figure 31](#) is an example of the denied access message that appears when **unauth-vid** is configured.

Invalid Credentials

Your credentials were not accepted. You may have limited network access. Please wait while the configuration completes.

Estimated time remaining: 35 seconds

Please contact your system administrator to obtain authentication privileges.

© 2009 Hewlett Packard Development Company, L.P.

Figure 31. Example of Web Page with Configured Access Denied Message When unauth-vid is Configured

Figure 32 shows an example of a web page displaying the access denied message when an **auth-vid** is not configured.

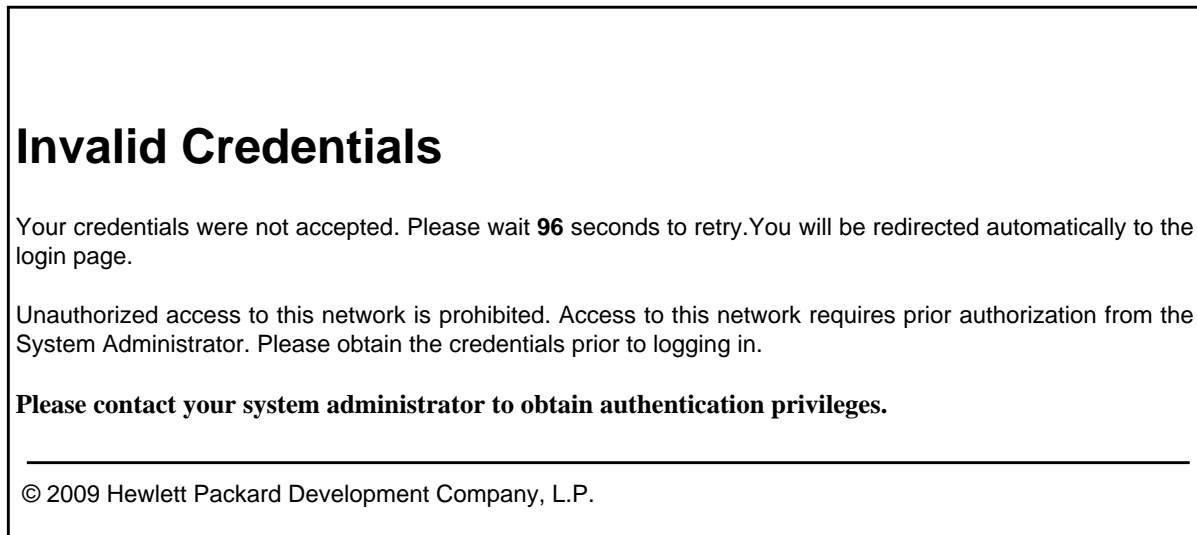


Figure 32. Example of Web Page with Configured Access Denied Message When unauth-vid is not Configured

The **show running-config** command displays the client's information, including the configured access denied message.

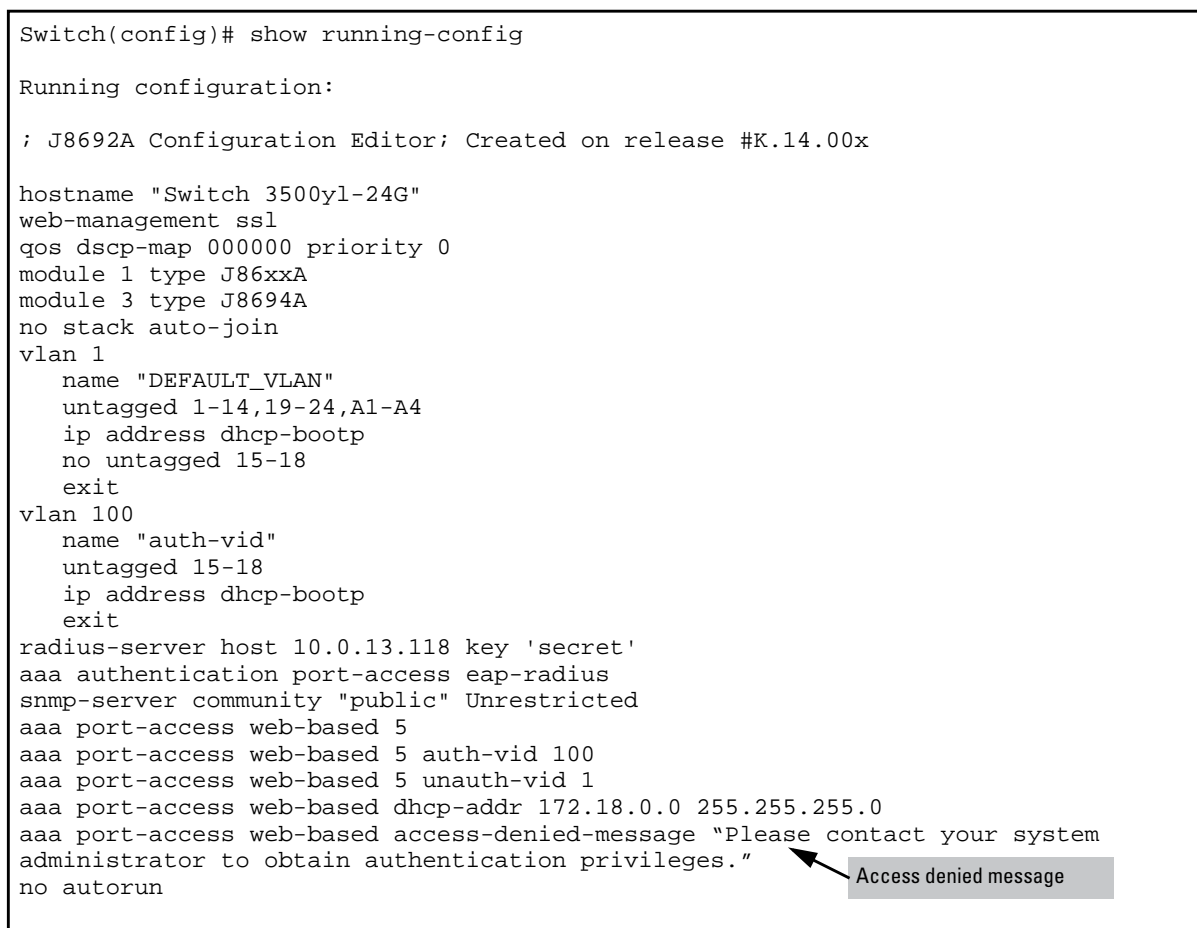


Figure 33. Example of Running Configuration Output Displaying Access Denied Message

```
Switch(config)# show running-config

Running configuration:

; J8692A Configuration Editor; Created on release #K.14.00x

hostname "Switch 3500yl-24G"
web-management ssl
qos dscp-map 000000 priority 0
module 1 type J86xxA
module 3 type J8694A
no stack auto-join
vlan 1
    name "DEFAULT_VLAN"
    untagged 1-14,19-24,A1-A4
    ip address dhcp-bootp
    no untagged 15-18
    exit
vlan 100
    name "auth-vid"
    untagged 15-18
    ip address dhcp-bootp
    exit
radius-server host 10.0.13.118 key 'secret'
aaa authentication port-access eap-radius
snmp-server community "public" Unrestricted
aaa port-access web-based 5
aaa port-access web-based 5 auth-vid 100
aaa port-access web-based 5 unauth-vid 1
aaa port-access web-based dhcp-addr 172.18.0.0 255.255.255.0
aaa port-access web-based access-denied-message radius-response
```

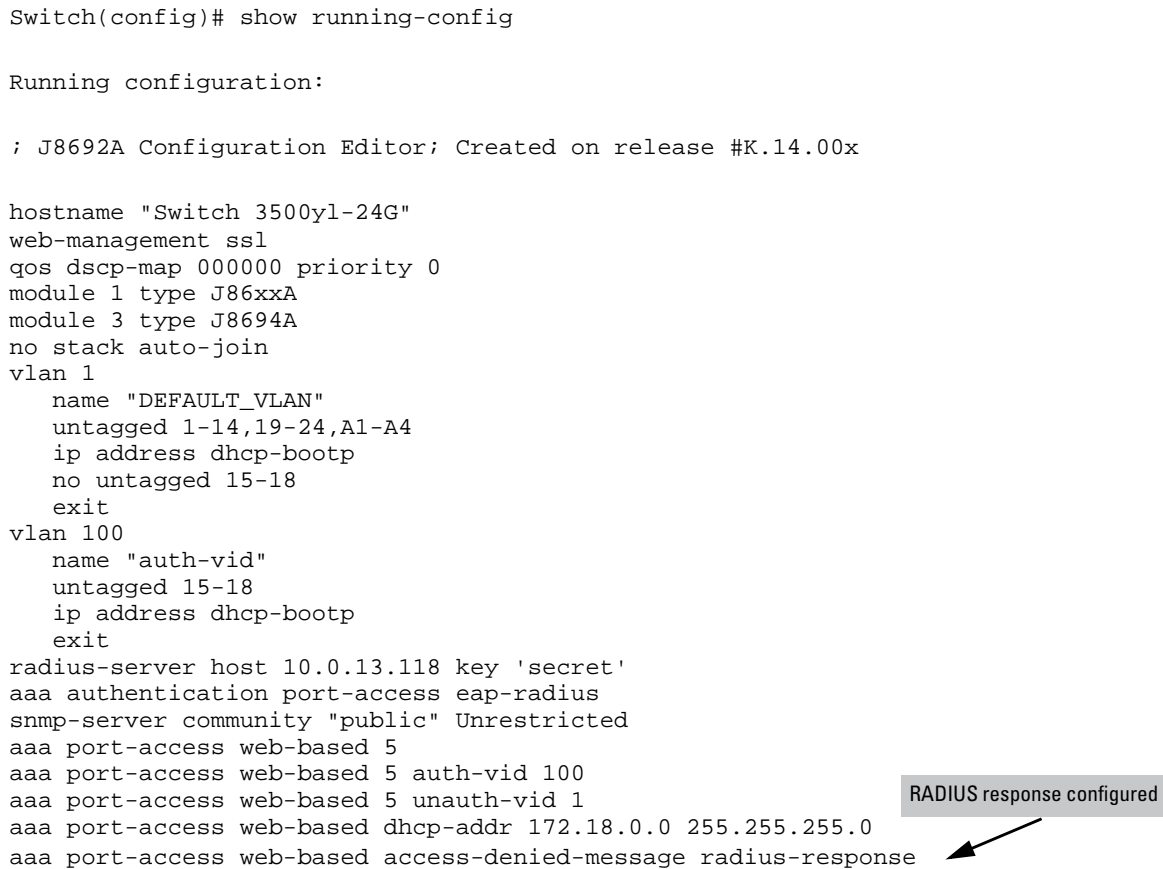


Figure 34. Example of Running Configuration Output When RADIUS Response is Configured

- **Enhancement (PR_0000045752)**—User-configurable per-port MAC address enhancement.

Port Security Per-Port MAC Increase

User-configurable per-port MAC addresses have been limited to 32 addresses. This enhancement increases the number of user-configurable per-port MAC addresses from 32 to 64 addresses. The switch-wide per-port address limit is unchanged.

- **Enhancement (PR_0000046912)** —Adds support for LLDP PoE+.

PoE with LLDP

Overview

The data link layer classification (DLC) for PoE provides more exact control over the power requirement between a PSE and PD. The DLC works in conjunction with the physical layer classification (PLC) and is mandatory for any Type-2 PD that requires more than 12.95 watts of input power.

Note DLC is defined as part of the IEEE 802.3at standard.

The power negotiation between a PSE and a PD can be implemented at the physical layer or at the data link layer. After the link is powered at the physical layer, the PSE can use LLDP to repeatedly query the PD to discover the power needs of the PD. Communication over the data link layer allows finer control of power allotment, which makes it possible for the PSE to supply dynamically the power levels needed by the PD. Using LLDP is optional for the PSE but mandatory for a Type 2 PD that requires more than 12.95 watts of power.

If the power needed by the PD is not available, that port is shut off.

PoE Allocation

There are two ways LLDP can negotiate power with a PD:

- Using LLDP MED TLVs: Disabled by default. Can be enabled using the **int <port-list> PoE-lldp-detect [enabled | disabled]** command, as shown below. LLDP MED TLVs sent by the PD are only used to negotiate power if the LLDP PoE+ TLV is disabled or inactive; if the LLDP PoE+ TLV is sent as well (not likely), the LLDP MED TLV is ignored.
- Using LLDP PoE+ TLVs: Enabled by default. The LLDP PoE+ TLV is always advertised unless it has been disabled. It is enabled using the **lldp config <port-list> dot3TlvEnable poeplus_config** command. See [“Enabling Advertisement of PoE+ TLVs” on page 41](#) for the command syntax.) It always takes precedence over the LLDP MED TLV.

Enabling **PoE-lldp-detect** allows the data link layer to be used for power negotiation. When a PD requests power on a PoE port, LLDP interacts with PoE to see if there is enough power to fulfill the request. Power is set at the level requested. If the PD goes into power-saving mode, the power supplied is reduced; if the need for power increases, the amount supplied is increased. PoE and LLDP interact to meet the current power demands.

Syntax: int <port-list> PoE-lldp-detect [enabled | disabled]

*Allows the data link layer to be used for power negotiation between a PD on a PoE port and LLDP.
Default: Disabled*

For example, you can enter this command to enable LLDP detection:

```
Switch(config)# int 7 PoE-lldp-detect enabled
```

or in interface context:

```
Switch(eth-7)# PoE-lldp-detect enabled
```

Note

Detecting PoE information via LLDP only affects power delivery; it does not affect normal Ethernet connectivity.

You can view the settings by entering the **show power-over-ethernet brief** command:

```
Switch(config)# show power-over-ethernet brief
```

Status and Counters - Port Power Status								
PoE Port	Power Enable	LLDP Detect	Power Priority	Alloc By	PoE Val	Configured Type	Detection Status	Power Class
A1	Yes	enabled	low	usage	5	Phone-1	Delivering	0
A2	Yes	disabled	low	usage	17		Searching	1
A3	Yes	disabled	low	usage	17		Searching	0
A4	Yes	disabled	low	usage	17		Searching	2
A5	Yes	disabled	low	usage	17		Searching	0
A6	Yes	disabled	low	value	17		Searching	0
A7	Yes	enabled	low	value	5	Phone-2	Delivering	0
A8	Yes	disabled	low	value	17		Searching	0

Figure 35. Example of Port with LLDP Configuration Information Obtained from the Device

Enabling Advertisement of PoE+ TLVs

To initiate the advertisement of power with PoE+ TLVs, the following command is configured with the **poeplus_config** option.

Syntax: `lldp config <port-list> dot3TlvEnable poeplus_config`

Enables advertisement of data link layer power using PoE+ TLVs. The TLV is processed only after the physical layer and the data link layer are enabled. The TLV informs the PSE about the actual power required by the device.

Default: Enabled

Displaying PoE When Using LLDP Information

Displaying LLDP Port Configuration. To display information about LLDP port configuration, use the **show lldp config** command.

Syntax: `show lldp config <port-list>`

Displays the LLDP port configuration information, including the TLVs advertised.

```
Switch(config)# show lldp config 4

LLDP Port Configuration Detail

Port : 4
AdminStatus [Tx_Rx] : Tx_Rx
NotificationEnabled [False] : False
Med Topology Trap Enabled [False] : False

TLVS Advertised:
* port_descr
* system_name
* system_descr
* system_cap

* capabilities
* network_policy
* location_id
* poe

* macphy_config
* poeplus_config

IpAddress Advertised:
```

Figure 36. Example of LLDP Port Configuration Information with PoE

See the chapter “Power over Ethernet (PoE/PoE+) Operation” in the *Management and Configuration Guide* for your switch for more information about PoE.

- **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.

Increase MAC Auth Client Limit to 256

The client limit is 256 clients per-port for MAC-auth and Web-auth; the client limit for 802.1X is 32 clients per port. The MAC-auth and Web-auth limit of 256 clients only applies when there are fewer than 16,384 authentication clients on the entire switch. After the limit of 16,384 clients is reached, no additional authentication clients are allowed on any port for any method.

The following commands are used to specify client limits:

```
aaa port-access mac-based <port-list> [addr-limit]
aaa port-access web-based <port-list> [client-limit]
aaa port-access authenticator <port-list> [client-limit]
```


- **Enhancement (PR_0000052801)**—Categorize CLI Return Messages enhancement.

Categorize CLI Return Messages

When a CLI command returns a message, that message is now prefixed with a category describing the type, as follows:

- Error
- Warning
- Information

Syntax: session show-message-type [enable | disable]

When enabled, the CLI return messages are prefixed with string that indicates the type of message. Entered at the manager level.

*The **disable** option disables prefixing returned messages for the session for which this command is executed.*

Note: *This setting is not saved when the switch is rebooted.*

Default: *Disabled on all CLI sessions*

```
Switch(config)# router rip
Error: IP Routing support must be enabled first.

Switch(config)# qinq mixed vlan
Warning: This command will reboot the device. Any prior configuration on this
config file will be erased and the device will boot up with a default configuration
for the new qinq mode.
Do you want to continue [y/n]? n

Switch(config)# snmp-server mib hpSwitchAuthMIB included
Information: For security reasons, network administrators are encouraged to
disable SNMPv2 before using the MIB.
```

Figure 37. Examples of Message Prefixes

To determine if message labeling is enabled, enter the **show session** command.

```
Switch(config)# show session
Show Message Type: Enabled
CLI Interactive Mode: Enabled
```

Figure 38. Example Showing the label cli-return-message Command is Enabled

CLI Interactive Commands

When the CLI interactive command mode is enabled, you must explicitly enter the choice of yes (y) or no (n) for interactive commands. When interactive command mode is disabled, the default choice for all command is **yes**, except as noted below. The CLI interactive mode command enables or disables interactive mode for the CLI session.

Syntax: session interactive-mode [enable | disable]

Enables or disables interactive mode for the CLI session.

*The **disable** option disables interactive mode. The default choice for yes/no interactive commands will be **yes** except for commands when there is a prompt to save the config. The default for that is **no**.*

*The default choice for rebooting the switch is **yes**.*

Note: *This setting is not saved when the switch is rebooted.*

Default: Enabled on all sessions.

```
Switch(config)# no password all
Password protection for all will be deleted, continue [y/n]? y
Default choice is yes.

Switch(config)# boot system flash secondary
System will be rebooted from secondary image. Do you want to continue [y/n]? y
Do you want to save current configuration [y/n]? n
Default choice for reboot is yes. Default choice for saving the current configuration is no.
```

Figure 39. Example of CLI Interactive Mode When Disabled

To determine if the CLI interactive mode is enabled or disabled, enter the **show session** command.

```
Switch(config)# show session
Show Message Type: Enabled
CLI Interactive Mode: Enabled
```

Figure 40. Example Showing CLI Interactive Mode is Enabled

Interactive Commands Requiring Additional Options

Interactive commands that require input other than yes or no are not affected when CLI interactive mode is disabled. A warning message is displayed when these commands are executed, for example:

Interactive mode is disabled; This command will be ignored. Enable cli-interactive-mode to use this command.

The following commands will issue this warning when interactive mode is disabled. An alternate way to enter the command (when one is available) is shown.

Command	Non-Interactive Alternate Command
setup mgmt-interfaces	No equivalent non-interactive command
aaa port-access supplicant <port-list> secret	aaa port-access supplicant <port-list> secret <secret-string>
password manager	password manager plaintext <password-string>
password operator	password operator plaintext <password-string>

Command	Non-Interactive Alternate Command
aaa port-access supplicant <port-list> secret	aaa port-access supplicant <port-list> secret <secret-string>
crypto host-cert generate self-signed	crypto host-cert generate self-signed <start-date> <end-date> <CNAME-STR> <ORG-UNIT-STR> <ORGANIZATION-STR> <CITY-STR> <STATE-STR> <code>

Menu Commands

When CLI interactive mode is disabled, all CLI commands that launch the menu interface will not be affected by the interactive mode. A warning message is displayed, for example:

```
Switch(config)# menu

Interactive mode is disabled; This command will be ignored. Enable
cli-interactive-mode to use this command.
```

Other menu-based commands that will not be affected are:

- setup
- show interfaces display

SNMPv3 Special Cases

The following are special cases when using SNMPv3 with interactive mode.

- **snmpv3 user:** In interactive mode, the command **snmpv3 user** will create snmpv3 users, even if snmpv3 has not been enabled.
- **snmpv3 enable:** When interactive mode is disabled, this command only enables snmpv3. It does not prompt for an authentication password. When the command is first executed, a default initial user is created. A message displays:
User 'initial' has been created.

Banner MOTD Command with Non-Interactive Mode

The use of escape characters allows the **banner motd** command to be used in non-interactive mode for multiple message lines. In non-interactive mode, you can create a banner message enclosed in double quotes or other delimiter that uses escape characters within the delimiters. Other existing CLI commands do not support the escape characters.

The following escape characters are supported:

\"	double q
\'	single quote
\`	forward quote
\\	backslash
\f	form feed
\n	newline
\r	carriage return
\t	horizontal tab
\v	vertical tab

```
Switch(config)# banner motd "You can use the \'banner motd\' CLI command in non-interactive mode.\n\n\tThe banner motd command will support escape characters."

Switch(config)# show banner motd

Banner Information

Banner status: Enabled

Configured Banner:

You can use the \'banner motd\' CLI command in non-interactive mode.

    The banner motd command will support escape characters."
```

Figure 41. Example of Configuring the Banner Message Using Escape Characters Within Double Quote Delimiters

The running configuration file contains the banner message as entered in the command line.

```
Switch(config)# show running-config

Running configuration:

;J8693A Configuration Editor; Created on release #K.14.00x

hostname "Switch"
vlan 1
    name "DEFAULT_VLAN"
    untagged 1-48, a1-a4
    ip address dhcp-bootp
    exit
banner motd "You can use the \'banner motd\' CLI command in non-interactive mode.\n\n\tThe banner motd command will support escape characters."
```

Figure 42. Example of the Running Config File with Banner MOTD Configured in Non-interactive Mode

You can use a delimiting character other than quotes as well, as shown in [Figure 43](#).

```
Switch(config)# banner motd #
Enter TEXT message. End with the character '#'
You can use the \'banner motd\' CLI command in non-interactive mode.\n\n\tThe banner motd command will support escape characters. #
```

Figure 43. Example of Configuring the Banner Message Using an Alternate Delimiter of '#'

- **Enhancement (PR_0000055430)** — Adds support for Energy Efficient Ethernet (IEEE 802.3az).

Energy Efficient Ethernet (EEE)

Energy Efficient Ethernet (EEE) follows the 802.3az standard, which provides support for a system to operate in low power idle mode during low link utilization. This allows both sides of a link to disable or turn off a portion of the system's transmit/receive circuitry, saving power. When traffic is ready for transmission, the interface sends a "wake-up" message to the link partner to prepare to receive the traffic. The circuitry is returned to "normal" mode. Both sides of the link must be EEE-capable to support the power-saving idle mode.

To enable EEE on a port or range of ports, enter this command.

Syntax: [no] int <port-list> energy-efficient-ethernet

Enables EEE for a given port or range of ports.

*The **no** form of the command disables EEE for a port or range of ports.*

Default: Enabled

```
Switch(config)# int B5-B7 energy-efficient-ethernet
Switch(config)# show energy-efficient-ethernet
```

Port	EEE Config	Current Status	txWake (µS)
B1	Enabled	Active	30
B2	Enabled	Inactive	-
B3	Disabled	Inactive	-
B4	Enabled	Unsupported	-
B5	Enabled	Active	30
B6	Enabled	Active	30
B7	Enabled	Inactive	-

Figure 44. Example of EEE Enabled on Ports B5 - B7

The parameters are explained in the following table.

Parameter	Description
EEE Config	The EEE configuration status, read from the configuration database.
– Enabled	EEE mode is enabled.
– Disabled	EEE mode is disabled.
Current Status	Current EEE operational status.
– Active	The port is advertised and auto-negotiated EEE with link partner (an EEE-capable partner). EEE mode is enabled.
– Inactive	Set to one of the following conditions: <ul style="list-style-type: none"> – EEE configuration is disabled on the local port. – Local port advertises EEE capabilities with “EEE disabled” link partner or non-EEE link partner. – Auto-negotiation is mandatory for EEE to work. EEE configuration will not be applied if the port is in Forced/Manual (speed-duplex) mode. The current status will be “inactive” for Forced/Manual mode port configuration. – EEE is not supported for 10Base-T. The current status will be ‘inactive’ if the link is operating in 10Base-T mode.
– Unsupported	The local physical interface does not have EEE capability.
txWake	Current value of Transmit wake-up time (in microseconds).

Note The interface modules do not support adjustment of both Transmit and Receive wake-up times. Therefore, txWake is constant.

LLDP Support for EEE

Layer 2 (Data Link Layer) EEE capability is a feature that allows fine-tuning for EEE that uses LLDP TLVs for the negotiation of physical link partners' wake up time values. An EEE-capable port notifies its link partner about the EEE capabilities supported. The ports then negotiate how to best optimize energy efficiency.

To enable Layer 2 EEE and the advertisement of the EEE TLV, enter this command.

Syntax: [no] lldp config <port-list> dot3TlvEnable eee_config

Enables the advertisement of Layer 2 EEE TLVs for a given port or range of ports.

*The **no** form of the command disables the advertisement of EEE TLVs.*

Default: Enabled

```
Switch(config)# lldp config B5 dot3TlvEnable eee_config

Switch(config)# show lldp config B5

LLDP Port Configuration Detail

  Port : B5
  Adminstatus [Tx_Rx] : Tx_Rx
  NotificationEnabled [False] : False
  Med Topology Trap Enabled [False] : False

  TLVs Advertised:
    *port_descr
    *system_name
    *system_descr
    *system_cap

    *capabilities
    *network_policy
    *location_id
    *poe

    *macphy_config
    *poe_config
    *eee_config
```

Figure 45. Example of Configuring Layer 2 TLVs on a Port

To display the EEE TLV information for the local port, enter the **show lldp info local-device <port-list>** command.

```
Switch(config)# show lldp info local-device B5

LLDP Local Port Information Detail

  Port      : B5
  PortType  : local
  PortID    : 5
  PortDesc  : B5
  Pvid      : 1

Energy Efficient Ethernet (EEE) Wake Times (microseconds)

  Transmit      : 10
  Receive       : 10
  Echo Transmit : 10
  Echo Receive  : 10
  Fallback Receive : 10
```

Figure 46. Example of Output for LLDP Information for a Local Port

To display the EEE TLV information for the link partner, enter the **show lldp info remote-device <port-list>** command.

```
Switch(config)# show lldp info remote-device B6

LLDP Remote Device Information Detail

  Local Port   : B6
  ChassisType  : mac-address
  ChassisID    : 00 15 23 ff 2d 49
  PortType     : Local
  PortID       : 3
  SysName      : HP Switch
  System Desc  : Switch
  PortDesc     : 3
  Pvid         : 22
  .
  .
  .
Energy Efficient Ethernet (EEE) Wake Times (microseconds)

  Transmit      : 10
  Receive       : 10
  Echo Transmit : 10
  Echo Receive  : 10
  Fallback Receive : 10
```

Figure 47. Example of Output for LLDP Information for a Remote Port

- **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

Version K.15.03.0003 Enhancements

Version K.15.03.0003 includes the following enhancements.

- **Enhancement (PR_0000045685)** — Allows creation of a custom default configuration for the switch.

Custom Default Configuration

The custom default configuration feature provides the ability to initialize a switch to a different state from the factory default state when you delete the active configuration file. The factory default configuration is not changed. If a custom configuration file has been created and the active configuration file is deleted, the switch will boot up using the custom configuration file.

The feature provides the ability to:

- Use a customized configuration file as a default configuration file
- Enable the switch to start up with the specified default configuration

The existence of a custom default configuration file does not affect the results of loading a remotely stored configuration file onto the switch.

Using a custom default configuration, you can configure the features you want to be in the default configuration. When the active configuration is deleted using the **erase startup** command, the active configuration is removed and the custom default configuration file will be used upon bootup. The standard default configuration file remains and is used if there is no custom default configuration.

Note

This feature does *not* change the system defaults. The custom default configuration file is automatically used when the startup configuration file is erased. It has no effect on what is loaded onto the switch when a remotely stored configuration file is restored.

Creating the Custom Default Configuration File

The default configuration file can be customized using commands at the CLI prompt or by copying a configuration file with the desired configuration using TFTP, USB, or XMODEM copy commands. The existing default configuration file also can be transferred from the switch using these commands.

To start creating the configuration file to be used as the custom default configuration file, enter the commands that configure the features desired and then save the configuration file using the **write memory** command. An example is shown in [Figure 48](#).


```
Switch(config)# spanning-tree
Switch(config)# interface 4 flow-control

Switch(config)# write memory
```

Figure 48. Example of Creating a Config File with the Desired Features

This configuration, which enables flow control on interface 4, and also spanning-tree on the switch, is stored in the startup configuration file.

To save this configuration as the custom default configuration, the startup configuration file is copied to the default configuration file, as shown in [Figure 49](#).

```
Switch(config)# copy startup-config default-config
```

Figure 49. Example of Copying the Startup Configuration File to the Custom Default Configuration File

Copying an Existing Configuration File to the Custom Default Configuration File

The switch can have up to 3 different configuration files stored in flash memory. (For more information about multiple configuration files, see “Multiple Configuration Files” in the *Management and Configuration Guide* for your switch.) To copy a configuration file that exists in flash memory to the custom default configuration file, use this command.

Syntax: copy config < source-filename > default-config

Copies the configuration file specified in <source-filename> to the custom default configuration file.

```
Switch(config)# copy abc.cfg default-config
```

Figure 50. Copying the abc.cfg Config File to the Custom Default Config File

Copying the Custom Default Config File onto the Switch

Using TFTP

To copy a configuration file stored on a TFTP server to the custom default configuration file, use the **copy tftp default-config** command.

Syntax: copy tftp default-config <ip-addr> <stored config file name>

Copies the stored configuration file on the TFTP server specified by <ip-addr> to the custom default configuration file.

```
Switch(config)# copy tftp default-config 10.10.10.1 stored_config.cfg
```

Figure 51. Copying a Stored Config File to the Default Config File Using TFTP

Using XMODEM

To copy a configuration file to the custom default configuration file using XMODEM, use the **copy xmodem default-config** command.

Syntax: copy xmodem default-config

Copies the configuration file specified by the XMODEM server device to the custom default configuration file.

```
Switch(config)# copy xmodem default-config
```

Figure 52. Copying a Stored Config File to the Custom Default Config File Using XMODEM

Using USB

To copy a configuration file to the custom default configuration file using USB, use the **copy usb default-config** command.

Syntax: copy usb default-config <stored config file name>

Copies the stored configuration file on the USB stick to the custom default configuration file.

```
Switch# copy usb default-config stored_config.cfg
```

Figure 53. Copying a Stored Config File to the Custom Default Config File Using USB

Copying the Custom Default Config File Off the Switch

Using TFTP

To transfer a custom default configuration file off the switch using TFTP, enter the following command.

Syntax: copy default-config tftp <server ip-address> stored_config.cfg

Copies the custom default configuration file to the stored_config.cfg file on the TFTP server.

Using XMODEM

To transfer a custom default config file off the switch using XMODEM, enter the following command.

Syntax: copy default-config xmodem

Copies the custom default configuration file to the configuration file specified by the XMODEM server device.

Using USB

To transfer a custom default configuration file off the switch using USB, enter the following command.

Syntax: copy default-config usb stored_config.cfg

Copies the custom default configuration file to the stored_config.cfg file on the USB device.

Using SFTP and SCP to Transfer the Custom Configuration

While the switch supports an SSH server with SCP and/or SFTP running on it, the switch is not an SCP or SFTP client. To transfer the default custom configuration file to or from the switch, you must connect to the switch's SSH server using any SCP or SFTP client. Instead of the actual name of the custom default configuration file, an alias name of "default-config" is displayed in the file listings and for get/store functions.

When you use an SCP client to connect to the switch, you must know the name of the file you wish to get or store. When you use SFTP client to connect to the switch, you are provided with a list of filenames that can be accessed by the switch.

Note You must have an SCP/SFTP client implemented in order to execute **copy scp** or **copy sftp** commands on the switch.

The following example shows the output from running **puTTY psftp** on a remote PC.

```
C:\PuTTY> psftp 10.1.243.209

We'd like to keep you up to date about:
* Software feature updates
* New product announcements
* Special events

Please register your products now at: www.ProCurve.com

Remote working directory is /
psftp> ls
Listing directory /
drwxr-xr-x  2 J9145A  J9145A          0 Jan 01 00:01 cfg
drwxr-xr-x  2 J9145A  J9145A          0 Jan 01 00:01 core
drwxr-xr-x  2 J9145A  J9145A          0 Jan 01 00:01 log
drwxrwxrwx  2 J9145A  J9145A          0 Jan 01 00:01 os
drwxrwxrwx  3 J9145A  J9145A          0 Jan 01 00:01 ssh

psftp> ls /cfg
Listing directory /cfg
-rwxrw-r--  1 J9145A  J9145A        1749 Jan 01 00:01 default-config
-rw-r--r--  1 J9145A  J9145A         745 Jan 01 01:19 running-config
-rwxrw-r--  1 J9145A  J9145A         360 Jan 01 01:19 startup-config

psftp>
```

This is the custom default config.




Figure 54. Example of Using SFTP

Erasing a Configuration File

If a custom default configuration file exists and the **erase startup-config** command is executed, the current active configuration is erased and the switch is booted with the custom default configuration.

```
Switch(config)# erase startup-config
Configuration will be deleted, and existing login passwords removed, and device
rebooted (using the custom default configuration), continue [y/n]?
```

Figure 55. Example of Erasing the Startup Config File When a Default Custom Config File Exists

If a custom default configuration file does not exist and the erase startup-config command is executed, the current active configuration is erased and the switch is booted with the system default configuration.

```
Switch(config)# erase startup-config
Configuration will be deleted, and existing login passwords removed, and device
rebooted, continue [y/n]?
```

Figure 56. Example of Erasing the Startup Config File When a Default Custom Config File Does Not Exist

To erase the custom default configuration file, execute the **erase default-config** command.

```
Switch(config)# erase default-config
The custom default configuration will be erased. The "erase startup-config"
command will now use system generated default configuration. Continue [y/n]?
```

Figure 57. Example of Erasing the Custom Default Config File

Displaying the Configuration Files

The **show config files** command displays the existing configuration files and indicates that a custom default configuration file exists.

```
Switch(config)# show config files

Configuration files:

id | act pri sec | name
---+-----+-----
 1  *   *       | config
 2              | secondaryconfig
 3              | Kconfig

=====
A Custom default configuration file exists.
```

A custom default configuration file exists.

Figure 58. Example Output Displaying 3 Configuration Files

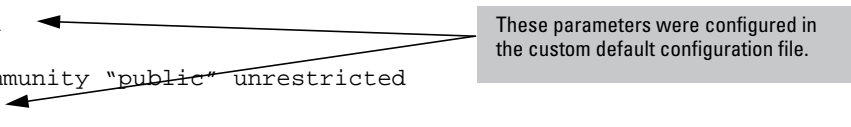
Enter the command **show default-config** to display the custom default configuration.

```
Switch(config)# show default-config

Custom default configuration:

; J8693A Configuration Editor; Created on release #K.15.XX

hostname "Switch"
module 1 type J86xxA
module 2 type J86xxA
vlan 1
    name "DEFAULT-VLAN"
    untagged 1-24
    ip address dhcp-bootp
    exit
interface 4
    flow-control
    exit
snmp-server community "public" unrestricted
spanning-tree
```



These parameters were configured in the custom default configuration file.

Figure 59. Example of Output for Custom Default Configuration File

If a custom default configuration file exists and you erase the current active config file (using the **erase startup-config** command), then issue the **show running-config** command, the output will display the contents of the custom default configuration file. The custom default configuration file is loaded upon bootup. See [Figure 60](#).

```
Switch(config)# show running-config

Custom default configuration:

; J8693A Configuration Editor; Created on release #K.15.XX

hostname "Switch"
module 1 type J86xxA
module 2 type J86xxA
vlan 1
    name "DEFAULT-VLAN"
    untagged 1-24
    ip address dhcp-bootp
    exit
interface 4
    flow-control
    exit
snmp-server community "public" unrestricted
spanning-tree
```

Figure 60. Example of Output of Custom Default Config File When Current Active Config File Erased

Troubleshooting Custom Default Configuration Files

- If the switch won't boot because of a problem with the custom default configuration file, the file can be removed using the ROM mode interface.
- The custom default configuration file cannot be erased using the front panel buttons on the switch. If the switch can be booted, use the **erase default-config** command to remove the custom default configuration file.
- **Enhancement (PR_0000045796)** — Adds the ability to enable SNMP traps when MAC addresses are added to or deleted from a port.

SNMP Trap Upon Port Addition or Deletion of MAC Addresses

When enabled, this feature allows the generation of SNMP traps for each MAC address table change. Notifications can be generated for each device that connects to a port and for devices that are connected through another device (daisy-chained).

Configuring SNMP Trap Generation

The **snmp-server enable traps mac-notify** command globally enables the generation of SNMP trap notifications.

Syntax: [no] snmp-server enable traps mac-notify [mac-move | trap-interval <0-120>]

Globally enables or disables generation of SNMP trap notifications.

trap-interval: *The time interval (in seconds) that trap notifications are sent. A value of zero disables the interval and traps are sent as events occur. If the switch is busy, notifications can be sent prior to the configured interval. Notifications may be dropped in extreme instances and a system warning is logged.*

The range is 0-120 seconds. Default: 30 seconds.

mac-move: *Configures the switch to capture data for MAC addresses that are moved from one port to another port. The **snmp-server enable traps mac-notify** command must have been enabled in order for this information to be sent as an SNMP notification.*

```
Switch(config)# snmp-server enable traps mac-notify trap-interval 60
```

Figure 61. Example of trap-interval Option

```
Switch(config)# snmp-server enable traps mac-notify mac-move
```

Figure 62. Example of mac-move Option

Additional mac-notify Options

Use the following command to configure SNMP traps for learned or removed MAC addresses on a per-port basis.

Note	The switch will capture learned or removed events on the selected ports, but will not send an SNMP trap unless mac-notify has been enabled with the snmp-server enable traps mac-notify command.
-------------	---

Syntax: [no] mac-notify traps <port-list> [learned | removed]

*When this command is executed without the **learned** or **removed** option, it enables or disables the capture of both learned and removed MAC address table changes for the selected ports in <port-list>.*

<port-list>: *Configures MAC address table changes capture on the specified ports. Use **all** to capture changes for all ports on the switch.*

learned: *Enables the capture of learned MAC address table changes on the selected ports.*

removed: *Enables the capture of removed MAC address table changes table on the selected ports.*

```
Switch(config)# mac-notify traps 5-6 learned
Switch(config)# show mac-notify traps 5-6

Mac Notify Trap Information

Mac-notify Enabled : Yes
Mac-move Enabled : Yes
Trap-interval : 60

Port    MAC Addresses trap learned/removed
-----
5       Learned
6       Learned
```

Figure 63. Example of Configuring Traps on a Per-Port Basis for Learned MAC Addresses

```
Switch(config)# mac-notify traps 3-4 removed
Switch(config)# show mac-notify traps

Mac Notify Trap Information

Mac-notify Enabled : Yes
Mac-move Enabled : Yes
Trap-interval : 60

Port    MAC Addresses trap learned/removed
-----
1       None
2       None
3       Removed
4       Removed
```

Figure 64. Example of Configuring Traps on a Per-Port Basis for Removed MAC Addresses

Interface Context Level Configuration

You can also execute the **mac-notify traps** command from the interface context.

```
Switch(config)# int 11
Switch(int-11)# mac-notify traps learned
```

Figure 65. Example of the Interface Context for mac-notify traps Command

Displaying the MAC Notify Traps Configuration Information

Use the **show mac-notify traps** command to display information about SNMP trap configuration.

Syntax: show mac-notify traps [port-list]

Displays SNMP trap information for all ports, or each port in the port-list.

```
Switch(config)# show mac-notify traps

Mac Notify Trap Information

Mac-notify Enabled : Yes
Mac-move Enabled : Yes
Trap-interval : 60

Port    MAC Addresses trap learned/removed
-----
1        None
2        None
3        Removed
4        Removed
5        Learned
6        Learned
```

Figure 66. Example of Information for SNMP Trap Configuration

The configured **mac-notify** commands display in the **show running-configuration** output.

```
Switch(config)# show running-config

Running configuration:

; J9087A Configuration Editor; Created on release #R.11.XX

hostname "Switch"
snmp-server community "public" Unrestricted
snmp-server host 15.255.133.236 "public"
snmp-server host 15.255.133.222 "public"
snmp-server host 15.255.133.70 "public"
snmp-server host 15.255.134.235 "public"
vlan 1
  name "DEFAULT_VLAN"
  untagged 1-28
  ip address dhcp-bootp
  exit
snmp-server enable traps mac-notify mac-move
snmp-server enable traps mac-notify trap-interval 60
snmp-server enable traps mac-notify
mac-notify traps 5-6 learned
mac-notify traps 3-4 removed
```

The mac-notify commands that were configured.

Figure 67. Example of Running Config File With mac-notify Parameters Configured

- **Enhancement (PR_0000052266)** — Adds the ability to enable an SNMP trap when the switch's startup configuration is changed.

Log Message When Startup Config Updated

This enhancement enables notification to a management station when changes to the startup configuration file occur and are written to flash. Changes to the configuration file can occur when executing a CLI **write** command, executing an SNMP **set** command directly using SNMP, or when using the WebAgent.

A log message is always generated when a change occurs. An example log entry is:

I 07/06/10 18:21:39 02617 mgr: Startup configuration changed by SNMP. New seq. number 8

The corresponding trap message is sent if the **snmp-server enable traps startup-config-change** command is configured.

Syntax: [no] snmp-server enable traps startup-config-change

Enables notification of a change to the startup configuration. The change event is logged.

Default: Disabled

An example of configuring the command with the CLI is shown in [Figure 68](#). The number that displays when **show config** is executed is global for the switch and represents the startup configuration sequence number.

```
Switch(config)# snmp-server enable traps startup-config-change
Switch(config)# show config
Startup configuration: 16
; J8697A Configuration Editor; Created on release #K.14.54
hostname "Switch"
module 1 type J8702A
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A24, B1-B10
  ip address dhcp-bootp
  exit
snmp-server community "public" unrestricted
```

The number "16" is global for the switch and represents the startup configuration sequence number.

Figure 68. Example of Enabling Notification of Changes to the Startup Config File

[Figure 69](#) displays an example of the fields in the trap when a change is made via SNMP (station ip=0xAC161251 (172.22.18.81), no username is set, and the new sequence number is 16).

```
Internet Protocol, Src: 172.22.18.57 (172.22.18.57), Dst: 172.22.18.81 (172.22.18.81)
User Datagram Protocol, Src Port: snmp (161), Dst Port: snmptrap (162)
Simple Network Management Protocol
  version: version-1 (0)
  community: public
  data: trap (4)
    trap
      enterprise: 1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1 (SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1)
      agent-addr: 172.22.18.57 (172.22.18.57)
      generic-trap: enterpriseSpecific (6)
      specific-trap: 6
      time-stamp: 65437
      variable-bindings: 6 items
        SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.9 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.9): 16
        SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.1 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.1): 2
        SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.2 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.2): 4
        SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.3 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.3): AC161251
        SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.4 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.4): «MISSING»
        SNMPv2-SMI::enterprises.11.2.14.11.5.1.7.1.29.1.0.5 (1.3.6.1.4.1.11.2.14.11.5.1.7.1.29.1.0.5): 1
```

Figure 69. Example of the Fields When the SNMP Trap is Set

- **Enhancement (PR_0000052738)** — Adds VLAN information to the output of the **show mac-address** commands.

Show MAC with VLAN

This feature displays the VLAN ID with each MAC address for the **show mac-address <option>** command.

```
Switch(config)# show mac-address 4-6

Status and Counters - Port Address Table - 4

MAC Address    VLAN
-----
001186-f47ff4 2

Status and Counters - Port Address Table - 5

MAC Address    VLAN
-----
001279-7fbaf4 4

Status and Counters - Port Address Table - 6

MAC Address    VLAN
-----
001321-1763ca 4
```

Figure 70. Example of Output for show mac-address <port-list> Command

```
Switch(config)# show mac-address 001635-36de76

Status and Counters - Address Table - 001635-36de76

Port  VLAN
----  ----
7     5
```

Figure 71. Example of Output for show mac-address <mac-address> Command

```
Switch(config)# show mac-address vlan 5

Status and Counters - Address Table - VLAN 5

MAC Address    Port
-----
001635-36de76 7
```

Figure 72. Example of Output for show mac-address vlan <vid> Command

```
Switch(config)# show mac-address

Status and Counters - Port Address Table

MAC Address      Port  VLAN
-----
001635-36de76 7    1
00934f-894rd2 5    1
098745-de4928 6    1
```

Figure 73. Example of Output showing Ports and VLAN IDs for all MAC Addresses

- **Enhancement (PR_0000054042)** — Adds the ability to monitor egress queues for dropped packets when QoS is configured.

Outbound Queue Monitor

When QoS is used to prioritize traffic, different kinds of traffic can be assigned to different egress queues. If there is a great deal of traffic, some of the traffic to the lower priority queues may be dropped. This feature allows the egress queues for a port to be monitored for dropped packets.

Syntax: [no] qos watch-queue <port> out

Configures the switch to start monitoring the specified port for the dropped packets for each queue. Disabling and then re-enabling monitoring on a port clears the per-queue dropped packet counters.

*The **no** form of the command stops the collection of dropped traffic information.*

Default: Disabled

- **Enhancement (PR_0000054055)** — This enhancement provides the ability to display OSPF neighbor timer information.

Show OSPF Neighbor Timers

This enhancement provides the ability to display the OSPF neighbor timer information by adding the **detail** option to the **show ip ospf neighbor** command.

Syntax: show ip ospf neighbor [detail [router-id]]

The detail option displays the OSPF neighbor timer information. You can optionally enter the router-id of the neighbor for which detail information is wanted.

There are two new counters that display neighbor timer information:

- **Dead-timer Expires (HH:MM:SS):** The time remaining for an active adjacency to expire if there are no more hello packets received.
- **Neighbor Uptime (HH:MM:SS):** The amount of time an adjacency is active.

If a neighbor loses adjacency and then re-establishes it, the Neighbor Uptime counter is set to zero. The Dead-timer Expires counter is set to the dead interval for the interface.

If a graceful restart of the neighbor occurs, the Neighbor Uptime counter continues to increment as the adjacency is considered active while the neighbor is restarting. The Dead-timer Expires counter is set to the hold timer for the neighbor. When the restart completes, the counter is set to the dead interval for the interface.

```
Switch(config)# show ip ospf neighbor detail

OSPF Neighbor Information for neighbor 10.10.10.2

IP Address: 10.10.10.2
Router ID : 10.10.10.2      State                : FULL
Interface : vlan-10        Designated Router   : 10.10.10.3
Area      : backbone       Backup Designated Router : 10.10.10.2
Priority   : 1              Retransmit Queue Length : 0
Options   : 0              Neighbor Uptime      : 0h:0m:32s
Events    : 6              Dead Timer Expires    : 32 sec
```

Figure 74. Example of Displaying OSPF Neighbor Timers

- **Enhancement (PR_0000054183)** — The user can now disable the IP addresses on specified VLANs, without deleting the configured IP addresses.

IP Enable/Disable for All VLANs

This enhancement allows you to administratively disable the IP address on specified VLANs with static IP addresses without removing the Layer 3 configuration. The switch can be pre-configured as a backup router, then quickly transition from backup to active by re-enabling Layer 3 routing on one or more VLANs. While the switch is in “backup” mode, it will still performing Layer 2 switching.

A MIB object will be toggled to make Layer 3 routing active or inactive on a VLAN.

Interaction with Other Features

The feature affects management access to the switch as follows:

- IP—SNMP, Telnet, SSH, HTTP, TFTP, SCP, SFTP
- Routing—RIP, OSPF, PIM, VRRP

When the **disable layer3** command is configured on a VLAN, the behavior is as if no IP address were configured for that VLAN. There is no other change in behavior.

Syntax: [no] disable layer3 vlan <vid | range of vids>

In config context, turns off Layer 3 routing for the specified VLAN or VLANs. When executed in vlan context, turns off Layer 3 routing for that VLAN.

*The **no** form turns on Layer 3 routing for the specified VLAN or VLANs.*

*If QinQ is enabled, **svlan** can be configured as well.*

The **show ip** command displays “disabled” in the IP Config column if Layer 3 has been disabled, or if the VLAN has no IP configuration. You can tell which is the case by viewing the remaining columns; if there is no IP configuration, the remaining columns are blank.

```
Switch(config)# show ip

Internet (IP) Service

  IP Routing : Disabled

Default Gateway : 172.22.16.1
Default TTL     : 64
Arp Age         : 20
Domain Suffix   :
DNS server      :

VLAN            | IP Config | IP Address   | Subnet Mask   | Proxy ARP
-----+-----+-----+-----+-----+
DEFAULT_VLAN    | DHCP/Bootp | 172.22.18.100 | 255.255.248.0 | No No
VLAN3           | Disabled   | 172.17.17.17  | 255.255.255.0 | No No
VLAN6           | Disabled   |                |                | 
VLAN7           | Manual     | 10.7.7.1      | 255.255.255.0 | No No
```

Figure 75. Example of VLAN Disabled for Layer 3

For IPv6, the “Layer 3 Status” field displays the status of Layer 3 on that VLAN.

```
Switch(config)# show ipv6

Internet (IPv6) Service

  IPv6 Routing : Disabled
Default Gateway :
ND DAD         : Enabled
DAD Attempts   : 3

Vlan Name      : DEFAULT_VLAN
IPv6 Status    : Disabled
Layer 3 Status : Enabled

Vlan Name      : layer3_off_vlan
IPv6 Status    : Disabled
Layer 3 Status : Disabled

Address      | Address
Origin       | IPv6 Address/Prefix Length | Status
-----+-----+-----+
manual       | abcd::1234/32               | tentative
autoconfig   | fe80::218:71ff:febd:ee00/64 | tentative
```

Figure 76. Example of IPv6 Layer 3 Status for a VLAN

Interactions with DHCP

Disabling Layer 3 functionality and DHCP are mutually exclusive, with DHCP taking precedence over **disable layer3** on a VLAN. The following interactions occur:

- If the **disable layer3** command is executed when DHCP is already configured, no disabling of the VLAN occurs. This error message displays —“Layer 3 cannot be disabled on a VLAN that has DHCP enabled.”
- From the CLI: If **disable layer3** is configured already, and an attempt is made to configure DHCP, DHCP takes precedence and will be set. The warning message displays— “Layer 3 has also been enabled on this VLAN since it is required for DHCP.”

- From the CLI: When disabling a range of VLAN IDs, this warning message displays—“Layer 3 will not be disabled for any LANs that have DHCP enabled.”
- From SNMP: If the disable layer3 command is executed when DHCP is already configured, no disabling of the VLAN occurs. An INCONSISTENT_VALUE error is returned.
- From SNMP: If disable layer3 is configured already, and an attempt is made to configure DHCP, DHCP takes precedence and will be set.

■ **Enhancement (PR_0000055367)** — Adds the ability to log ACL **permit** entries.

Logging for Routing ACLs

This feature will provide functionality for logging ACL “permit” entries in the same manner that ACL “deny” entries are currently logged.

Operating Notes

- Affects only ACLs that are statically configured using the CLI command interface.
- Existing ACL logging for “deny” entries does not change
- A detailed event will be logged for the first packet that matches a “permit” or “deny” ACL logged entry with the appropriate action specified.
- Subsequent packets matching ACL logged entries will generate a new event that summarizes the number of packets that matched each specific entry (with the time period), for example:

```
Mar 1 10:01:01 10.10.20.1 ACL:
ACL 03/01/10 10:01:01: ACL NO-TELNET seq#10 permitted 6 packets
```

- Events are logged as specified by the **debug <destination>** command.
- Events are only logged when ACL logging is enabled using the **debug acl** command. This feature should only be used to troubleshoot and verify ACL configurations as it can impact switch performance even when ACL debugging is disabled.

Standard ACLs

The following abbreviated syntax is for standard, named ACLs. See the chapter “IPv4 Access Control Lists (ACLs)” in the *Access Security Guide* for your switch for more information on ACLs and ACL syntax.

Syntax: ip access-list standard < name-str >

Places the CLI in the “Named ACL” (nacl) context specified by the < name-str > alphanumeric identifier. This enables entry of individual ACEs in the specified ACL. If the ACL does not already exist, this command creates it.

< name-str >: *Specifies an identifier for the ACL. Consists of an alphanumeric string of up to 64 case-sensitive characters. Including spaces in the string requires that you enclose the string in single or double quotes. For example: “Accounting ACL”.*

< deny | permit >

< any | host < SA > | SA < mask | SA / mask-length > > [log]

Executing this command appends the ACE to the end of the list of ACEs in the current ACL. In the default ACL configuration, ACEs are automatically assigned consecutive sequence numbers in increments of 10 and can be renumbered using **resequence**.

SA=Source Address

Note: *To insert a new ACE between two existing ACEs, precede **deny** or **permit** with an appropriate sequence number.*

< deny | permit >

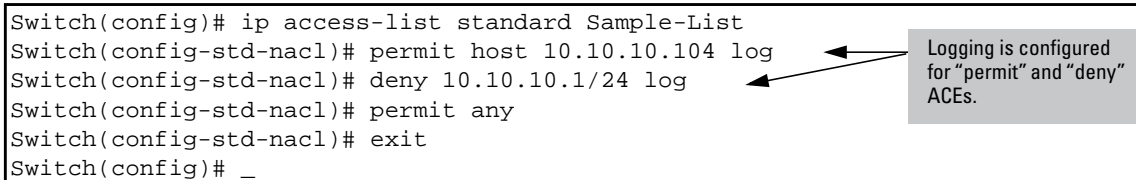
For named ACLs, used in the “Named ACL” (**nacl**) context to configure an ACE. Specifies whether the ACE denies or permits a packet matching the criteria in the ACE, as described below.

[log]

This option generates an ACL log message if:

- There is a match.
- ACL logging is enabled on the switch.

(Use the debug command to direct ACL logging output to the current console session and/or to a Syslog server. Note that you must also use the **logging < ip-addr >** command to specify the addresses of Syslog servers to which you want log messages sent.



```
Switch(config)# ip access-list standard Sample-List
Switch(config-std-nacl)# permit host 10.10.10.104 log
Switch(config-std-nacl)# deny 10.10.10.1/24 log
Switch(config-std-nacl)# permit any
Switch(config-std-nacl)# exit
Switch(config)# _
```

Figure 77. Example of Standard ACL showing the log Option configured for both “permit” and “deny” ACEs

Extended ACLs

The following abbreviated syntax is for extended, named ACLs. See the chapter “IPv4 Access Control Lists (ACLs)” in the *Access Security Guide* for your switch for more information on ACLs and ACL syntax.

Syntax: ip access-list extended < name-str >

Places the CLI in the “Named ACL” (**nacl**) context specified by the < name-str > alphanumeric identifier. This enables entry of individual ACEs in the specified ACL. If the ACL does not already exist, this command creates it.

< name-str >: Specifies an alphanumeric identifier for the ACL. Consists of an alphanumeric string of up to 64 case-sensitive characters. Including spaces in the string requires that you enclose the string in single or double quotes. For example: “**Accounting ACL**”. You can also use this command to access an existing, numbered ACL.

Syntax: < deny | permit > < ip | *ip-protocol* | *ip-protocol-nbr* >
(nacl < any | host < *SA* > | *SA/mask-length* | *SA* < *mask* > >
context) < any | host < *DA* > | *DA/mask-length* | *DA* < *mask* > >
[precedence] [tos] [log]

*Appends an ACE to the end of the list of ACEs in the current ACL. In the default configuration, ACEs are automatically assigned consecutive sequence numbers in increments of 10 and can be renumbered using **resequence**.*

SA=Source Address

DA=Destination Address

Note: *To insert a new ACE between two existing ACEs in an extended, named ACL, precede **deny** or **permit** with an appropriate sequence number along with the ACE keywords and variables you want.*

For a match to occur, a packet must have the source and destination addressing criteria specified in the ACE, as well as:

- the protocol-specific criteria configured in the ACE, including any included, optional elements (described later in this section)*
- any (optional) precedence and/or ToS settings configured in the ACE.*

< deny | permit >

*For named ACLs, these keywords are used in the “Named ACL” (**nacl**) context to specify whether the ACE denies or permits a packet matching the criteria in the ACE, as described below.*

[log]

This option can be used after the DA to generate an Event Log message if:

- There is a match.*
- ACL logging is enabled.*

```
Switch(config)# ip access-list extended Extended-List-01
Switch(config-ext-nacl)# permit tcp host 10.10.10.44 host
10.10.20.78 eq telnet
Switch(config-ext-nacl)# deny ip 10.10.10.1/24 10.10.20.1/24
Switch(config-ext-nacl)# permit ip 10.10.10.2/24 log
Switch(config-ext-nacl)# exit
Switch(config)# vlan 10 ip access-group Extended-List in
```

Logging is configured
for “permit” ACE.

Figure 78. Example of Standard ACL showing the log Option configured for a “permit” ACE

IPv6 Access Lists

The following abbreviated syntax is for IPv6, named ACLs. See the chapter “IPv6 Access Control Lists (ACLs)” in the *IPv6 Configuration Guide* for your switch for more details about IPv6 ACLs.

Syntax: `ipv6 access-list <ascii-str>`

*Places the CLI in the IPv6 ACL (**ipv6-acl**) context specified by the <ascii-str> alphanumeric identifier. This enables entry of individual ACEs in the specified ACL. If the ACL does not already exist, this command creates it.*

<ascii-str>: Specifies an alphanumeric identifier for the ACL. Consists of an alphanumeric string of up to 64 case-sensitive characters. Including spaces in the string requires that you enclose the string in single or double quotes. For example: “Accounting ACL”. You can also use this command to access an existing ACL.

Syntax: `<deny | permit> <ipv6 | ipv6-protocol | ipv6-protocol-nbr>
(ipv6 acl context) <any | host <SA> | SA/prefix-length>
<any | host <DA> | DA/prefix-length>
[dscp <tos-bits | precedence>] [log]`

*Appends an ACE to the end of the list of ACEs in the current ACL. In the default configuration, ACEs are automatically assigned consecutive sequence numbers in increments of 10 and can be renumbered using **resequence**.*

SA=Source Address

DA=Destination Address

Note: *To insert a new ACE between two existing ACEs in an ACL, precede **deny** or **permit** with an appropriate sequence number.*

For a match to occur, a packet must have the source and destination IPv6 addressing criteria specified in the ACE, as well as:

- the protocol-specific criteria configured in the ACE, including any optional elements (described later in this section)*
- any (optional) DSCP settings configured in the ACE*

`<deny | permit>`

*These keywords are used in the IPv6 (**ipv6-acl**) context to specify whether the ACE denies or permits a packet matching the criteria in the ACE, as described below.*

`[log]`

This option can be used after the DA to generate an Event Log message if:

- There is a match.*
- ACL logging is enabled.*

*For a given ACE, if **log** is used, it must be the last keyword entered.*

```
Port-1(config)# show access-list config

ipv6 access-list "Test-01"
 10 permit ipv6 2001:db8::1:10:10/128 ::/0 log
 20 deny tcp 2001:db8::1:20:0/121 2001:db8::1:10:3/128 eq 23 log
 30 deny ipv6 2001:db8::1:20:0/121 2001:db8::1:10:4/128 log
 40 deny tcp 2001:db8::1:30:0/121 2001:db8::1:10:4/128 eq 23 log
 50 deny ipv6 2001:db8::1:30:0/121 2001:db8::1:10:3/128
 60 deny icmp ::/0 ::/0 133
 70 permit ipv6 ::/0 ::/0
exit
```

Logging is configured for "permit" and "deny" ACEs.

Figure 79. Example of Standard ACL showing the log Option configured for "permit" and "deny" ACEs

- **Enhancement (PR_0000058115)** — Allows the use of TCP/UDP source and destination port number for trunk load balancing.

Trunk Load Balancing Using L4 Ports

This enhancement allows the use of TCP/UDP source and destination port number for trunk load balancing. This is in addition to the current use of source and destination IP address and MAC addresses. Configuration of Layer 4 load balancing would apply to all trunks on the switch. Only non-fragmented packets will have their TCP/UDP port number used by load balancing. This ensures that all frames associated with a fragmented IP packet are sent through the same trunk on the same physical link.

The priority for using Layer 4 packets when this feature is enabled is as follows:

1. If the packet protocol is an IP packet and has Layer 4 port information, use Layer 4.
2. If the packet protocol is an IP packet and does not have Layer 4 information, use Layer 3 information.
3. If the packet is not an IP packet, use Layer 2 information.

Enabling L4-based Trunk Load Balancing

Enter the following command with the **L4-based** option to enable load balancing on Layer 4 information when it is present.

Syntax: trunk-load-balance <L3-based | L4-based>

*When the **L4-based** option is configured, enables load balancing based on Layer 4 information if it is present. If it is not present, Layer 3 information is used if present; if Layer 3 information is not present, Layer 2 information is used. The configuration is executed in global configuration context and applies to the entire switch.*

Default: L3-based load balancing

<L3-based>: Load balance on Layer 3 information if present, or Layer 2 information.

<L4-based>: Load balance on Layer 4 port information if present, or Layer 3 if present, or Layer 2.

```
HPswitch(config)# trunk-load-balance L4-based
```

Figure 80. Example of Enabling L4-based Trunk Load Balancing

```
HPswitch(config)# show trunk

Load Balancing Method: L4-based, L2-based if non-IP traffic

  Port | Name | Type | Group | Type
  ---- + - - - - - - - - - - - - - - - - - - + - - - - -
  41    |      | 100/1000T | Trk1 | Trunk
  42    |      | 100/1000T | Trk1 | Trunk
```

Figure 81. Example of Output When L4-based Trunk Load Balancing is Enabled

```
HPswitch(config) # show running-config

Running configuration:

; J9091A Configuration Editor; Created on release #K.15.02.0001x

hostname "Switch"
module 1 type J8702A
module 5 type J9051A
module 7 type J8705A
module 10 type J8708A
module 12 type J8702A
trunk-load-balance L4-based
vlan 1
  name "DEFAULT_VLAN"
  untagged A1-A24,G1-G24,J1-J4,L1-L24
  ip address dhcp-bootp
  tagged EUP
  no untagged EDP
  exit
snmp-server community "public" unrestricted
```

If L4 trunk load balancing is enabled, a line appears in the running-config file. If it is not enabled, nothing appears as this is the default and the default values are not displayed.

Figure 82. Example of Running Config File when L4-based Trunk Load Balancing is Enabled

- **Enhancement (PR_0000058512)** — Adds Wake-on-LAN support across VLANs.

Wake-on-LAN Support Across VLANs

Wake-on-LAN is an Ethernet networking standard that allows a computer to be awakened by a network message, referred to as a “magic packet”. The packet is typically sent by a remote server to systems that are enabled to respond to these packets. This allows network administrators to troubleshoot or perform maintenance with minimal or no user intervention, even if the computers are turned off.

Wake-on-LAN commonly uses a broadcast address on UDP port 7 or port 9. The Layer 3 switches or routers must be configured to allow the broadcast packets, known as “directed broadcasts”. HP switches currently support directed broadcasts at the global switch level. This enhancement allows the configuration of directed broadcasts on a specific VLAN. An ACL can be configured to limit the Wake-on-LAN traffic to a specific subnet. This limits the servers that can send Wake-on-LAN packets, which helps prevent Denial-of-Service smurf attacks on the network.

The **ip directed-broadcast** command executed in VLAN context allows the configuration of Wake-on-LAN for a specific VLAN. Enabling directed broadcasts on an interface supersedes globally disabled directed broadcasts.

Syntax: [no] ip directed-broadcast

Enables or disables directed broadcast forwarding. Must be executed in VLAN context.

An example Wake-on-LAN configuration is shown in the following figure.

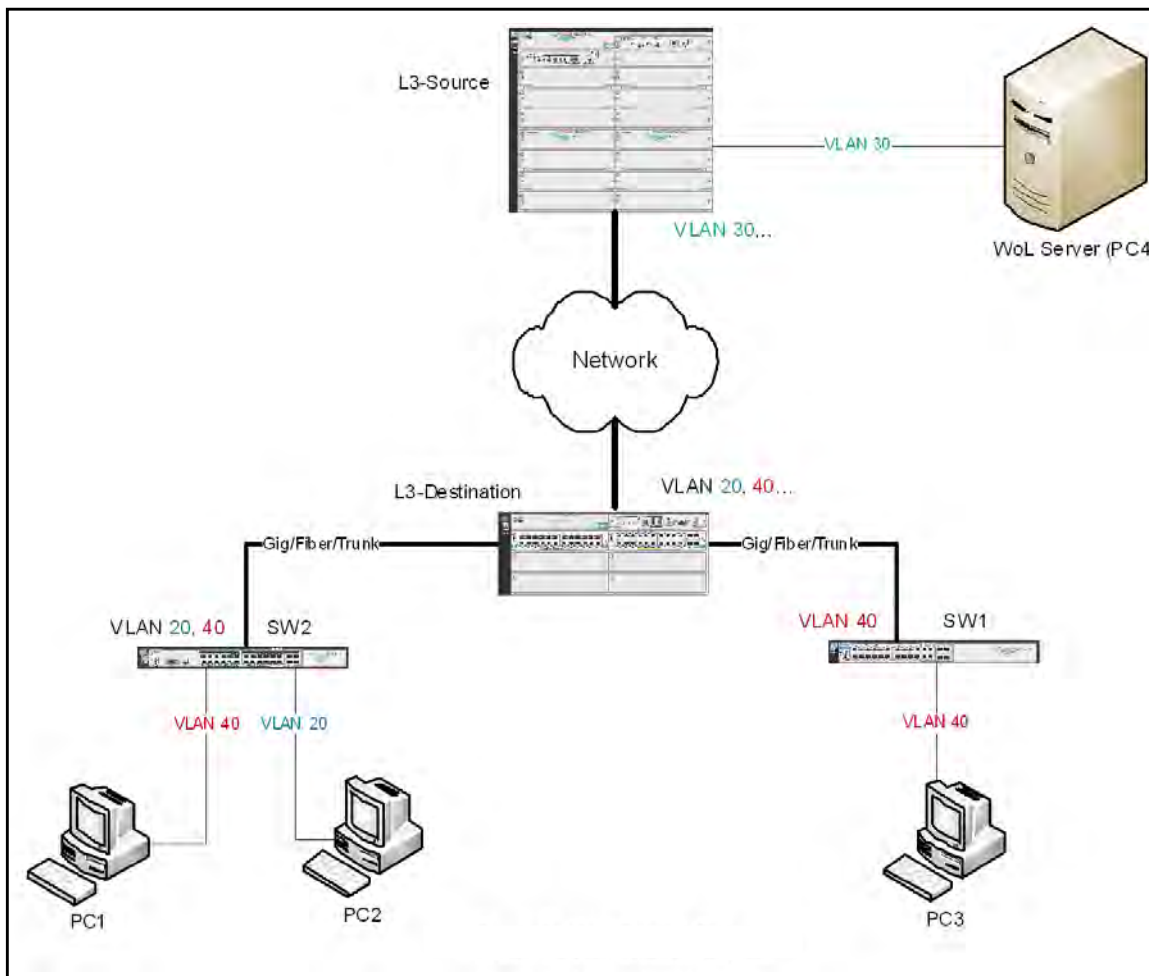


Figure 83. Example of Wake-on-LAN Configuration

In the example shown in [Figure 83](#):

- PC1, PC2 and PC3 are the client PCs that need to be awakened.
- PC4 is the Wake on LAN (WoL) server. This PC can also be the DHCP server with IP scopes for each of the VLANs (20, 30, 40). In this example the IP addresses are 172.168.20.1/24, 172.168.30.1/24 and 172.168.40.1/24, respectively.
- The WoL server is configured with a static IP address of 172.168.30.2/24.
- SW1 and SW2 are Layer 2 switches.
- L3-Source and L3-Destination are Layer 3 switches.

The configuration steps for the Layer 3-Destination switch are shown in [Figure 84](#).

```
HP Destination Switch(config)# ip routing      Enable routing.

Create ACL for VLAN 20, allow traffic on UDP port 7 only from WoL server.

HP Destination Switch(config)# ip access-list extended VLAN_20
HP Destination Switch(config-ext-nacl)# permit udp host 172.168.30.2 host
172.168.20.255 eq 7

Deny any other directed-broadcast traffic on this subnet.
HP Destination Switch(config-ext-nacl)# deny ip any 172.168.20.255/24
HP Destination Switch(config-ext-nacl)# permit ip any any
HP Destination Switch(config-ext-nacl)# exit

Create ACL for VLAN 40, allow traffic on UDP port 7 only from WoL server.

HP Destination Switch(config)# ip access-list extended VLAN_40
HP Destination Switch(config-ext-nacl)# permit udp host 172.168.30.2 host
172.168.40.255 eq 7

Deny any other directed-broadcast traffic on this subnet.
HP Destination Switch(config-ext-nacl)# deny ip any 172.168.40.255/24
HP Destination Switch(config-ext-nacl)# permit ip any any
HP Destination Switch(config-ext-nacl)# exit

Configure VLAN 20; enable directed-broadcast.

HP Destination Switch(config)# vlan 20
HP Destination Switch(vlan-20)# ip address 172.168.20.1/24
HP Destination Switch(vlan-20)# ip helper-address 172.168.30.2
HP Destination Switch(vlan-20)# ip directed-broadcast
HP Destination Switch(vlan-20)# ip access-group VLAN_20 out
HP Destination Switch(vlan-20)# exit

Configure VLAN 40; enable directed-broadcast.

HP Destination Switch(config)# vlan 40
HP Destination Switch(vlan-20)# ip address 172.168.40.1/24
HP Destination Switch(vlan-20)# ip helper-address 172.168.30.2
HP Destination Switch(vlan-20)# ip directed-broadcast
HP Destination Switch(vlan-20)# ip access-group VLAN_40 out
HP Destination Switch(vlan-20)# exit

Configure trunks, assign ports/trunks to VLANs, establish route to VLAN 30. Not shown in this example.

HP Destination Switch(config)# write memory
```

Figure 84. Example Configuration for the Destination Switch

The configuration steps for the Layer 3-Source switch are shown in [Figure 85](#).

- **Enhancement (PR_0000058564)** — Adds the ability to send syslog messages via TCP.

Syslog via TCP

This enhancement provides TCP as a transport protocol option for delivering logging messages to the syslog server. Because TCP is a connection-oriented protocol, a connection must be present before the logging information is sent. This helps ensure that the logging message will reach the syslog server.

Each configured syslog server needs its own connection. You can configure the destination port that is used for the transmission of the logging messages.

Syntax: [no] logging <ip-addr> [udp <1024-49151> | tcp <1024-49151>]

Allows the configuration of the UDP or TCP transport protocol for the transmission of logging messages to a syslog server.

Specifying a destination port with UDP or TCP is optional.

*Default ports: UDP port is 514
TCP port is 1470*

Default Transport Protocol: UDP

Examples

HPswitch(config)# logging 192.123.4.5 tcp	Default TCP port 1470 is used.
---	--------------------------------

Figure 87. Example of Configuring TCP for Logging Message Transmission Using the Default Port

HPswitch(config)# logging 192.123.4.5 tcp 9514	TCP port 9514 is used.
--	------------------------

Figure 88. Example of Configuring TCP for Logging Message Transmission Using a Specified Port

HPswitch(config)# logging 192.123.4.5 udp	Default UDP port 514 is used.
---	-------------------------------

Figure 89. Example of Configuring UDP for Logging Message Transmission Using the Default Port

HPswitch(config)# logging 192.123.4.5 udp 9512	UDP port 9512 is used.
--	------------------------

Figure 90. Example of Configuring UDP for Logging Message Transmission Using a Specified Port

- **Enhancement (PR_0000058798)** — Adds the ability to enable an SNMP trap for any configuration change made in the switch's running configuration file.

SNMP Trap on Running Configuration Changes

This enhancement provides the functionality for sending a specific SNMP trap for any configuration change made in the switch's running configuration file. The trap will be generated for changes made from any of these interfaces:

- CLI
- Menu
- WebAgent (Web UI)
- SNMP (remote SNMP set requests).

The SNMP trap will contain the following information.

Information	Description
Event ID	An assigned number that identifies a specific running configuration change event.
Method	Method by which the change was made—CLI, Menu, WebAgent, or remote SNMP. For configuration changes triggered by internal events, the term "Internal-Event" is used as the source of the change.
IP Address Type	Indicates the source address type of the network agent that made a change. This is set to an address type of unknown when not applicable.
IP address	IP address of the remote system from which a user accessed the switch. If not applicable, this is an empty string and nothing is displayed, for example, if access is through a management console port.
User Name	User name of the person who made the change. Null if not applicable.
Date and Time	Date and time the change was made.

The SNMP trap alerts any interested parties that someone has changed the switch's configuration and provides information about the source for that change. It does not specify what has been changed.

Enabling Running Configuration Change SNMP Traps

The following command is used to enable SNMP traps for this feature.

Syntax: [no] snmp-server enable traps running-config-change [transmission-interval <0-4294967295>]

Enabled SNMP traps being sent when changes to the running configuration file are made.

Default: Disabled

transmission-interval <0-2147483647>: Controls the egress rate for generating SNMP traps for the running configuration file. The value configured specifies the time interval in seconds that is allowed between the transmission of two consecutive traps. All running configuration change events that occur within the specified interval will not generate SNMP traps, although they will be logged in the Configuration Changes History Table.

A value of 0 (zero) means there is no limit; traps can be sent for every running configuration change event.

Default: Zero.

Displaying Configuration File Change Information

The **changes-history** parameter is added to the existing **show running-config** command to display the history information for changes occurring to the running configuration file.

Syntax: show running-config [changes-history [1-32]] [detail]

Displays the history up to 32 events for changes made to the running-configuration file. The changes are displayed in descending order, the most recent change at the top of the list. You can specify from 1 to 32 entries for display.

*The **detail** option will display a more detailed amount of information for the configuration changes.*

```
HPSwitch(config)# show running-config changes-history
```

```
Running Config Last Changed    : 02/19/10 16:30:09
Number of Changes Since Reboot : 150086
```

Event ID	Config Method	Date	Time
150086	CLI	02/19/10	16:30:09
150085	SNMP	02/03/10	14:50:12
150084	SNMP	02/03/10	14:50:12
150083	SNMP	02/03/10	14:45:59
150082	SNMP	02/03/10	14:27:15
150081	SNMP	02/03/10	13:11:00
150080	SNMP	02/03/10	13:11:00
150079	CLI	01/18/10	09:09:17

Figure 91. Example of Output for Running Configuration Changes History for All Ports

```
HPswitch(config)# show running-config changes-history 6
```

```
Running Config Last Changed    : 08/04/10 16:35:31
Number of Changes since Reboot : 120
```

Event ID	Config Method	Date	Time
120	CLI	08/04/10	16:35:31
119	CLI	08/04/10	16:34:01
118	SNMP	08/04/10	15:32:22
117	WEBUI	08/03/10	12:55:21
116	MENU	07/01/10	01:45:26
115	CLI	06/23/10	11:34:23

Figure 92. Example of Output for Running Configuration Changes History

Figure 93 and Figure 94 display detailed information for configuration changes history.

```
HPswitch(config)# show running-config changes-history 3 detail
```

```
Event ID      : 120
User          : switch_admin
Remote IP Address : 10.11.12.4
Config Method  : CLI
Date          : 08/04/10
Time          : 16:35:31
```

```
Event ID      : 119
User          : switch_admin
Remote IP Address : 10.11.12.4
Config Method  : CLI
Date          : 08/04/10
Time          : 16:34:01
```

```
Event ID      : 118
User          : switch_admin
Remote IP Address : 10.11.12.4
Config Method  : SNMP
Date          : 08/04/10
Time          : 15:32:22
```

Figure 93. Example of Detailed Output for Running Configuration Changes History

```
HPswitch(config)# show running-config changes-history detail
```

```
Running Config Last Changed: 01/01/90 00:35:44
Number of changes since last boot : 6
```

```
Event ID      : 6
User          :
Remote IP Address :
Config Method  : CLI
Date          : 01/01/90
Time          : 00:35:44
```

```
Event ID      : 5
User          :
Remote IP Address :
Config Method  : CLI
Date          : 01/01/90
Time          : 00:35:39
```

```
Event ID      : 4
User          :
Remote IP Address :
Config Method  : CLI
Date          : 01/01/90
Time          : 00:35:33
```

```
Event ID      : 3
User          :
Remote IP Address :
Config Method  : CLI
Date          : 01/01/90
Time          : 00:35:27
```

Figure 94. Example of Output for Running Config Changes History with Detail

Figure 95 displays the current status (enabled/disabled) of the SNMP trap type for running-configuration changes.

```
HPswitch(config)# show snmp-server traps

Trap Receivers

Link-Change Traps Enabled on Ports [All] : All

Traps Category                Current Status
-----
SNMP Authentication           : Extended
Password change                : Enabled
Login failures                 : Enabled
Port-Security                  : Enabled
Authorization Server Contact   : Enabled
DHCP-Snooping                  : Enabled
Dynamic ARP Protection         : Enabled
Dynamic IP Lockdown            : Enabled
Running Configuration Changes  : Enabled

Address      Community      Events   Type   Retry   Timeout
-----
173.33.25.201 public      None     trap   3       15

Excluded MIBs
```

SNMP trap status for running-config changes is enabled.

Figure 95. Example of SNMP Trap Configuration Status Information

- **Enhancement (PR_0000058804)** — Allows the redistribution into RIP of static blackhole or reject routes.

Static Summary Route to RIP

Overview

This enhancement allows the redistribution into RIP of static blackhole or reject routes. Blackhole or reject route redistribution can be manually enabled using the **redistribute static include-all** command.

Note Reject routes are null routes configured to drop traffic for the device at the configured address and return an ICMP error message. Blackhole routes are null routes that silently drop traffic for the configured network.

Redistributing Static Reject and Blackhole Routes

The static configuration of blackhole and reject routes is configured with the existing command:

```
[no] ip route <dest-ip-address/mask-length> <reject | blackhole>
```

Use the **include-all** parameter in the following command to enable redistribution of static reject and blackhole routes. The **include-all** option operates in conjunction with any other statically configured routes. It does not change the behavior of routes that are excluded from redistribution by the **restrict** option, that is, static blackhole and reject routes will not be redistributed if a matching **restrict** configuration exists.

Syntax: [no] redistribute <static [include-all] | connected | ospf> [route-map <name>]

Enables redistribution of the specified route type to the RIP domain. Executed in RIP context.

static: *Redistribute from manually configured routes.*

include-all: *Enables redistribution of static reject and blackhole routes. Default is disabled.*

connected: *Redistribute from locally connected network(s).*

ospf: *Redistribute from OSPF routes*

route-map <name>: *Optionally specify the name of a route-map to apply during redistribution*

*The **no** form of the command disables redistribution for the specified route type.*

Default: Disabled

```
HPswitch(config)# router rip
HPswitch(rip)# redistribute static include-all
HPswitch(rip)# restrict 11.0.0.0 255.0.0.0
HPswitch(rip)# write mem
HPswitch(rip)# exit
```

Figure 96. Example of Redistributing Static Reject and Blackhole Routes

```
HPswitch(config)# show ip rip redistribute

RIP redistributing

Route type RouteMap      Options
-----
connected  PRNMAP
static     SRVMAP           Includes blackhole
                                and reject
```

Figure 97. Example of RIP Redistribution Information Including Reject and Blackhole Routes

- **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.

Dynamic Port Access Auth via RADIUS

Overview

In some situations, it is desirable to configure RADIUS attributes for downstream supplicant devices that allow dynamic removal of the 802.1X, MAC, and Web authentication limits on the associated port of the authenticator switch. This eliminates the need to manually reconfigure ports associated with downstream 802.1X-capable devices, and MAC relay devices such as IP phones, on the authenticator switches. When the RADIUS authentication ages out, the authentication limits are dynamically restored. This enhancement 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. The changes are always applied to the port on the authenticator switch associated with the supplicant being authenticated.

Note

All the changes requested by the VSAs must be valid for the switch configuration. For example, if either MAC-based or Web-based port access is configured while 802.1X port access is in client mode, a RADIUS client with a VSA to change the 802.1X port access to port-based mode is not allowed. 802.1X in port-based mode is not allowed with MAC-based or web-based port access types. However, if the authenticating client has VSAs to disable MAC-based and Web-based authentication in conjunction with changing 802.1X to port-based mode, then client authentication is allowed.

Configuring the RADIUS VSAs

Only RADIUS -authenticated port-access clients will be able to dynamically change the port access settings using the new proprietary RADIUS VSAs. The settings that can be overridden are:

- Client limit (address limit with mac-based port access)
- Disabling the port-access types
- Setting the port mode in which 802.1X is operating

If the VSA client limit decreases the switch's configured client limit, all clients except the client that is overriding the settings is deauthenticated. Only one client session at a time can override the port-access settings on a port. When the client session is deauthenticated, the port resets itself to the configured settings. This port reset causes the deauthentication of all clients for the port-access authentication types that had their settings changed dynamically.

The new VSAs are:

- **HP-Port-Client-Limit-Dot1x:** This VSA temporarily alters the 802.1X authentication client limit to the value contained in the VSA. Values range from 0 to 32 clients. A zero client limit means this VSA is disabled. This is an HP proprietary VSA with a value of 10.
- **HP-Port-Client-Limit-MA:** This VSA temporarily alters the MAC authentication client limit to the value contained in the VSA. Values range from 0 to 256 clients. A zero client limit means this VSA is disabled. This is an HP proprietary VSA with a value of 11.
- **HP-Port-Client-Limit-WA:** This VSA temporarily alters the Web authentication client limit to the value contained in the VSA. Values range from 0 to 256 clients. A zero client limit means this VSA is disabled. This is an HP proprietary VSA with a value of 12.
- **HP-Port-Auth-Mode-Dot1x:** This VSA temporarily alters the 802.1X authentication mode to be either port-based or user-based depending on the value in the VSA. A port-based VSA is set with a value of 1; a user-based VSA is set with a value of 2. This is an HP proprietary VSA with a value of 13.
- If an 802.1X port is operating in port-based mode, it is invalid to set the 802.1X client limit using the HP-Port-Client-Limit VSA.

Note

The changing of the client limits for a port using VSAs is temporary. The running configuration file is not changed and still displays the client limit and address limit settings.

Each authentication type may have a unique value for the client limit. If the value of the VSA is zero, the authentication type corresponding to that VSA will be disabled.

Settings for these VSAs are in effect for the duration of the authenticated session of the downstream supplicant switch. If for any reason there is a loss of the session (link loss between authenticator switch and supplicant switch, or authentication failure during reauthentication), the originally configured 802.1X and MAC authentication limits are restored.

Displaying the Port-access Information

The **show port-access summary** command displays the dynamically changed client limit settings.

Syntax: show port-access summary [radius-overridden]

Displays summary configuration information for all ports, including the ports that have client limits set by RADIUS VSAs.

radius-overridden: *Displays only the ports with client limits that are overridden by RADIUS attributes.*

Note If the command **no aaa port-access authentication <port-list> client-limit** is executed, the port access is in port-mode. If the 802.1X client-limit is configured with a value from 1-32, the port access is in user-mode.

```
HPswitch(config)# show port-access summary

Port Access Status Summary

Port-access authenticator activated [No] : No
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

Note: * indicates values dynamically overridden by RADIUS
```

Port	Authenticator		Limit	Web Auth		MAC Auth	
	Enabled	Mode		Enabled	Limit	Enabled	Limit
1	Yes	user*	1*	Yes	1	Yes	1
2	Yes	user	32	Yes	32*	Yes	32
3	Yes	port	1	No	1	No	1
4	No	port	1	No	1	No*	1

Figure 98. Example of Summary Configuration Information Showing RADIUS Overridden Client Limits

To display the configuration information for just those ports that are dynamically overridden by RADIUS attributes, use the **show port-access summary radius-overridden** command.

```
HPswitch(config)# show port-access summary radius-overridden

Port Access Status Summary

Port-access authenticator activated [No] : No
Allow RADIUS-assigned dynamic (GVRP) VLANs [No] : No

Note: * indicates values dynamically overridden by RADIUS
```

Port	Authenticator		Limit	Web Auth		MAC Auth	
	Enabled	Mode		Enabled	Limit	Enabled	Limit
1	Yes	user*	1*	Yes	1	Yes	1
2	Yes	user	32	Yes	32*	Yes	32
4	No	port	1	No	1	No*	1

Figure 99. Example of Output for Client-limit Values that are RADIUS Overridden

Operating Notes

- Only RADIUS authentication supports the new VSAs. Other authentication types, such as TACACS, are not supported.
- The new VSAs are not supported in IDM and they cannot be specified in the configurations. The new VSAs must be configured manually.
- If the RADIUS server delivers a new VSA to an authenticator switch that does not understand it, the Access-Accept message is rejected.

Version K.15.04.0002 Enhancements

Version K.15.04.002 includes the following enhancements.

- **Enhancement (PR_0000060667)** — Adds DHCPv6 client authentication options.

DHCPv6 Client Authentication Options Added

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.

SSH Client

This feature provides a method for establishing a secure session from one HP switch to another. In addition to providing secure sessions, SFTP is enhanced to allow bidirectional secure copying of files between a switch and an SFTP server, initiated from the switch with the copy command. The SFTP server can be another switch or a workstation/server with a running SSH server that supports SFTP.

Each switch with the SSH Client feature will have a known hosts file that can contain the public key from switches and servers that have been determined to be genuine. New public keys can be added to the known hosts file when new SSH servers are contacted, up to a maximum of 100 entries (if memory allows). The known hosts file can also be copied to another switch or to a server where it can be edited.

Note You must be in manager context to use this SSH and SFTP feature.

Opening a Secure Session to an HP Switch

To initiate an SSH client session to another network device, use the following command, executed in the manager context.

Syntax: `ssh [user <username | username@>] <hostname | IPv4 | IPv6> [port <1-65535>]`

Enables an SSH client to open a secure session to an HP switch. Opening secure sessions to devices other than HP switches is not supported.

[user <username | username@>]: Optional; the username on the destination (remote) system. Usernames for Operator and Manager must be configured.

If **<username@>** is specified, enter the remote system information of either hostname, IPv4 address, or IPv6 address.

If no **username** is configured, the **username** of the current login is used. There will be a prompt for a password if needed.

hostname: Hostname of the remote system.

IPv4: IPv4 address of the remote system.

IPv6: IPv6 address of the remote system.

[port <1-65535>]: The TCP port running the SSH server on the remote system. If no port number is specified, the default port 22 is used.

Default: Port 22

Operating Notes

- The SSH server may challenge the client to authenticate itself depending on the authentication methods configured on the destination SSH server. The client first tries the “none” method of authentication; if that is unsuccessful, it examines the list of supported authentication methods from the server, if provided. If the server does not provide such a list, all methods of authentication will be tried in the following order until the session is successfully opened or rejected by the server:
 - Authentication Method “publickey”, if a private key has been loaded onto the switch.
 - Authentication method “password”.
- During “public-key” authentication, the client must use its private key to authenticate itself to the server. There can be only one key pair on the switch for the manager.
- The private key should be passphrase protected for highest security; the user is prompted to enter the passphrase.
- The private key can be configured by copying it to the SSH client switch (using the **copy** command).
- If the public-key authentication fails or the client has not been configured with a key pair, the “password” method of authentication is used and the user is prompted for a password.
- Successful TACACS or RADIUS logins will give the user either operator or manager privileges. This is important if there are chained SSH sessions.

Copying Client Key Files

Only one ssh client key for authenticating the manager is allowed on a switch. The **copy** command allows you to copy the client key files using **sftp**, **tftp**, and **usb or xmodem**, allowing encryption and authentication through SSH. There is no way to generate the private key on the switch; it must be copied onto the switch.

To load the client's private key onto the switch, use one of these commands.

Syntax: `copy sftp ssh-client-key [user <username> | <username@>] <hostname | IPv4 | IPv6> <private-key-filename> [port <tcp-port-num>]`
`copy tftp ssh-client-key <hostname | IPv4 | IPv6> <private-key-filename>`
`copy usb ssh-client-key <private-key-filename>`
`copy xmodem ssh-client-key`

Copies the client key file <private-key-filename> onto the switch.

ssh-client-key: *The client key file being copied to the switch. The file must contain an RSA or DSA key.*

[user <username | username@>]: *Optional; there must be configured usernames for Operator and Manager.*

*If no **username** is specified, the client's current **username** is used. There will be a prompt for a password if needed.*

hostname: *Specifies the hostname of the SFTP or TFTP server.*

IPv4: *Specifies the SFTP or TFTP server's IPv4 address.*

IPv6: *Specifies the SFTP or TFTP server's IPv6 address.*

<private-key-filename>: *The remote filename containing the key.*

[port <tcp-port-num>]: *TCP port of the SSH server on the remote system.*

The copied private key is stored in the ssh directory of the switch's file system and is persistent across switch reboots. After the initial copying is complete, the client key can be overwritten by repeating the **copy** command. No verification of the validity of the key is done when executing the copy command.

Copying the SSH-Client-Known-Hosts File

Replacing or Appending the SSH-Client-Known-Hosts File. There is one SSH client known hosts file per switch, stored in the ssh directory of the switch's file system. The SSH client known hosts file can be overwritten or appended using the commands below. If the file already exists at that location, you will be prompted for confirmation before overwriting the existing file:

Warning: The existing known hosts file will be overwritten, continue [y/n] ?

Syntax: `copy sftp ssh-client-known-hosts [user <username> | <username@>] <hostname | IPv4 | IPv6> <filename> [append]`
`copy tftp ssh-client-known-hosts <hostname | IPv4 | IPv6> <filename> [append]`
`copy usb ssh-client-known-hosts <filename> [append]`
`copy xmodem ssh-client-known-hosts [append]`

Copies the SSH client known hosts file to the switch.

ssh-client-known-hosts: *The known hosts file.*

[user <username | username@>]: *Optional; there must be configured usernames for Operator and Manager.*

*If no **username** is specified, the client's current **username** is used. There will be a prompt for a password if needed.*

hostname: *Specifies the hostname of the TFTP server.*

IPv4: *Specifies the TFTP server's IPv4 address.*

IPv6: *Specifies the TFTP server's IPv6 address.*

<filename>: *The remote filename containing the key.*

[append]: *Append hosts to the existing ssh-client-known-hosts file.
Default: Replace the existing known hosts file.*

Copying the SSH Client Known Hosts File to Another Location. The SSH client known hosts file can be copied to a location on a remote device using the commands below. If the file already exists on the remote device, you are prompted for confirmation before overwriting the file:

Warning: The remote file will be overwritten, continue [y/n] ?

Syntax: copy ssh-client-known-hosts sftp [user <username> | <username@>] <hostname | IPv4 | IPv6> <filename>
copy ssh-client-known-hosts tftp <hostname | IPv4 | IPv6> <filename>
copy ssh-client-known-hosts <filename> usb
copy ssh-client-known-hosts xmodem

Copies the SSH client known hosts file to another location.

ssh-client-known-hosts: *The known hosts file.*

[user <username | username@>]: *Optional; there must be configured usernames for Operator and Manager.*

*If no **username** is specified, the client's current **username** is used. There will be a prompt for a password if needed.*

hostname: *Specifies the hostname of the TFTP server.*

IPv4: *Specifies the TFTP server's IPv4 address.*

IPv6: *Specifies the TFTP server's IPv6 address.*

<filename>: *The remote filename containing the key.*

Copying the Host Public Key

The following **copy** commands can be used to manage public keys in a known hosts file. The public key can only be copied from the switch to a server or other media, not to another switch.

Syntax: copy ssh-server-pub-key sftp [user <username> | <username@>] <hostname | IPv4 | IPv6> <filename>
copy ssh-server-pub-key tftp <hostname | IPv4 | IPv6> <filename>
copy ssh-server-pub-key usb
copy ssh-server-pub-key xmodem

Copies the switch's SSH server public key to a server or other media.

[user <username | username@>]: *Optional; there must be configured usernames for Operator and Manager.*

*If no **username** is specified, the client's current **username** is used. There will be a prompt for a password if needed.*

hostname: *Specifies the hostname of the TFTP server.*

IPv4: *Specifies the TFTP server's IPv4 address.*

IPv6: *Specifies the TFTP server's IPv6 address.*

<filename>: *The name of the file to be copied.*

Removing the SSH Client Key Pair

To remove the SSH client key pair file, use this command.

Syntax: `crypto key zeroize ssh-client-key`

Deletes the SSH client key pair.

You will be prompted for confirmation with the message:

Warning: The manager key pair will be deleted, continue [y/n] ?

Removing the SSH Client Known Hosts File

To remove the SSH client known hosts file, use this command.

Syntax: `crypto key zeroize ssh-client-known-hosts`

Deletes the SSH client known hosts file.

You will be prompted with a message:

Warning: The SSH client known hosts file will be deleted, continue [y/n] ?

Displaying Open Sessions

To view all open sessions, including console, telnet and ssh, enter the command **show session-list**.

Syntax: `show session-list`

Displays the active incoming and outgoing sessions.

```
Switch(config)# show session-list

Session Information

Source IP Selection: Outgoing Interface
-----
Session   :      1
Privilege: Superuser
From      : Console
To        :
-----
Session   :      2
Privilege: Manager
From      : 172.22.16.3
To        : 10.1.248.198
-----
Session   : **   3
Privilege: Manager
From      : 10.1.248.179
To        :
-----
```

Figure 100. Example of Open Sessions Listing

- **Enhancement (PR_0000061695)** — Adds encoded version information to the config file.

Encoded Version Information Added to Config File

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, fields are now added in authentication requests for management telnet, ssh, and http service.

Fields Added to Authentication Requests

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.

Include RADIUS and TACACS Only Credentials

The **include-credentials** feature is enhanced to provide a **radius-tacacs-only** option to the command. The new **show include-credentials** command displays the current **include-credentials** status on the switch. When **include-credentials** has been executed, resulting in the authentication information such as passwords and SSH keys being stored in the configuration file, **include-credentials** is “activated”. The status can be enabled or disabled.

Currently, **include-credentials** can be disabled, but the internal changes are not reversed. The **include-credentials store-in-config** command is identical in execution to the **include-credentials** command, however, when executed in the **no** form of the command, that is, **no include-credentials store-in-config**, the changes implemented when **include-credentials** was executed are reversed to the factory default settings.

Include-credentials radius-tacacs-only Option

This option allows you to execute **include-credentials** for *only* RADIUS and TACACS. The **radius-tacacs-only** option does not cause the switch to store authentication passwords and SSH keys in the configuration file.

Syntax: [no] include-credentials [radius-tacacs-only | store-in-config]

Enables the inclusion of passwords and security credentials in each configuration file when the file is saved onto a remote server or workstation.

*When **no include-credentials** is executed, include-credentials is disabled. Credentials continue to be stored in the active and inactive configuration files but are not displayed.*

radius-tacacs-only: *When executed with the **radius-tacacs-only** option, only the RADIUS and TACACS security keys are included in the configuration when saving files remotely.*

*The **radius-tacacs-only** option can be disabled with either command:*

no include-credentials

no include-credentials radius-tacacs-only

store-in-config: *Stores passwords and SSH authorized keys in the configuration files. This happens automatically when **include-credentials** is enabled.*

*The **no include-credentials store-in-config** command disables include-credentials and removes credentials stored in the configuration files. The switch reverts to storing only a single set of passwords and SSH keys, regardless of which configuration file is booted.*

When **include-credentials radius-tacacs-only** is executed, this warning message displays.

```
Switch(config)# include-credentials radius-tacacs-only

          **** CAUTION ****

This will insert possibly sensitive information in switch configuration files,
and as a part of some CLI commands output. It is strongly recommended that you
use SFTP rather than TFTP for transfer of the configuration over the network,
and that you use the web configuration interface only with SSL enabled.

Erasing configurations with 'include-credentials' enabled will erase stored
passwords and security credentials. The system will reboot with the factory
default configuration.
```

Figure 101. Example of Caution Message Displayed for radius-tacacs-only Option

Executing include-credentials or include-credentials store-in-config

When **include-credentials** or **include-credentials store-in-config** is executed for the first time, for example, on a new switch, or when you previously have successfully executed the **no include-credentials store-in-config** command, the passwords and SSH keys are not currently stored in the configuration file (not activated). This warning message displays.

```
Switch(config)# include-credentials

          **** CAUTION ****

You have invoked the command 'include-credentials'. This action will make changes
to the password and SSH public-key storage.

It will affect *all* stored configurations, which might need to be updated.
Those credentials will no longer be readable by older software revisions.
It also may break some of your existing user scripts. Continue?[y/n] y

When you enter 'y', this caution appears.

Erasing configurations with 'include-credentials' enabled will erase stored
passwords and security credentials. The system will reboot with the factory
default configuration.

Proceed?[y/n]
```

Figure 102. Example of Caution Message Displayed When Executing include-credentials (or include-credentials store-in-config)

No Include-credentials store-in-config Option

The **no include-credentials** command disables include-credentials as before. Credentials continue to be stored in the active and inactive configurations, but are not displayed in the config file.

When **no include-credentials** is used with the **store-in-config** option, **include-credentials** is disabled and the credentials stored in the config files are removed. The switch is restored to its default state and only stores one set of operator/manager passwords and SSH keys.

If you choose to execute the **no include-credentials store-in-config** command, you are also presented with the option of setting new switch passwords, as shown in [Figure 103](#).

You are also queried about retaining the current SSH authorized keys on the switch. If you enter “y”, the currently active authorized key files are renamed to the pre-include-credentials names, for example:

```
/file/mgr_auth_keys.2 -> /file/mgr_auth_keys
/file/authorized_keys.2 -> /file/authorized_keys
```

All remaining authorized keys files with an extension are deleted.

```
Switch(config)# no include-credentials store-in-config

This will remove any switch passwords and inactive SSH authorized keys from all
configuration files. This will also restore the functionality to store only a
single set of passwords and authorized keys on the switch.
Do you want to continue (y/n)? y

The SSH authorized keys associated with the active configuration will be deleted.
Would you like to retain these as the switch global SSH authorized keys (y/n)? y

Do you want to set new switch passwords (y/n)? y

Operator username: admin
Operator password: *****
Confirm password: *****
Manager username: GeorgeV
Manager password: *****
Confirm password: *****

Switch(config)#
```

Setting new passwords for multiple usernames.

Figure 103. Example of no include-credentials store-in-config Messages and Options

Displaying the Status of include-credentials on the Switch

The **show include-credentials** command provides the current status of include-credentials on the switch.

Syntax: show include-credentials

Displays information about the passwords and SSH keys stored in the configuration.

Stored in Configuration - Yes: *The passwords and SSH keys are stored in the configuration. Include-credentials was executed.*

Stored in Configuration - No: *There is only one set of operator/manager passwords and one set of SSH keys for the switch.*

Enabled in Active Configuration: *Include-credentials is either enabled or disabled.*

RADIUS/TACACS only: *Displayed when the option is configured.*

```
Switch(config)# show include-credentials

Stored in Configuration           : Yes
Enabled in Active Configuration  : N/A
RADIUS/TACACS Only               : Yes
```

Figure 104. Example of Output for show include-credentials Command

Storage States When Using Include-Credentials

The following table shows the states of several access types when the factory default settings are in effect or when include-credentials is enabled or not enabled.

Type	Factory Default	Include-Credentials Enabled	Include-Credentials Disabled but Active	No Include-Credentials Executed
Manager/Operator Passwords & port access	Single set for switch Stored outside config Not displayed in config file	One set per stored config Stored in config Displayed in config	Same as include-credentials enabled Not displayed in config	One set for switch No credentials displayed in config
SSH Public Key	One set for switch Stored in flash Not displayed in config	One set per stored config Stored in flash Displayed in config	Same as include-credentials enabled Not displayed in config	One set for switch No credentials displayed in config
SNMPv3 auth and priv	Stored in flash Not displayed in config	Stored in flash Displayed in config	Same as include-credentials enabled Not displayed in config	No credentials displayed in config
RADIUS & TACACS keystings	Not displayed in config	Stored in flash Displayed in config	Same as include-credentials enabled Not displayed in config	No credentials displayed in config

Note: When **no include-credentials store-in-config** is executed, the switch is restored to its default state and only stores one set of operator/manager passwords and SSH keys.

- **Enhancement (PR_0000065022)** — Provides a way to gracefully shut down OSPF routing on HP switches without losing packets that are in transit.

OSPF Neighbor Shutdown Notification

This feature provides a way to gracefully shut down OSPF routing on HP switches without losing packets that are in transit. OSPF neighbors are informed that the router should not be used for forwarding traffic, which allows for maintenance on the switch without interrupting traffic in the network. There is no effect on the saved switch configuration.

Prior to a switch shutdown, the CLI/SNMP **reload** command or the CLI **boot** command is executed to initiate the sending of OSPF “empty Hello list” messages on the interfaces that are part of the OSPF routing configuration. After a small delay (approximately 2 seconds) that allows the messages to be transmitted on all applicable interfaces the **boot** or **reload** command continues.

Modules Operating in NonStop Mode

When a switch is in standalone mode and OSPF routing is enabled, the “empty Hello list” is transmitted whenever the **boot** or **reload** commands are executed.

When the switch is operating in nonstop switching mode (redundant) and a single module is being reloaded or booted, the standby module will notify neighboring switches of the management module failover. If the failover fails, the “empty Hello list” is transmitted before the switch is rebooted.

When a switch is operating with multiple management modules in warm standby mode, the “empty Hello list” is sent when a **reload** or **boot** command is executed. The standby management module sends out OSPF Hello packets after becoming the active management module.

- **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.

Accept CDP/LLDP Packets Tagged for VLAN 1

This feature allows incoming CDP and LLDP packets tagged for VLAN 1 to be processed even if VLAN 1 does not contain any ports. VLAN 1 must be present, but it is typically present as the default VLAN for the switch.

Note The switch may pick up CDP and LLDP multicast packets from VLAN 1 even when CDP- and/or LLDP-enabled ports are not members of VLAN 1.

- **Enhancement (PR_0000065218)**—Provides a way to define a fixed, user-assigned cost of an OSPF LSA type 3 summarized prefix.

Define Cost of LSA Type 3 Summarized Prefix

This enhancement provides a way to define a fixed, user-assigned cost of an LSA type 3 summarized prefix. To accomplish this, the **area** command (in **router ospf** context) has an optional new metric-cost parameter.

Syntax: [no] area <ospf-area-id | backbone > range <ip-addr/mask-length> [no-advertise] type [summary [cost <1-16777215>]] | nssa

Use this command on a routing switch intended to operate as an ABR for the specified area to do either of the following:

- *Simultaneously create the area and corresponding range setting for routes to summarize or block.*
- *For an existing area, specify a range setting for routes to summarize or block.*

< ospf-area-id | backbone>: A normal area identified by a single integer or an IP address. Use 0.0.0.0 or the **backbone** option to specify the backbone area.

range < ip-addr/mask-length >: Defines the range of route advertisements to either summarize for injection into the backbone area or to prevent from being injected into the backbone area.

The **ip-addr** value specifies the IP address portion of the range, and **mask-length** specifies the leftmost significant bits in the address. The ABR for the specified area compares the IP address of each outbound route advertisement with the address and significant bits in the mask to determine which routes to select for either summarizing or blocking. For example, a range of 10.10.32.1/14 specifies all routes in the range of 10.10.32.1 - 10.10.35.254.

[no-advertise]: Use this keyword only if you want to configure the ABR to prevent advertisement to the backbone of a specified range of routes. (This has the effect of “hiding” the specified range from the backbone area.) If you do not use this option, the ABR advertises the specified range of routes according to the **type < summary | nssa >** selection described below.

[type < summary [cost <1-16777215>] | nssa >]: Configures the type of route summaries to advertise or block. If **type** is not used in the command, then the ABR defaults this setting to **summary**.

summary [cost <1-16777215>]: Specifies internal routes in the configured range of route advertisements. If **no-advertise** (above) is used in the command, then the ABR prevents the selected internal routes from being summarized in a type-3 LSA and advertised to the backbone. If **no-advertise** is not used in the command, then the selected routes are summarized to the backbone in a type-3 LSA.

[cost <1-16777215>]: User configured cost for an area summary range. If **cost** is specified, then the range will advertise the specified cost instead of the calculated cost.

nssa: Specifies external routes (type-7 LSAs) in the configured range of route advertisements. If **no-advertise** (above) is used in the command, then the ABR prevents the selected external routes from being summarized in a type-5 LSA and advertised to the backbone. (Configure this option where an ABR for an NSSA advertises external routes that you do not want propagated to the backbone.) If **no-advertise** is not used in the command, then the selected routes learned from type-7 LSAs in the area are summarized to the backbone in a type-5 LSA.

To set the summary cost to 100 for area 10 with and address range of 10.10.0.0/16, enter the command shown in [Figure 105](#).

```
Switch(ospf)# area 10 range 10.10.0.0/16 type summary cost 100
```

Figure 105. Example of Setting a Summary Cost to an Area

To use the standard method for determining the summarized cost, enter the command shown in [Figure 106](#).

```
Switch(ospf)# area 10 range 10.10.0.0/16 type summary
```

Figure 106. Example of Using a Standard Summary Cost for an Area

You must execute **write mem** in order to preserve these settings across reboots.

Displaying the OSPF Cost Settings

The **show ip ospf** command displays information about summary costs. An entry of “auto” indicates that the cost is calculated by the OSPF standard for summarized networks.

```
Switch(config)# show ip ospf

OSPF Configuration Information
:
:
Currently defined address ranges:
Area ID          LSA Type   IP Network   Network Mask   Advertise Cost
-----
0.0.0.10         Summary   10.10.0.0    255.255.0.0    yes           auto
0.0.0.20         Summary   10.20.0.0    255.255.0.0    yes           16777215
0.0.0.30         Summary   10.30.0.0    255.255.0.0    no            auto
```

Figure 107. Example of Output Showing Settings for Summary Costs

- **Enhancement (PR_0000069103)** — Additional support added for zl modules.

Additional Support 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 “Chassis Redundancy” in the *Management and Configuration Guide*.

OSPFv2 Logging commands and command output

- **Enhancement (PR_0000052548)** - Adds improved logging, commands, and command output for OSPFv2 troubleshooting. See “IP Routing” in the *Multicast and Routing Guide*.

VLAN Multicast Filter Global Configuration

- **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*.

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 2. 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 Tunking” 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 Tunking” 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 Tunking” 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 Guide* for your switch.

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.*xxx* or earlier), see the Release Notes provided with those versions.

Version K.15.01.0031

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 18](#).
- **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 18](#).
- **Enhancement (PR_0000040783)** — This enhancement reduces the down time when unicast routing indicates a Candidate Rendezvous Point (C-RP) is not reachable. Upon detecting a C-RP has become unreachable, the Bootstrap Router (BSR) sends a new Bootstrap Message (BSM) with a zero holdtime for the unreachable C-RP. All devices in the PIM domain should then remove this C-RP from their RP-set.
- **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 18](#).
- **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 20](#).
- **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

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 22](#).
- **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

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

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 23](#).
- **Enhancement (PR_0000044183)** — Display interface configuration enhancement. For more information, see [“Display Configuration of Selected Interface” on page 24](#).
- **Enhancement (PR_0000045649)** — Post-login banner enhancement. For more information, see [“Post-login Banner Enhancement” on page 30](#).
- **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 32](#).
- **Enhancement (PR_0000045711)** — Web authentication message enhancement. For more information, see [“Web Auth Deny Message” on page 36](#).
- **Enhancement (PR_0000045752)** — User-configurable per-port MAC address enhancement. For more information, see [“Port Security Per-Port MAC Increase” on page 39](#).
- **Enhancement (PR_0000046912)** — Adds support for LLDP PoE+. For more information, see [“PoE with LLDP” on page 39](#).
- **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 42](#).
- **Enhancement (PR_0000052801)** — Categorize CLI Return Messages enhancement. For more information, please see [“Categorize CLI Return Messages” on page 43](#).
- **Enhancement (PR_0000055430)** — Adds support for Energy Efficient Ethernet (IEEE 802.3az). For more information, please see [“Energy Efficient Ethernet \(EEE\)” on page 46](#).
- **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 supernatted IP addresses, and supernatted 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

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

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 50](#).
- **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 Port Addition or Deletion of MAC Addresses” on page 56](#).
- **Enhancement (PR_0000052266)** — Adds the ability to enable an SNMP trap when the switch's startup configuration is changed. For more information, see [“Log Message When Startup Config Updated” on page 58](#).
- **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 60](#).
- **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 61](#).
- **Enhancement (PR_0000054055)** — This enhancement provides the ability to display OSPF neighbor timer information. For more information, see [“Show OSPF Neighbor Timers” on page 61](#).
- **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 62](#).
- **Enhancement (PR_0000055367)** — Adds the ability to log ACL **permit** entries. For more information, see [“Logging for Routing ACLs” on page 64](#).
- **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 68](#).
- **Enhancement (PR_0000058512)** — Adds Wake-on-LAN support across VLANs. For more information, see [“Wake-on-LAN Support Across VLANs” on page 69](#).
- **Enhancement (PR_0000058564)** — Adds the ability to send syslog messages via TCP. For more information, see [“Syslog via TCP” on page 73](#).
- **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 74](#).
- **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 77](#).
- **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 78](#).
- **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

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

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

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

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

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 81](#).
- **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 86](#).
- **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 90](#).
- **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 91](#).
- **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 91](#).
- **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 Opware 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

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

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 OSPFv3 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 OSPF 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

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

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

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

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 2](#) . For more information about the feature, see the chapter "Configuring Username and Password Security" in the *Access Security Guide* for your switch.

Version K.15.05.0006

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

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

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.
- **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 Tunking" 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 modified or added. For more information see the "Port Tunking" 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 Tunking" 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)** - PCMLive 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

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=0x000000035 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

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.

Technology for better business outcomes

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

© Copyright 2010-2011 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP will not be liable for technical or editorial errors or omissions contained herein.



November 2011

Manual Part Number
5998-1186