



Release Notes:

Version ST.1.0.090603 Software

for the HP ProCurve Threat Management Services zl Module

These release notes include information on the following:

- Downloading documentation from the Web ([page 1](#))
- Downloading and installing software updates ([page 2](#))
- Software fixes included in release ST.1.0.090603 ([page 7](#))
- Known Issues in release ST.1.0.090603 ([page 15](#))

Support Notices

Caution

The HP ProCurve Series 5400 zl and 8200zl switches require software version K.13.40 or later to support the Threat Management Services (TMS) zl Module. To download the latest switch software, please go to the [Software for switches](#) page on the HP ProCurve Web site.

Caution

Before you update software to a new version, ProCurve strongly recommends that you save a copy of your config file to an external location. See "Backup and Restore System Configuration" in the *HP ProCurve Threat Management Services zl Module Management and Configuration Guide* for more information ([ProCurve manuals](#)).

© Copyright 2009 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

Publication Number

5900-0224
June 2009

Applicable Products

HP ProCurve Threat Management Services zl Module	(J9155A)
HP ProCurve Threat Management Services zl Module with 1-year IPS subscription service bundle	(J9156A)
ProCurve Switch 5412zl	(J8698A)
ProCurve Switch 5406zl-48G	(J8699A)
ProCurve Switch 5412zl-96G	(J8700A)
ProCurve Switch 8212zl	(J8715A)

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.

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 Customer Support/Warranty booklet included with the product.

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/go/procurve

Contents

Software Management	1
Download Switch Documentation from the Web	1
View or Download the Software Manual Set	1
Software Updates	1
Software Releases and Support	1
Downloading Software to the TMS zl Module	2
Updating the Module Software Using the Web Browser Interface	3
Updating the Module Software Using the CLI	4
Software Fixes ST.1.0.090603	7
Release ST.1.0.090603	7
General	7
Firewall	8
IPS/IDS	11
Monitor Mode	13
High Availability	13
VPN	13
Known Issues	15
Release ST.1.0.090603	15
Upgrading to ST.1.0.090603 from ST.1.0.090213	15
General	16
Firewall	23
IPS	24
VPN	24
High Availability (HA)	25
Monitor Mode	26
Release ST.1.0.090213	26
IPS/IDS	40
VPN	40
High Availability (Active/Standby)	41
Monitor Mode Only	42

(This page intentionally left blank.)

Software Management

Download Switch Documentation from the Web

You can download software updates and the corresponding product documentation from the ProCurve Networking Web site as described below.

View or Download the Software Manual Set

Go to: www.hp.com/go/procurve/manuals

You may want to bookmark this Web page for easy access in the future.

Software Updates

Check the ProCurve Networking Web site frequently for software updates for the various ProCurve products you may have in your network.

Software Releases and Support

In addition to the HP ProCurve Lifetime Warranty* on the module and five year warranty on the hard disk drive (HDD), technical support and software releases are included in the purchase price of the HP ProCurve TMS zl Module, as described below.

The HP ProCurve TMS zl Module includes one (1) year of telephone and mail support, providing you technical assistance during HP local business hours. This assistance is for product-specific questions on product features and specifications, installation, general configuration, basic troubleshooting, and usage. The support is provided on a commercially reasonable effort basis, and there is no charge by HP to use this support. The product also includes:

- software maintenance releases (which provide fixes for defects), when and if available, for as long as you own the product
- software update releases (which provide minor enhancements), when and if available, for one year
- software upgrade releases (which provide major enhancements), when and if available, for one year

Fee-based services can be purchased to uplift the telephone support to 24x7 coverage. Services are also available to provide telephone support after one year, or to receive software update or upgrade releases beyond one year.

* For as long as you own the product, with next-business-day advance replacement (available in most countries). The following hardware products and their related series modules have a one-year hardware warranty with extensions available: HP ProCurve Routing Switch 9300m series, HP ProCurve Switch 8100fl series, HP ProCurve Network Access

Software Management

Software Updates

Controller 800, and HP ProCurve DCM Controller. The following hardware mobility products have a one-year hardware warranty with extensions available: HP ProCurve M111 Client Bridge, HP ProCurve MSM3xx-R Access Points, HP ProCurve MSM7xx Mobility and Access Controllers, HP ProCurve RF Manager IDS/IPS Systems, HP ProCurve MSM Power Supplies, HP ProCurve 1 Port Power Injector, and HP ProCurve CNMS Appliances. Disk drives in the HP ProCurve ONE Services zl Modules have a five year hardware warranty. Standalone software, upgrades, or licenses may have a different warranty duration. For details, refer to the ProCurve Software License, Warranty, and Support booklet at www.hp.com/go/procurve/warranty.

Downloading Software to the TMS zl Module

ProCurve Networking periodically provides TMS zl Module software updates through the ProCurve Networking Web site (www.hp.com/go/procurve). After you acquire a new software file, you can use the Web browser interface or the TMS zl Module CLI to install it.

Note

After installing the update software using one of the methods described below, you must reboot your module to load and begin using the new software.

Updating the Module Software Using the Web Browser Interface

This section describes how to use the Web browser interface to download software to the module. For more detailed information, refer to "Update Software with the Web Browser Interface" in the *HP ProCurve Threat Management Services zl Module Management and Configuration Guide* ([ProCurve manuals](#)). Also, you can click **Help** in the Web browser interface to access context sensitive help for downloading and other interface screens. If you are running Firefox 3, ensure that you have an ActiveX plug-in, otherwise, some of the features in the Help Files will not function.

The module's Web browser interface supports Internet Explorer 7 or 8 or Firefox2.x or 3.

Note

In routing mode, make sure that your access policies permit traffic between the **SELF** zone and the FTP, TFTP, or SCP server.

1. Download the new software image from procurve.com.
2. Transfer the compressed image to an FTP, TFTP, or SCP server.
3. Select **System > Maintenance** and then click the **Update Software** tab.
4. For **Server Type**, select **FTP, TFTP, or SCP**.
5. Complete the **Download Information** with the information required by the server type you selected above.
6. Click **Download and install** to download the software to the module and install it.

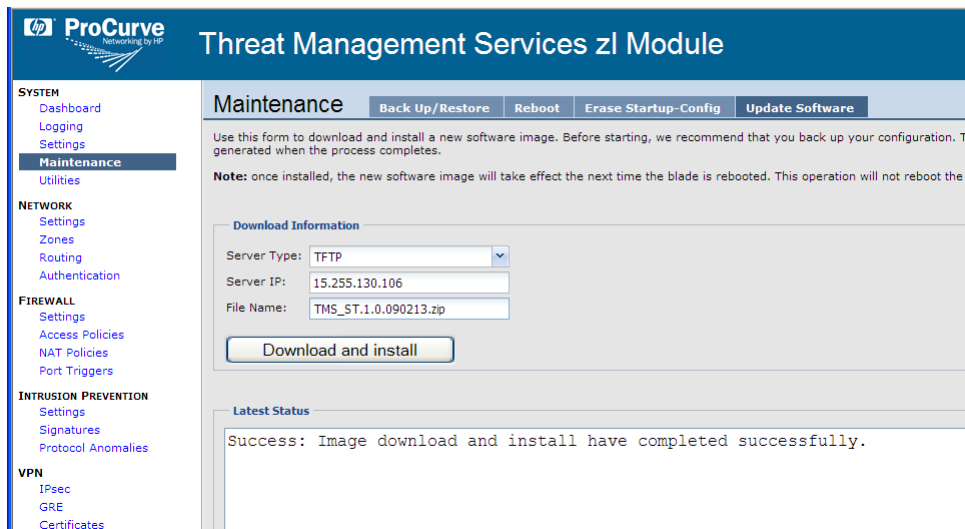


Figure 1. A Successful TMS zl Module Software Update Using the Web Browser Interface

7. Wait for this message in the **Latest Status** field: **Success: Image download and install have completed successfully.** (see [Figure 1](#)).
8. Select the **Reboot** tab and click the **Reboot** button to complete the installation.

Updating the Module Software Using the CLI

Three separate processes are available for updating the module software using the TMS zl Module CLI.

- Using an FTP or SCP server
- Using a TFTP Server
- Using a USB Drive

For more detailed information, refer to "Update Software with the CLI" in the *HP ProCurve Threat Management Services zl Module Management and Configuration Guide* ([ProCurve manuals](#)).

Using an FTP or SCP server.

1. Transfer the compressed image onto an FTP or SCP server.
2. Initiate a console session with the host switch.
3. Enter the ProductOS context for the TMS zl Module.

```
hostswitch# services c 2
```

4. Copy the image from the server and install.
5. Reboot the module to complete the update.

```
hostswitch(tms-module-C)# reboot
```

For example, suppose that you copied the image to an FTP server that has the parameters shown below:

- IP address — 192.168.1.13
- Username — PROCURVEUIUSR_CA
- Password — procure
- Filename — ST.1.0.090603.zip (copied to the root directory)

1. You would type the following:

```
hostswitch(tms-module-C)# copy ftp image 192.168.1.13 ST.1.0.090603.zip user  
PROCURVEUIUSR_CA
```

2. After you press **Enter**, the module prompts you for the password.

```
Password: procure
```

3. The image is copied to the module, then automatically installed.

4. When the prompt says that the installation is finished, reboot the module to complete the update.

```
hostswitch(tms-module-C)# reboot
```

Using a TFTP Server.

1. Transfer the compressed image onto a TFTP server.
2. Initiate a console session with the host switch.
3. Enter the ProductOS context for the TMS zl Module.

```
hostswitch# services c 2
```

4. Copy the image from the server and install.
5. Reboot the module to complete the update.

```
hostswitch(tms-module-C)# reboot
```

For example, suppose that you copied the image to a TFTP server that has the parameters shown below:

- IP address—192.168.1.13
- Filename—ST.1.0.090603.zip (copied to the root directory)

1. You would type the following:

```
hostswitch(tms-module-C)# copy tftp image 192.168.1.13 ST.1.0.090603.zip
```

2. The image is uploaded to the module, then automatically installed.
3. When the prompt says that the installation is finished, reboot the module to complete the update.

```
hostswitch(tms-module-C)# reboot
```

Using a USB Drive.

1. Extract the compressed software image.
2. Transfer the extracted image folder onto a USB drive in a directory called /services/images.

Note: The first partition on the USB drive should be in FAT32 format. You can reset the USB format, if necessary, using the HP USB Creator tool.

3. Initiate a console session with the host switch.
4. Boot to the Services OS.

```
hostswitch# services c 1
```

```
hostswitch(services-module-C:PR)# boot service
```

5. When the module comes back online, enter the Services OS again.

```
hostswitch# services c 1
```

6. Insert the USB drive in the USB port on the TMS zl Module.

7. Wait a few seconds, then mount the USB drive.

```
hostswitch(services-module-C:HD)# usb mount
```

8. Copy the image from the drive to the module.

For example, if the image directory name is **ST.1.0.090603**, you would type:

```
hostswitch(services-module-C:HD)# usb copyfrom ST. 1. 0. 090603
```

You can type the first few letters of the directory name, then press the Tab key to complete the name. You might need to add the last few characters of the directory name if the USB drive contains more than one image.

9. Update the software.

For example, if the new image directory is **ST.1.0.090603**, you would type:

```
hostswitch(services-module-C:HD)# update product ST. 1. 0. 090603
```

Again, you can use tab completion for the file name.

10. When the prompt says that the installation is finished, unmount and remove the USB drive.

```
hostswitch(services-module-C:HD)# usb unmount
```

Remove the USB drive from the module.

Caution: The module cannot boot (the next step) if the USB drive remains inserted in the module.

11. Boot the module to the ProductOS to complete the update.

```
hostswitch(services-module-C:HD)# boot product
```

Software Fixes ST.1.0.090603

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

Release ST.1.0.090213 was the first production software release for the HP ProCurve Threat Management Services zl Module.

Release ST.1.0.090603

The following problems were resolved in release ST.1.0.090603

General

- **PR_6127/ PR_16218** — The output of the **show run** command will show an `FDPoll Returned Error` message, which is not relevant to the output and inconsequential. It can safely be ignored.
- **PR_13105** — When using the **show vlans** command in a CLI session established by going through the switch interface, the VLAN information displayed is overlapped.
- **PR_15153** — When using the TMS zl Module CLI, two commands provide an **insert-at <position>** extended option: **access-policy** and **nat**. There is no error checking on the position number provided - it is assumed that a policy or rule exists at that location.
- **PR_16218** — The output of the **show run** command will show an `FDPoll Returned Error` message, which is not relevant to the output and inconsequential. It can safely be ignored.
- **PR_16539** — When using the TMS zl Module CLI, the **radius-server help** command gives options that are not available.
- **PR_16585** — An SNMP walk of the TMS zl Module MIB can go into a recursive loop when SNMP trap receiver entries that have been created are disabled.
- **PR_16690** — When an SNMP application is utilizing the ScriptMIB, the **User Group** command is failing with `Invalid Input` if hash mark character (`#`) is included in the Group Name, even though the `#` character is valid for a Group Name.
- **PR_17313** — For a VLAN association, the user can specify DHCP as a method for getting an IP address for the TMS zl Module. If the user goes in and edits the VLAN association and changes the IP address method to a Static IP address, the DHCP client process still runs in the background and can overwrite the static IP address.

- **PR_18770** — It was possible that a management denial of service would happen with the TMS zl Module if the httpd stopped or crashed. Now the httpd is added to a monitoring watchdog service that will automatically restart the httpd if it stops.
- **PR_19098** — TMS zl Module was not showing any log entries that were generated due to multicast traffic.
- **PR_38256** — Using the Web browser interface, disabling PIM on a VLAN did not also disable IGMP on the VLAN.
- **PR_38257** — On the HA configuration page in the Web browser interface, if you change the Multicast IP and then refresh the HA page, you lose your changes. You must save and reboot for the changes to take effect.
- **PR_39059** — Time zone specification in **show time** was inconsistent between the switch and TMS zl Module. Changed the TMS zl Module to match the switch's method of displaying time to avoid confusion.
- **PR_39493** — When editing a routing protocol that has authentication set, if the authentication value is not provided, an error message is displayed. However, the changes that were made during an edit were still accepted, even though an error message was displayed.
- **PR_40662** — Log entries with the following message identifiers: 630, 631, 632, and 633 are marked as critical when they are not considered critical messages. They should be a warning. These messages occurred during port scan related activities and have been disabled at the present time.
- **PR_40780** — In the command line interface (CLI), the wrong number for the total number of connections in all zones is displayed in the connection-settings help text. The command is:

```
(tms-module-<slot-ID>:config)#connection-settings help
```

The output of this command would show **500000** instead of the correct value of **600000**.

Firewall

- **PR_11023** — Log messages tracking the login and logout of authenticated users are not generated by the firewall.
- **PR_37837** — Log messages with message IDs of 657 and 625 are logged as critical when they should not be critical.

```
time="2009-03-30 09:17:09" severity=critical pri=1  
fw=ProCurve-TMS-zl-Module id=fw_l213_attack msg="FW: packet with  
invalid tcp flags found, packets dropped" srczone=INTERNAL  
src=192.168.0.134 srcport=18155 dstzone=EXTERNAL dst=192.168.1.128  
dstport=80 proto=TCP subfamid=packetheaderanomaly mtype=attack  
mid=625
```

The log messages are no longer logged as critical. Instead the log message is displayed with severity as warning and with the priority as 4.

- **PR_38246** — Log messages with message IDs of 685 and 651 are logged as critical when they are not critical.

```
time="2009-03-25 15:51:17" severity=critical pri=1
fw=ProCurve-TMS-zl-Module id=fw_l2l3_attack msg="MCAST: packet
spooof detected" srczone=INTERNAL src=10.1.70.1 srcport=0
dstzone=UNKNOWN_ZONE dst=224.0.0.1 dstport=0 proto=IGMP subf-
amid=ipspoofing mtype=attack duplicatecount=5 mid=685
```

```
time="2009-03-25 15:48:47" severity=critical pri=1
fw=ProCurve-TMS-zl-Module id=fw_l2l3_attack msg="ICMP: Duplicate
ICMP error message received, dropping packet" srczone=EXTERNAL
src=192.168.5.194 srcport=5060 dstzone=INTERNAL dst=192.168.6.194
dstport=5060 proto=UDP icmptype=3 subfamid=icmpreplayattack
mtype=attack mid=651 icmpcode=3
```

- **PR_38335** — Multicast firewall does not timeout IGMP related sessions properly when the IGMP policy is deleted.

Example:

Multicast Sender (Zone1) <--> TMS <--> Multicast Receiver (INTERNAL)

1. Multicast group address 224.1.1.1 port 60.
2. Enable PIM and IGMP on both VLANs.
3. Setup an Access Policy for 224.1.1.1 port 60 from Zone1 to INTERNAL.
4. Setup an IGMP Policy.
5. Allow multicast traffic to pass.
6. Delete IGMP Policy.

Multicast Receiver can still receive traffic by sending IGMP Join messages to TMS zl Module.

- **PR_38532** — When Synflood Protection is disabled, log messages continue to be seen as if it were enabled.
- **PR_38564** — The log message with the messageID of 648 is marked as critical should not be.

```
time="2009-04-01 11:41:59" severity=critical pri=1
fw=ProCurve-TMS-zl-Module id=fw_l2l3_attack msg="ICMP:Error message
not allowed by firewall" srczone=INTERNAL src=192.168.0.1
dstzone=EXTERNAL dst=192.168.1.56 proto=ICMP icmptype=3 subf-
amid=icmppacketanomaly mtype=attack mid=648 icmpcode=1
```

The severity has been changed to warning and the priority attribute has been changed from 1 to 4.

- **PR_39231** — Log message with message ID 643 is marked as critical but is not critical.

```
time="2009-04-15 09:25:53" severity=critical pri=1
fw=ProCurve-TMS-z1-Module id=fw_l2l3_attack msg="ICMP: packet with
invalid sequence number appeared, packets dropped" srczone=INTERNAL
src=192.168.80.1 dstzone=INTERNAL dst=192.168.80.5 proto=ICMP icmp-
type=0 subfamid=icmppacketanomaly mtype=attack mid=643 icmpcode=0
```

- **PR_39235** — Log messages for message IDs of 655, 653, 612, 601,1356, 608, and 642 are marked as critical are not critical

```
time="2009-04-15 10:18:02" severity=critical pri=1
fw=ProCurve-TMS-z1-Module id=fw_l2l3_attack msg="IPROUTE: source ip
address is set to be broadcast ip, packets dropped" srczone=INTERNAL
src=255.0.0.0 srcport=0 dstzone=INTERNAL dst=192.168.80.1 dstport=0
proto=235 subfamid=routeanomaly mtype=attack mid=655
```

```
time="2009-04-15 10:20:22" severity=critical pri=1
fw=ProCurve-TMS-z1-Module id=fw_l2l3_attack msg="FW: no protocol
option set in packet header, packets dropped" srczone=INTERNAL
src=192.0.80.5 dstzone=UNKNOWN_ZONE dst=192.168.80.1 proto=ICMP
subfamid=packetheaderanomaly mtype=attack duplicatecount=500
mid=612
```

```
time="2009-04-15 10:19:55" severity=critical pri=1
fw=ProCurve-TMS-z1-Module id=fw_l2l3_attack msg="FW: packet
checksum check failed, packets dropped" srczone=UNKNOWN_ZONE
src=192.0.80.5 srcport=0 dstzone=UNKNOWN_ZONE dst=192.168.80.1
dstport=0 proto=244 subfamid=checksumanomaly mtype=attack mid=601
```

```
time="2009-04-15 10:17:15" severity=critical pri=1
fw=ProCurve-TMS-z1-Module id=fw_l2l3_attack msg="IP fragment data-
length is not in units of 8 octets" srczone=UNKNOWN_ZONE src=0.0.0.0
srcport=0 dstzone=UNKNOWN_ZONE dst=0.0.0.0 dstport=0 proto=0 subf-
amid=intergritycheck mtype=attack mid=1356
```

```
time="2009-04-15 10:20:00" severity=critical pri=1
fw=ProCurve-TMS-z1-Module id=fw_l2l3_attack msg="FW: icmp header is
less than expected, packets dropped" srczone=EXTERNAL
src=192.168.80.5 dstzone=SELF dst=192.168.80.1 proto=ICMP subf-
amid=packetheaderanomaly mtype=attack mid=608
```

```
time="2009-04-15 10:19:33" severity=critical pri=1
fw=ProCurve-TMS-z1-Module id=fw_l2l3_attack msg="ICMPREPLAY:
packets with duplicate sequence number found, packets dropped"
srczone=EXTERNAL src=192.168.80.5 dstzone=SELF dst=192.168.80.1
proto=ICMP icmpstype=8 subfamid=icmpreplayattack mtype=attack
mid=653 icmpcode=0
```

```
time="2009-04-15 10:18:48" severity=critical pri=1  
fw=ProCurve-TMS-zl-Module id=fw_l2l3_attack msg="ICMP: echo  
response packet appeared without request, packets dropped"  
srczone=SELF src=192.168.80.1 dstzone=EXTERNAL dst=255.255.255  
proto=ICMP icmpctype=0 subfamid=icmppacketanomaly mtype=attack  
mid=642 icmpcode=0
```

- **PR_39337** — Log message with the message ID of 1356 is marked as critical but should not be critical.

```
time="2009-04-16 18:08:59" severity=critical pri=1  
fw=ProCurve-TMS-zl-Module id=fw_l2l3_attack msg="IP fragment data-  
length is not in units of 8 octets" srczone=UNKNOWN_ZONE src=0.0.0.0  
srcport=0 dstzone=UNKNOWN_ZONE dst=0.0.0.0 dstport=0 proto=0 subf-  
amid=intergritycheck mtype=attack mid=1356
```

- **PR_39412** — Fuzzing DNS requests and responses can cause a TMS zl Module denial of service if a DNS-based access policy is configured.
- **PR_39735** — During FTP stress testing, a denial of service attack could be executed against the FTP Application Layer Gateway (ALG).

IPS/IDS

- **PR_12937** — In a certain condition, when the TCP RST timeout value is set to zero and IPS is enabled, the TMS zl Module will not forward a TCP RST packet from one peer to another. If there is a TCP session established or half-established between client and server, and the server sends an RST Packet to close the session, the TMS zl Module will mark the session to be deleted. If IPS is enabled, the TMS zl Module will forward the RST packet to IPS. After IPS finishes processing the packet, the TMS zl Module gets the RST packet. Since TMS zl Module has already marked the session to be deleted and the RST timeout value is 0, the RST packet is not forwarded to the peer and is dropped. The problem only happens for RST packets. By setting the RST timeout value to something other than zero, this issue can be avoided.
- **PR_18204** — If you filter signatures by severity, then disable a family of signatures, the expected result is that all displayed signatures in that family will be disabled. However, the actual result is that only some of the signatures displayed get disabled. This can be observed by viewing **info** signatures, then disabling the XSS family. When the operation completes, refresh the page, and view **info** signatures. When you inspect the XSS family you will see that not all XSS family **info** signatures are disabled.
- **PR_37450** — TMS zl Module was not saving the IPS or IDS configuration in its configuration backup file.
- **PR_37834** — When IPS settings are changed for threat level actions and an IPS attack was detected, the log entry for that attack did not display the changed rule action.

- **PR_37838** — The log does not display the correct message when an attack is detected by IPS

The following log is displayed during an IPS attack:

```
time="2009-03-19 09:57:14" severity=critical pri=1  
fw=ProCurve-TMS-zl-Module id=ips_attack_family rule=3331 msg="IPS  
detection: Allow: Backdoor FeRAT 1.00" src=192.168.1.20 srcport=1079  
dst=192.168.3.20 dstport=1234 proto=TCP ruleaction=Allow ruleth-  
reat=Critical connectiondirection=initiator packetdirection=2 pack-  
etlength=43 ipidentification=914 rulefam=BACKDOOR ruledsc="Backdoor  
FeRAT 1.00" subfamid=ips_signature_based_logs attackid=no-id  
mtype=iips_15_17_attack mid=3331 timetolive=3 actiontype=log
```

Go to **IPS>Settings>Actions** page and set the threat level to the default values:

Critical=Terminate session
Severe=Block traffic
Minor=Block traffic
Warning=Allow traffic
Information=Allow traffic

The following log is displayed, which does not display the correct action:

```
time="2009-03-19 02:01:49" severity=major pri=2  
fw=ProCurve-TMS-zl-Module id=ips_attack_family rule=3101 msg="IPS  
detection: Allow: Doly Backdoor for Windows detection"  
src=192.168.1.20 srcport=1051 dst=192.168.3.20 dstport=1015  
proto=TCP ruleaction=Allow rulethreat=Severe connectiondirec-  
tion=initiator packetdirection=2 packetlength=44 ipidentifica-  
tion=42240 rulefam=BACKDOOR ruledsc="Doly Backdoor for Windows  
detection" subfamid=ips_signature_based_logs attackid=no-id  
mtype=iips_15_17_attack mid=3101 timetolive=3 actiontype=block  
  
time="2009-03-19 02:01:49" severity=critical pri=1  
fw=ProCurve-TMS-zl-Module id=ips_attack_family rule=3189 msg="IPS  
detection: Allow: BackDoor Digital Root Beer" src=192.168.1.20  
srcport=1050 dst=192.168.3.20 dstport=2600 proto=TCP ruleac-  
tion=Allow rulethreat=Critical connectiondirection=initiator pack-  
etdirection=2 packetlength=60 ipidentification=38912  
rulefam=BACKDOOR ruledsc="BackDoor Digital Root Beer" subf-  
amid=ips_signature_based_logs attackid=no-id  
mtype=iips_15_17_attack mid=3189 timetolive=3 actiontype=terminate
```

- **PR_38512** — When the same IPS attack was continuously launched against the TMS zl Module and generating log entries, log throttling was not working and many of the same IPS log entries were populating the log file.

Monitor Mode

- **PR_14582** — In monitor mode, the CLI command **ips help** does not reflect the commands that are actually available in monitor mode as opposed to routing mode.

High Availability

- **PR_38385** — Connection reservations do not fail over from the Master to the Participant in an Active-Standby configuration.

Example:

```
PC    DMZ 10.10.30.254   |TMS|   Zone1 192.168.1.254   PC Server
10.10.30.1                                     192.168.1.1
```

Zone limits DMZ = 5

Connection reservation DMZ, inbound, reserved for 192.168.1.1, Reservation count = 3

If the PC opens TCP connections through the Master, and a fail over situation occurs, the reservation count was not correctly followed.

- **PR_38959** — In High Availability **Active-Standby** configuration, when running a mix of RTSP and SMTP traffic for a period, the command **no connections** does not reset some of the current connections.

VPN

- **PR_38173** — Misleading error messages appear when adding or editing an IKE policy in the Web browser interface (**VPN > Certificates > IPsec Certificates**).
- **PR_38217** — When setting up an IPsec policy with a Key Exchange of Manual, it was possible to specify an SPI number that was already in use by another IPsec policy and it would not be detected. Duplicate SPI numbers across IPsec policies are not allowed and an error needs to be displayed.
- **PR_38223** — When adding an IPsec policy with action **Bypass** or **Ignore**, and setting the direction to **Inbound**, the traffic selector's local and remote addresses would be swapped.
- **PR_38226** — Changing a **bypass** or **ignore** IPsec policy to **apply** shows an erroneous key exchange method.
- **PR_38228** — A misleading error occurs when the traffic selector's IP range starts or ends with **255**. Workaround: Correct the range.
- **PR_38229** — IPsec policy advanced settings are displayed incorrectly after the default settings are changed and then edited in the Web browser interface.
- **PR_38231** — On the advanced settings screen (**VPN > IPsec > IPsec Policies**) **Enable fragment before IPsec** cannot be disabled.

- **PR_38240** — Cannot import IPsec Certificates (intermittently fails) from the Web browser interface (**VPN > Certificates > IPsec Certificates**).
- **PR_38887** — In the Web browser interface, when viewing the IPsec VPN Tunnels, the local gateway IP address may be truncated in the display.
- **PR_39898** — A denial of service attack against the TMS zl Module is possible when an IPSecuritas client establishes a VPN connection with the TMS zl Module. Set the IKE authentication method to RSA certificates on both the client and the TMS zl Module. On the IPSecuritas client, clear the **Request Certificate**, **Send Certificate**, and **Verify Certificate** check boxes in the **Options** tab of the Connections window. When the IPSecuritas client attempts to establish a VPN connection with the TMS zl Module, the module will be inoperable with its current settings.
- **PR_40144** — When using Internet Explorer 7 and viewing IPsec VPN tunnels, the information does not appear. However, when using Firefox 3.x, the IPsec VPN tunnel does show up. This has been changed in this release so that the IPsec VPN tunnel information does appear in Internet Explorer.
- **PR_41209** — A Certificate Revocation List (CRL) was not retained across a reboot.
- Example:
 1. Go to **VPN-->Certificates--> CRL** page and load a CRL list.
 2. Save the entire configuration.
 3. Reboot the TMS zl Module.
 4. Once the TMS zl Module is available, go to **VPN--> Certificates--> CRL** page and the CRL is no longer available.

Known Issues

Known issues fixed in a later software release are indicated using the following format:

- PR_xxxxxxxxxx —

To confirm what release fixed the issue, use the issue number to search the PDF file.

Known issues that are open as of the latest software release appear as follows:

- **PR_xxxxxxxxxx** —

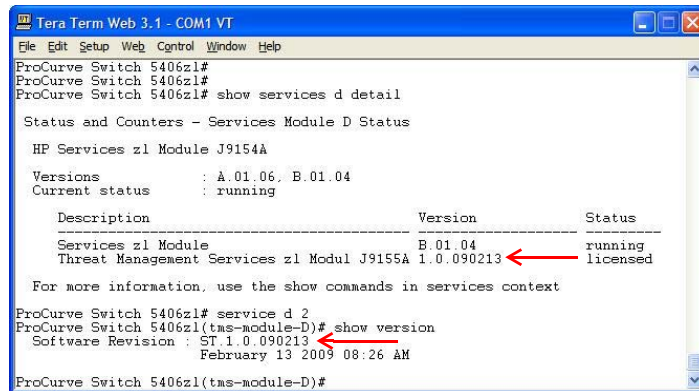
Release ST.1.0.090603

The following problems are known issues as of release ST.1.0.090603.

Upgrading to ST.1.0.090603 from ST.1.0.090213

PR_41849/PR_41855 — After upgrading, the switch command line reports the first installed TMS z1 Module software version (ST.1.0.090213) rather than the updated version (ST.1.0.090603)

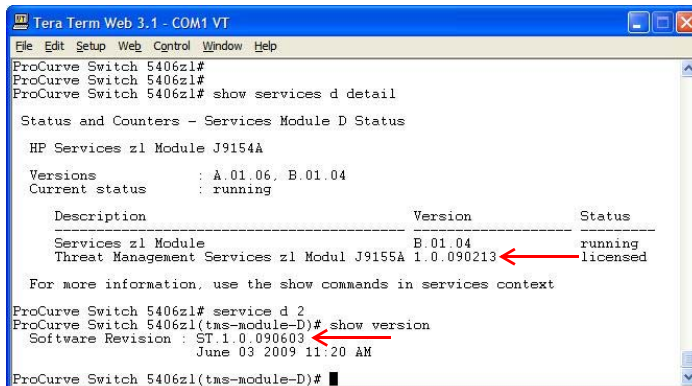
When the TMS z1 Module is running ST.1.0.090213, the following behavior is observed:



```
Tera Term Web 3.1 - COM1 VT
File Edit Setup Web Control Window Help
ProCurve Switch 5406z1#
ProCurve Switch 5406z1#
ProCurve Switch 5406z1# show services d detail
Status and Counters - Services Module D Status
HP Services z1 Module J9154A
Versions          : A.01.06, B.01.04
Current status    : running
Description       Version          Status
-----
Services z1 Module  B.01.04          running
Threat Management Services z1 Modul J9155A 1.0.090213 ← running licensed
For more information, use the show commands in services context
ProCurve Switch 5406z1# service d 2
ProCurve Switch 5406z1(tms-module-D)# show version
Software Revision : ST.1.0.090213 ←
                  February 13 2009 08:26 AM
ProCurve Switch 5406z1(tms-module-D)#
```

The output of the switch CLI command, **show services <slot-ID> detail**, and the output of the TMS z1 Module CLI command, **show version**, are both correct.

After the TMS zl Module has been updated to ST.1.0.090603, the following behavior is observed:



```
ProCurve Switch 5406zl#
ProCurve Switch 5406zl# show services d detail

Status and Counters - Services Module D Status

HP Services zl Module J9154A

Versions          : A.01.06, B.01.04
Current status    : running

-----
Description              Version              Status
-----
Services zl Module       B.01.04              running
Threat Management Services zl Modul J9155A 1.0.090213 ← licensed

For more information, use the show commands in services context

ProCurve Switch 5406zl# service d 2
ProCurve Switch 5406zl(tms-module-D)# show version
Software Revision : ST.1.0.090603 ←
                  June 03 2009 11:20 AM

ProCurve Switch 5406zl(tms-module-D)#
```

The output of the switch CLI command, **show services <slot-ID> detail** reports the software version initially installed rather than the updated version. The output of the TMS zl Module CLI command, **show version**, is correct. Additionally, the software version information in the TMS zl Module's Web browser interface correctly identifies the updated version, ST.1.0.090603, as the current version.

General

- **PR_38053** — Unnecessary log information is displayed when an invalid user tries to login via SSH.

1. Open the TMS zl Module Web browser interface.
2. Go to the logging section.
3. Select the View Log tab.
4. Open a tool that allows to connect via SSH to the TMS zl Module.
5. Try to login to the TMS with an invalid user.
6. The following log entries are displayed:

```
time="2009-03-20 17:14:30" severity=warning pri=4
fw=ProCurve-TMS-zl-Module id=ssh msg="Failed password for invalid
user one from 192.168.8.103 port 16123 ssh2"
```

```
time="2009-03-20 17:14:24" severity=info pri=6
fw=ProCurve-TMS-zl-Module id=ssh msg="Failed none for invalid user
one from 192.168.8.103 port 16123 ssh2"
```

```
time="2009-03-20 17:14:24" severity=info pri=6
fw=ProCurve-TMS-zl-Module id=ssh msg="Invalid user one from
192.168.8.103"
```

Only the last log entry should be generated.

■ **PR_38154** — A misleading log entry generated when logging in as the user Operator.

1. Open the TMS zl Module Web browser interface.
2. Login as Operator.
3. Go to the logging section.
4. Select the View Log tab.
5. Search for the log entry generated when logging in as Operator.
6. The following log entries are displayed:

```
time="2009-03-24 10:52:39" severity=info pri=6 fw=ProCurve-TMS-zl-Module  
id=user_statistics msg="Web- config user logged in " srczone=SELF  
dstzone=SELF logintime="2009-03-24 10:52:39" logouttime=0 useri-  
paddr=192.168.8.103 pktstransfered=0 username=operator usersessionid=0  
subfamid=useraccounting mtype=userlogin mid=1202
```

```
time="2009-03-24 10:52:39" severity=warning pri=4 fw=ProCurve-TMS-zl-Module  
id=user_statistics msg="Web- Attempt to login with a wrong name:"  
srczone=SELF dstzone=SELF logintime="2009-03-24 10:52:39" logouttime=0  
useripaddr=192.168.8.103 pktstransfered=0 username=operator userses-  
sionid=0 subfamid=useraccounting mtype=userlogin mid=1204
```

The second log entry should not be displayed.

■ **PR_38181** — The wrong log entry generated when logging in as a local user.

1. Open the TMS zl Module Web browser interface.
2. Login as a previously created local user.
3. Go to the logging section.
4. Select the View Log tab.
5. Search for the log entry generated when logging in as Local user previously created.
6. The following log entry is displayed:

```
time="2009-03-24 17:00:02" severity=warning pri=4 fw=ProCurve-TMS-zl-Module  
id=user_statistics msg="Radius authentication failed" srczone=SELF  
dstzone=SELF logintime=0 logouttime=0 useripaddr=0.0.0.0 pktstransfered=0  
usersessionid=0 subfamid=useraccounting mtype=userlogin mid=4579
```

■ **PR_38247** — Unknown log message generated when a local user failed to authenticate mid=4507.

```
time="2009-03-25 16:11:54" severity=info pri=6 fw=ProCurve-TMS-zl-Module  
id=fw_access_control ruleid=0 msg="Authentication failed for TIM user"  
srczone=UNKNOWN_ZONE src=0.0.0.0 srcport=0 dstzone=UNKNOWN_ZONE dst=0.0.0.0  
dstport=0 proto=0 rcvd=0 rcvdsc=0 sent=0 sentsc=0 srcnatport=0 destnatport=0  
destnatipaddr=0.0.0.0 subfamid=accessdeny mtype=access_control mid=4507  
srcnatipaddr=0.0.0.0
```

- **PR_38705** — RIP: Connected VLANs are not sent correctly when RIPv1-v2 is set. The TMS zl Module does not send the connected VLANs to another router (R1), when RIP version has been set as v1-v2.

In the following example the TMS zl Module is using RIPv1-v2 and router R1 has RIP version 2 set.

Routes in TMS zl Module

Destination	Gateway	Metric	Distance	VLAN	Type
10.10.30.0/24	10.10.30.254	1	0	lan30	connected
10.10.40.0/24	10.10.40.254	1	0	vlan40	connected
192.168.1.0/24	192.168.1.254	1	0	vlan100	connected
192.168.2.0/24	192.168.3.250	3	100	vlan300	rip
192.168.3.0/24	192.168.3.254	1	0	vlan300	connected
192.168.5.0/24	192.168.1.253	2	110	vlan100	ospf
192.168.11.0/24	192.168.11.96	1	0	vlan1	connected

Routes in R1 when VLAN300 has v2 enabled in TMS zl Module

Destination	Gateway	Metric	Distance	VLAN	Type
10.10.30.0/24	192.168.3.254	3	100	vlan300	rip
10.10.40.0/24	192.168.3.254	3	100	vlan300	rip
192.168.1.0/24	192.168.3.254	3	100	vlan300	rip
192.168.2.0/24	192.168.2.250	1	0	vlan200	connected
192.168.3.0/24	192.168.3.250	1	0	vlan300	connected
192.168.5.0/24	192.168.3.254	3	100	vlan300	rip
192.168.11.0/24	192.168.11.95	1	0	vlan1	connected

Routes in R1 when VLAN300 has v1-v2 enabled in TMS zl Module

Destination	Gateway	Metric	Distance	VLAN	Type
192.168.1.0/24	192.168.3.254	3	100	vlan300	rip
192.168.2.0/24	192.168.2.250	1	0	vlan200	connected
192.168.3.0/24	192.168.3.250	1	0	vlan300	connected
192.168.5.0/24	192.168.3.254	3	100	vlan300	rip
192.168.11.0/24	192.168.11.95	1	0	vlan1	connected

As a workaround, use RIP version 2 in the TMS zl Module.

- **PR_38775** — Using the Command Line Interface, there is no mechanism to disable PIM globally. The Web browser interface must be used instead.
- **PR_38776** — Using the Command Line Interface, the **rp-address** command is not listed in the PIM context. As a result, if you have a static RP, the RP can't be deleted in PIM context.

Example:

1. Open a CLI session.
2. Go into PIM context.

```
<config>#router pim
```

3. Press the tab key.

```
end          Return to the Manager Exec context.
exit         Return to the previous context or terminate session.
logout       Terminate current session.
show         Display TMS device operation information.
```

The rp-address should be listed in PIM context.

- **PR_38778** — Learned RP are deleted when setting a static RP from the TMS module.

Example:

1. Open CLI session
2. Verify the learned RP

```
#show ip pim rp-set
```

```
Status and Counters - PIM-SM Static RP-Set Information
```

```
Group Address      Group Mask          RP Address
```

```
[empty]
```

Status and Counters - PIM-SM Learned RP-Set Information

Group Address	Group Mask	RP Address	Hold Time	Expire Time
224. 0. 0. 0	240. 0. 0. 0	192. 168. 3. 253	150	100
239. 0. 0. 0	255. 192. 0. 0	92. 168. 3. 253	150	100

3. Set a static RP

```
#router pim rp-address 192.168.2.253 224.0.0.0/6
```

4. Verify learned and static RP

```
#show ip pim rp-set
```

Status and Counters - PIM-SM Static RP-Set Information

Group Address	Group Mask	RP Address
224. 0. 0. 0	240. 0. 0. 0	192. 168. 2. 253

Status and Counters - PIM-SM Learned RP-Set Information

Group Address	Group Mask	RP Address	Hold Time	Expire Time
224. 0. 0. 0	240. 0. 0. 0	192. 168. 2. 253		

The PIM implementation of the TMS module will only allow Static RPs or Learned RPs to be used. They cannot both be used simultaneously.

- **PR_38849** — A incorrect log entry is generated when logging in with a user authenticated by a RADIUS server:

1. Open the TMS zl Module Web browser interface.
2. Login as correctly a user associated with a RADIUS user previously created (i.e. user1@tms.local)
3. Click the log out button
4. Log in as Manager
5. Go to the logging section
6. Select the View Log tab
7. Search for the log entry generated when logging in as the user associated to the RADIUS server
8. The following log entry is displayed:

```
time="2009-04-07 16:37:38" severity=warning pri=4 fw=ProCurve-TMS-zl-Module  
id=user_statistics msg="Web- Attempt to login with a wrong name:"  
srczone=SELF dstzone=SELF logintime="2009-04-07 16:37:38" logouttime=0  
useripaddr=192.168.8.103 pktstransfered=0 username=user1@tms.local  
usersessionid=0 subfamid=useraccounting mtype=userlogin mid=1204
```


The "Log in" and "log out" log entries are displayed properly but this log entry should not be generated.

- **PR_39239** — Some OSPF log entries have different priorities, can have duplicate entries, and lack general details.

- **Example:**

```
time="2009-04-15 11:57:12" severity=warning pri=4 fw=ProCurve-TMS-zl-Module  
id=routing msg="OSPF: invalid DD packet: Initialize flag mismatch (15)"
```

```
time="2009-04-15 11:59:32" severity=warning pri=5 fw=ProCurve-TMS-zl-Module  
id=routing msg="OSPF: invalid HELLO packet: Options mismatch (13)"
```

- **PR_39240** — A log message with message ID 705 has a spelling mistake: 'recoerd' should be 'record'.

```
time="2009-04-15 12:13:51" severity=info pri=6 fw=ProCurve-TMS-zl-Module  
id=config_configuration ruleid=1 msg="POLGRP: policy group recoerd deleted  
successfully" srczone=UNKNOWN_ZONE dstzone=UNKNOWN_ZONE result=0 subf-  
amid=configurationchanges operation=2 mtype=config mid=705 recname=.
```

- **PR_40003** — The TMS zl Module does not have an equivalent command to the switch's **show ip pim neighbor** to see adjacent PIM routers
- **PR_40292** — When a user has a local account on the TMS zl Module and has an account with the same name on the RADIUS server, the user will always be authenticated to the local account and no attempt is made to access the RADIUS server, even if the user name includes the realm, as in username@domain.
- **PR_40313** — When adding a RADIUS server, the administrator can specify a NAS-ID that accepts a script as input allowing code injection to RADIUS Web interface page.
- **PR_40319** — In the log file, log entries with the following message IDs may truncate the username: 1213, 1214, and 1204. Other information, such as the user's IP address and login time are displayed correctly.
- **R_40320** — In the log file, the RADIUS Log message IDs of 4518 and 4512 do not contain any details. Message ID of 4512 refers to an authentication request being sent to a RADIUS server (severity is **info**) and message ID of 4518 refers to a response from the RADIUS server that was received without any attributes (severity is **info**).
- **PR_40321** — When a RADIUS authentication fails, the log entry with message ID of 4579 displays the wrong user IP address. The username is displayed correctly.
- **PR_40340** — A trusted administrator is not prevented from adding thousands of RADIUS server entries in the Web browser interface. This large number of RADIUS servers will cause problems when trying to modify RADIUS settings.
- **PR_40352** — Adding a RADIUS server into the TMS zl Module by CLI scripting will fail after a while.

- **PR_40312** — Log messages with message IDs of 609, 618, 629, and 659 are marked as critical but should not be critical. They should be a warning.

```
time="2009-05-08 21:13:47" severity=critical pri=1
fw=ProCurve-TMS-zl-Module id=fw_l2l3_attack msg="FW: udp packet header
length is less than expected, packets dropped" srczone=INTERNAL
src=192.168.70.100 srcport=0 dstzone=ZONE6 dst=192.168.70.100 dstport=0
proto=UDP subfamid=packetheaderanomaly mtype=attack mid=609
```

```
time="2009-05-11 17:32:41" severity=critical pri=1
fw=ProCurve-TMS-zl-Module id=fw_l2l3_attack msg="FW: tcp packet header
length is less than expected, packets dropped" srczone=ZONE1 src=10.1.10.151
srcport=0 dstzone=SELF dst=10.1.10.6 dstport=0 proto=TCP subfamid=packet-
headeranomaly mtype=attack mid=618
```

```
time="2009-05-09 11:06:54" severity=critical pri=1
fw=ProCurve-TMS-zl-Module id=fw_l2l3_attack msg="Excessive number of TCP
connections with Zero bytes detected, possible TCP connect scan. One of the
possible five tuples are captured in this message" srczone=INTERNAL
src=192.168.1.209 srcport=36940 dstzone=EXTERNAL dst=192.168.2.21
dstport=25 proto=TCP subfamid=tcp-ipportscan mtype=attack mid=629
```

```
time="2009-05-08 22:03:53" severity=critical pri=1
fw=ProCurve-TMS-zl-Module id=fw_l2l3_attack msg="FW: protocol value is not
set, packets dropped" srczone=EXTERNAL src=192.168.70.100 srcport=0
dstzone=INTERNAL dst=192.168.70.100 dstport=0 proto=0 subfamid=protocola-
nomaly mtype=attack mid=659
```

- **PR_40662** — Log entries with mid=681 and mid=611 are marked as critical when they should not be considered critical.

```
time="2009-05-17 15:44:53" severity=critical pri=1
fw=ProCurve-TMS-zl-Module id=fw_l2l3_attack msg="NON-ALG traffic, Possible
WinNuke attack detected, packets dropped" srczone=INTERNAL
src=192.168.80.67 srcport=554 dstzone=INTERNAL dst=192.168.70.67
dstport=1029 proto=TCP subfamid=dosattack mtype=attack mid=681
```

```
time="2009-05-17 16:08:38" severity=critical pri=1
fw=ProCurve-TMS-zl-Module id=fw_l2l3_attack msg="FW: packet ip header is
less than expected, packets dropped" srczone=UNKNOWN_ZONE src=0.0.0.0
srcport=0 dstzone=UNKNOWN_ZONE dst=0.0.0.0 dstport=0 proto=0 subf-
amid=packetheaderanomaly mtype=attack mid=611
```

- **PR_40710** — Cannot open /var/log/sysstat/sa18: No such file or directory is erroneously displayed when a TMS zl Module SSH session is opened and the **show tech** command is executed.

Example:

1. Open a SSH session.
2. Run the **show tech** command.

The initial output will show the erroneous output, but the rest of the output is unaffected.

Firewall

- **PR_38165** — When editing a connection reservation, the direction can't be modified.

Example:

1. Go to **Firewall>Settings>Connection Allocations** page.
2. Add a connection reservation. For example:
Zone INTERNAL, direction = inbound, 10.10.40.1, Reservation count = 3
3. Edit the connection reservation added in step 2 and change the direction to **outbound**.
4. Refresh the Connection allocation page. The direction remains after refreshing the page.

The connection allocation must be deleted and recreated to change the direction.

- **PR_39730** — Using the Authenticated Firewall feature, the TMS zl Module could experience an httpd crash on malformed RADIUS packets coming from the trusted RADIUS server on the internal network.
- **PR_40534** — An error message is displayed after applying changes on an attack settings page. This occurs if the user enables the option **Sequence Number Out of range** and sets the ranges with low values, then refreshes the page and clicks the **Apply My changes** button. The page loads slowly and the problem appears to be due to clicking the **Apply My changes** button while the page is loading.

Example:

1. Go to **Firewall -> Settings -> Attack Settings** page
2. Select the option **Sequence Number Out of range**
3. Set as **Range** and **RST Range** the value **10** and check the **Drop packets outside the range**.
4. Click **Apply My Changes** button
5. Refresh the page
6. Immediately click again the **Apply My Changes** button

You now see the error message.

- **PR_40663** — Log entries from the ping-of-death and jolt attacks are missing source and destination zone information. However, the IP addresses are reported.

```
time="2009-05-17 16:06:33" severity=major pri=2 fw=ProCurve-TMS-zl-Module  
id=fw_1213_attack msg="Jolt attack detected" srczone=UNKNOWN_ZONE  
src=192.168.70.67 srcport=0 dstzone=UNKNOWN_ZONE dst=192.016870.1 dstport=0  
proto=UDP subfamid=dosattack mtype=attack mid=1001
```

```
time="2009-05-17 16:06:33" severity=major pri=2 fw=ProCurve-TMS-zl-Module  
id=fw_l2l3_attack msg="PingOfDeath attack detected" srczone=UNKNOWN_ZONE  
src=192.168.70.67 dstzone=UNKNOWN_ZONE dst=192.168.70.1 proto=ICMP subf-  
amid=dosattack mtype=attack mid=1000
```

- **PR_40664** — Even though ICMP Error and ICMP Replay Message are not enabled in Attack Protection, the following log entry is still generated.

```
time="2009-05-17 16:14:42" severity=warning pri=4 fw=ProCurve-TMS-zl-Module  
id=fw_l2l3_attack msg="ICMP:Error message not allowed by firewall"  
srczone=EXTERNAL src=192.168.80.100 dstzone=INTERNAL dst=192.168.70.100  
proto=ICMP icmp-type=3 subfamid=icmppacketanomaly mtype=attack mid=648 icmp-  
code=1
```

- **PR_40665** — Some log entries for ALGs show that the max size has been exceeded, but the max size is not defined. For example:

```
time="2009-05-17 16:17:20" severity=warning pri=4 fw=ProCurve-TMS-zl-Module  
id=fw_l2l3_attack msg="IRC:Size of Message is more than MAX_IRCSIZE"  
srczone=INTERNAL src=192.168.80.100 srcport=39489 dstzone=EXTERNAL  
dst=192.168.70.100 dstport=6667 proto=TCP subfamid=intergritycheck  
mtype=attack mid=118
```

```
time="2009-05-17 16:11:58" severity=warning pri=4 fw=ProCurve-TMS-zl-Module  
id=fw_l2l3_attack msg="TFTP-ALG: Request size length exceeded Max  
size...dropping connection!" srczone=INTERNAL src=192.168.70.67  
srcport=1599 dstzone=SELF dst=192.168.70.1 dstport=69 proto=UDP subf-  
amid=intergritycheck mtype=attack mid=131
```

- **PR_40666** — TMS zl Module reports an entry in the log about being unable to complete firewall processing due to a memory allocation failure, but does not experience any firewall processing problems. For example:

```
time="2009-05-17 14:30:54" severity=minor pri=3 fw=ProCurve-TMS-zl-Module  
id=system_error msg="FW: could not complete firewall processing due to  
memory allocation failure" srczone=EXTERNAL dstzone=INTERNAL error-  
type=memory_allocation subfamid=memoryallocationfailure mtype=syserr  
mid=685
```

IPS

- **PR_38562** — The Port Scan IPS Signature category is listed in the Help file. It should be removed as it describes functionality that is not present.

VPN

- **PR_40354** — When 4893 Internet Key Exchange Security Associations are established, no more IKE responses are generated by the TMS zl Module and no logs reporting this condition are generated.

- **PR_40903** — When an L2TP Policy exists and is disabled, traffic continues passing through the tunnel. The L2TP Policy must be deleted.

Example:

1. Go to **VPN -> IPSec -> L2TP Remote Access**.
2. Add an L2TP Policy.
3. Create access policies.
4. Verify that the traffic gets through the tunnel.
5. Edit the L2TP Policy, uncheck the **Enable this policy** check box.

Traffic gets through the tunnel.

High Availability (HA)

- **PR_38143** — A better description should be added to the log message when the Participant leaves the Active-Standby configuration. The current message is as follows:

```
19:11:44" severity=info pri=6 fw=POSTMR id=hacl_vsrp msg="Detected device  
down" proto=VRRP masterid=2 vsrpstate="MASTER" clusterstatus="Disabled"  
mgmt_ipaddress="10.10.10.200" vsrp_id=4 hastatus="Enabled"  
devicerole="MASTER" deviceid=2 subfamid=vsrpsubfamily mtype=vsrp mid=22076
```

- **PR_38921** — In the High Availability Active-Standby mode, saving and synchronizing in Internet Explorer 7 from the signature page will result in a **Slow Script** dialog being displayed.

Example:

Preconditions:

- IE7 browser
- IPS signatures have been downloaded
- HA A/S has been enabled

1. Go to **IPS>Signatures>View** page and wait until signatures are loaded.
2. Save the configuration and select **Yes** in the Confirm window. The warning message **Stop running this script?** is displayed and the Participant does not synchronize.

As a workaround, synchronize the Participant from another location in the Web Interface.

- **PR_38948** — In an HA environment, should the administrator need to delete the fail-over connections on a participant, they can only delete up to 200,000 connections at a time and not the entire connection list (up to 600,000).

Monitor Mode

- **PR_39263** — The following log messages are shown in Monitor Mode and are not applicable to Monitor Mode: mid=625, mid=626, mid=675, mid=715, mid=1008, and mid=1356.

```
time="2009-04-15 15:59:01" severity=warning pri=4 fw=ProCurve-TMS-zl-Module  
id=fw_l2l3_attack msg="FW: packet with invalid tcp flags found, packets  
dropped" srczone=INTERNAL src=192.168.80.5 srcport=48654 dstzone=INTERNAL  
dst=192.168.80.1 dstport=22 proto=TCP subfamid=packetheaderanomaly  
mtype=attack mid=625
```

```
time="2009-04-15 15:59:02" severity=warning pri=5 fw=ProCurve-TMS-zl-Module  
id=fw_access_control ruleid=10 msg="FW: packet appears after connection is  
closed, packets dropped" srczone=INTERNAL src=192.168.80.5 srcport=48668  
dstzone=INTERNAL dst=192.168.80.1 dstport=22 proto=TCP rcvd=0 rcvdisc=0  
sent=0 sentsc=0 srcnatport=0 destnatport=0 destnatipaddr=0.0.0.0 subf-  
amid=accessdeny mtype=access_control mid=626 srcnatipaddr=0.0.0.0
```

```
time="2009-04-15 16:14:04" severity=warning pri=4 fw=ProCurve-TMS-zl-Module  
id=fw_l2l3_attack msg="TCP: invalid ACK packet, packets dropped"  
srczone=INTERNAL src=192.168.80.5 srcport=60290 dstzone=INTERNAL  
dst=192.168.80.1 dstport=22 proto=TCP subfamid=tcpconnectionanomaly  
mtype=attack mid=675
```

```
time="2009-04-16 17:49:17" severity=minor pri=3 fw=ProCurve-TMS-zl-Module  
id=system_error msg="FW: ICMP echo packets exceeds to maximum limit,  
connection dropped" srczone=UNKNOWN_ZONE dstzone=UNKNOWN_ZONE error-  
type=memory_allocation subfamid=resourceallocationfailure mtype=syserr  
mid=715
```

```
time="2009-04-16 18:08:59" severity=info pri=6 fw=ProCurve-TMS-zl-Module  
id=fw_l2l3_attack msg="Overlapped IP fragment recieved"  
srczone=UNKNOWN_ZONE src=10.29.32.10 dstzone=UNKNOWN_ZONE dst=88.1.10.12  
proto=ICMP subfamid=intergritycheck mtype=attack mid=1008
```

```
time="2009-04-16 18:08:59" severity=critical pri=1  
fw=ProCurve-TMS-zl-Module id=fw_l2l3_attack msg="IP fragment datalength is  
not in units of 8 octets" srczone=UNKNOWN_ZONE src=0.0.0.0 srcport=0  
dstzone=UNKNOWN_ZONE dst=0.0.0.0 dstport=0 proto=0 subfamid=intergritycheck  
mtype=attack mid=1356
```

Release ST.1.0.090213

The following problems are known issues as of release ST.1.0.090213.

- **PR_000000665** — When an IPv4 address is entered into a field, regardless of whether the administrator is using the Web browser interface or CLI interface, the TMS zl Module is not doing the complete validation on the address based upon the field being used. For example, a multicast or broadcast address can be entered into source address fields. It is up to the user to ensure the correctness of the address for the field in question.

Related PRs:

PR_0000000665
PR_0000001794
PR_0000002068
PR_0000002252
PR_0000002253
PR_0000002254
PR_0000002424
PR_0000002613
PR_0000003824

- **PR_0000000906** — When the Web browser interface of the TMS zl Module is left at the login screen without the user logging into the TMS zl Module, the inactivity timer still applies, resulting in the user having to go back to the login screen manually. The inactivity timer should only apply once a user has logged in, but instead applies at all times.
- **PR_0000000961** — The initial login banner text of the Web browser interface in the TMS zl Module differs in size depending on whether the user is accessing it with HTTP or HTTPS. While noticeable, this difference in size does not impair functionality.
- **PR_0000001044** — From the TMS zl Module CLI, when a TMS zl Module is operating in Routing Mode using OSPF, the command **show ip ospf neighbor** has an output that is not the same as a ProCurve switch that is running OSPF. Important information about OSPF neighbors is still shown, how the information that is shown is different from the switch.
- **PR_0000001143** — The options for VLAN IPv4 functionality change depending on how a command is accessed. For example, **vlan <id> ip** options are different than going into the VLAN context via **vlan <id>** and then typing **ip**.

Example:

```
ProCurve Switch(tms-module-D:config)# vlan 20 ip
address          Set IP parameters for communication within an IP network.
igmp             Enable IGMP on the VLAN.
pim-sparse       Enable PIM-SM on the device.
ProCurve Switch(tms-module-D:config)# vlan 20
ProCurve Switch(tms-module-D:vlan-20)# ip
address          Set IP parameters for communication within an IP network.
igmp             Enable IGMP on the VLAN.
rip              Configure RIP on the VLAN.
ospf             Configure OSPF settings.
pim-sparse       Enables PIM-SM on the VLAN.
```

The impact to the user is that some commands cannot be typed in a single line and the VLAN configuration context must be entered in order to configure some items.

- **PR_0000003186** — From the CLI, the schedule command does not auto-complete when the Tab key is pressed as other commands from the command line do.

For example, the following command will not auto-complete to **daily** when the Tab key is pressed after only **dail** is typed:

```
ProCurve Switch(tms-module-D:config)#schedule time1 dail
```

The impact to the user is that the entire parameter must be typed out.

- **PR_0000004155** — The two internal Ethernet ports of the TMS z1 Module have an actual speed of 10Gbps. However, in the SNMP MIB, they are reported as 10Mbps. This issue only affects the reporting of the speed via SNMP. The actual speed is 10Gbps.
- **PR_0000004266** — There is a discrepancy between the Web browser interface and the CLI in regards to how the subnet mask is specified in a static route configuration. The CLI requires the subnet mask to be specified in dotted decimal format while the Web browser interface uses CIDR addresses. No functionality is impacted.
- **PR_0000004577** — When the CLI command **show logging local** is used with paging disabled, extra blank lines are seen. These blank lines should be ignored.
- **PR_0000004766** — When there are multiple syslog servers on the same IP address, differing by facility or port, the user is unable to delete the specific entry in question because only the syslog IP address is used for removing a syslog server. Having more than one syslog server with the same IP address, the syslog server removed will be the first to appear on the list.

Example:

1. Add a syslog server

```
ProCurve Switch(tms-module-D:config)# logging syslog 192.168.1.59 513 facility local0
```

2. Add a second syslog server using the same IP address

```
ProCurve Switch(tms-module-D:config)# logging syslog 192.168.1.59 514 facility local2
```

3. Delete the syslog server

```
ProCurve Switch(tms-module-D:config)# no logging syslog 192.168.1.59
```

The first syslog server is deleted and there is no way to specify the second syslog server except to execute the **no logging syslog 192.168.1.59** command again.

- **PR_0000005390** — The administrator cannot change the password for MD5 authentication on an OSPF interface without knowing the previous password. As a workaround, first disable the VLAN from OSPF and then re-enable it with the new password.

- **PR 0000006127/PR 0000016218** — The output of the **show run** command will show an `FDPoll Returned Error` message, which is not relevant to the output and inconsequential. It can safely be ignored.
- **PR_0000007300/PR_0000007303** — From the CLI, the logging command does not auto-complete when the Tab key is pressed as other commands from the command line do. As a result, the user must fully type the parameter needed.

For example, the following commands do not auto-complete to **enable** when the Tab key is pressed after only **en** is typed:

```
ProCurve Switch(tms-module-D:config)# logging syslog en
ProCurve Switch(tms-module-D:config)# logging snmpv2 en
ProCurve Switch(tms-module-D:config)# logging snmpv3 en
```

- **PR_0000007394** — A vague message is displayed when the maximum number of users have already been added to a group and an administrator attempts to add another user to the group.

```
CLI: Error: Failed to add user group: 88
```

```
Web browser interface: The user could not be added.
```

- **PR_0000007723** — In the TMS zl Module CLI, an error message should be displayed and the entry rejected when an invalid mask value is used for *IP Address/Mask* when specifying an IP address for a VLAN. The user must carefully validate their input.

In the following example the incorrect mask value may result in the wrong subnet mask being used:

```
ProCurve Switch(tms-module-D:config)# vlan 1 ip address 192.168.11.25/2254
Success: Set VLAN 1 IP address to: 192.168.11.25 255.255.252.0
```

- **PR_0000007740** — During a UDP flood, the log incorrectly refers to it as a TCP flood by using `tcpconnectionanomaly`. As a result, the administrator will not know whether a UDP flood is occurring or a TCP flood is occurring.
- **PR_0000007914** — The TMS zl Module Web browser interface is designed to only have one client logged in as **manager** at any given time to avoid one manager's changes overwriting another manager's changes. In most cases, this works as expected. However, multiple clients can log in as manager by following the steps below.
 1. Using the Web browser interface, login as manager on the TMS zl Module.
 2. Connect to the Web browser interface page on a second client.
 3. Login as manager. The TMS zl Module prompts to interrupt current manager, click **cancel**.
 4. This brings up the logout prompt (**Save&Logout, Do Not Save& Logout, Cancel**), click **Cancel**.

Now, the additional client is logged into the Web browser interface as **manager**.

- **PR_000008044** — The TMS zl Module has been configured for VLAN IP addresses and HA is enabled but not configured (that is, there is only one device in the cluster). If HA is subsequently disabled, the VLAN IP addresses are lost. This could result in a loss of management connectivity.
- **PR_000008136** — Only 1,000 NAT Policies are supported on the TMS zl Module. The TMS zl Module incorrectly accepts more than 1,000 NAT policies. These NAT policies work fine, but they should not be used as a future software release may restrict the NAT policies. Please keep the number of NAT policies used to 1,000 or fewer.

- **PR_000008274** — The log entry that is logged when a new access policy is added has the wrong zone information. Refer to the following log sample:

```
time="2008-08-14 10:54:36" severity=info pri=6 fw=ProCurve-TMS-zl-Module  
id=config_configuration ruleid=123 msg="IAPPOL: adding new IA Policy record  
" srczone=SELF dstzone=SELF result=0 throttledcount=20 subfamid=configura-  
tionchanges operation=0 mtype=config mid=697
```

IA Policy refers to an Internet Access Policy, but both zones are indicated as "SELF" which is incorrect.

- **PR_000008428** — Multicast routing is enabled after adding or editing multicast on a VLAN and refreshing the screen. If multicast routing is going to be configured and disabled until a later time, the user should always disable multicast routing as the last step, after configuring **VLAN Settings**.

Example:

1. Launch the TMS zl Module's Web browser interface.
2. Go to the **Network** section.
3. Select the **Routing**.
4. Go to the **Multicast** tab.
5. Under **Multicast Settings**, disable Multicast Routing by unchecking the box next to **Enable multicast routing..** Click the **Apply My Changes** button.
6. Multicast routing is disabled.
7. Add or edit a VLAN with Multicast enabled.
8. Refresh the Multicast page by pressing F5.
9. Multicast routing is now enabled (the box next to **Enable multicast routing..** is checked).

Expected Result: Multicast routing should remain disabled.

- **PR_000009404** — SSH Buffer errors are shown in logs with varying severity. These messages represent temporary and recoverable conditions, but they should all be of the same severity. Example log entries are as follows:

```
time="2008-09-30 22:14:25" severity=warning pri=5 fw=ProCurve-TMS-zl-Module  
id=ssh msg="fatal: buffer_get_string: buffer error"
```

```
time="2008-09-30 22:14:25" severity=info pri=6 fw=ProCurve-TMS-zl-Module  
id=ssh msg="fatal: buffer_get_string: buffer error"
```

```
time="2008-09-30 22:14:25" severity=minor pri=3 fw=ProCurve-TMS-zl-Module  
id=ssh msg="fatal: buffer_get_string: buffer error"
```

- **PR_0000009486** — ICQ ALG does not allow two-way file transfer, but only one-way file transfer. There is no workaround for this issue. An example of the problem is described below:

Using ICQ 5.1., configure the firewall to allow TCP 5190-5193, HTTP, HTTPS and DNS. Chatting between ICQ clients works fine, but when it comes to file transfer, transferring a file from a client on the Internal Zone to the External Zone works, but one cannot transfer a file from a client on the External Zone to the Internal Zone.

- **PR_0000010267** — The TMS zl Module detects the denial of service attack 'jolt2' as 'jolt' and does not detect 'jolt'. This issue is described as follows:

There are 2 mode of operation for jolt2

- Invalidly fragmented ICMP ECHOs (pings)
- Invalidly fragmented UDP packets

The TMS zl Module only detects invalidly fragmented UDP packets and generates a log with mid=1001 with msg="Jolt attack detected". This log message should identify jolt2.

The TMS zl Module does not detect the following:

- Jolt- which sends very large fragmented ICMP packets to a target machine.
- Jolt2- Invalidly fragmented ICMP ECHOs (pings)

- **PR_0000010767** — When using RADIUS authentication, the field **NAS-Identifier** is sent for CHAP and MS-CHAP authentication requests, but not for PAP requests. If any network infrastructure requires the NAS-Identifier field, a user needs to use to CHAP or MS-CHAP at this time.
- **PR_0000011016** — When users are being authenticated by the TMS zl Module and the user accidentally closes the logout window, the user no longer has the ability to explicitly logout. The user must wait for the timeout to occur and then login again or must be explicitly disconnected by the administrator of the TMS zl Module.
- **PR_0000010023** — The TMS zl Module does not log authenticated user logins and logouts. There is no workaround for this issue at this time.
- **PR_0000011190** — When a RADIUS user attempts to login to a TMS zl Module, a log is always generated with Attempted to login with a wrong name despite the user being able to successfully login.

- **PR_0000011703** — When a TMS zl Module is moved between two switch chassis with different configurations, references to VLANs can remain on the OSPF and Multicast pages.

Example:

1. Add several VLANs to the VLAN Associations page.
2. Enable RIP on one of the VLANs just added, for example, VLAN 40.
3. Enable OSPF on the same VLAN, for example, VLAN 40.
4. Enable Multicast on the same VLAN for example, VLAN 40.
5. Save changes.
6. Move the TMS zl Module to another chassis where the VLAN (VLAN 40) used on OSPF, Multicast, and RIP, does not exist.
7. Verify that the information related to that particular VLAN (VLAN 40) is not displayed anymore on the Zone and Routing pages.
8. Save changes.
9. Put the TMS zl Module back to the first chassis and verify that the information associated with the VLAN (VLAN 40) is not displayed here either, since changes were saved on previous chassis.
10. Again add VLAN 40 to the VLAN Association page.

Actual Result: VLAN 40 is displayed on OSPF and Multicast pages.

Expected Result: VLAN 40 should only be displayed on the VLAN Associations page.

- **PR_0000011856** — When using the Web browser interface, an error message is displayed when a valid IP Address is trying to be set in some pages, such as RADIUS, IPsec Policies, and so forth. For example, this may occur when an otherwise valid IP address is added with a final space at the end. As a workaround, be sure there are no white space characters in the IP address. This behavior is seen in Web browser interface fields such as the following:

- RADIUS (server address)
- IKEv1 (local and remote gateway, local and remote Id IPsec Policies (Traffic Selectors))
- GRE (IP Tunnel, local and remote IP, selector IP and MASK)
- SCEP (SCEP server)

- **PR_0000012477** — When logging in as an operator in the Web browser interface, some drop down selections are not disabled. This behavior does not allow an operator to perform any management functions, but the drop down selections should be disabled to prevent the impression that management operations can be performed.

Example:

1. Log in as an operator.

2. Go to **Maintenance > Update Software > Server Type** drop down selection box.
or
Go to **Authentication > RADIUS > Protocol** drop down selection box.

- **PR_0000012250** — In environments where high connection rates and high connection counts are in use, management interfaces can be slow or locked up. This will occur when the administrator has not specified a **Priority VLAN** for management in their configuration. A Priority VLAN ensures that the administrator will always have management access from the specified VLAN.
- **PR_0000012607** — ICMP replay will generate a log entry even when the setting is disabled.
- **PR_0000012802** — When adding an NSSA or STUB area to the OSPF configuration, leading zeros in the area ID are flagged as an error. For instance, **10.10.01.10** would not be accepted but **10.10.1.10** would be accepted.
- **PR_0000012838** — Using SNMP, the values of system name, contact, and location via the RFC 1213 system table cannot be changed.
- ***PR_0000012937*** — In a certain condition, when the TCP RST timeout value is set to zero and IPS is enabled, the TMS zl Module will not forward a TCP RST packet from one peer to another. If there is a TCP session established or half-established between client and server, and the server sends an RST Packet to close the session, the TMS zl Module will mark the session to be deleted. If IPS is enabled, the TMS zl Module will forward the RST packet to IPS. After IPS finishes processing the packet, the TMS zl Module gets the RST packet. Since TMS zl Module has already marked the session to be deleted and the RST timeout value is 0, the RST packet is not forwarded to the peer and is dropped. The problem only happens for RST packets. By setting the RST timeout value to something other than zero, this issue can be avoided.
- ***PR_0000013105*** — When using the **show vlans** command in a CLI session established by going through the switch interface, the VLAN information displayed is overlapped.

Example:

- MGMT VLAN has been added.
DNS Server, default gateway and domain suffix have been added.
1. Open a Web browser interface session.
 2. Go to **Network > Zones > VLAN Associations**.
 3. Add two or three VLAN Associations.
 4. Open a CLI session with the TMS zl Module via the switch,

ProCurve Switch# services d 2
 5. Display VLAN information by using the **show vlans** command.

- **PR_0000013220** — When a software update is performed by retrieving the image via FTP, SCP, or TFTP, a generic error message is displayed for any user input error. For example, if the IP address is incorrect, if the username is wrong, or if the password is wrong, the error message simply indicates a failure and does not call out the specific problem.
- **PR_0000013324** — In the TMS zl Module CLI, the Help text for the copy command needs to be updated. For example, the following command reveals incorrect help text.

```
ProCurve Switch (tms-module-D)# copy ftp image help
```

- **PR_0000013391** — An error is produced when removing VLAN 1 from a TMS zl Module Zone: HPESP: Services zl Module C: unable to create VLAN. Configuration error. To reproduce this, start with a default switch configuration where all TMS zl Module ports are untagged in VLAN 1 by default. Then, from the TMS zl Module's CLI, use a command similar to: **vlan 1 zone external allow-switch-ip**. At this point, type **no vlan 1**. The above error message is displayed in the switch event log.
- **PR_0000013539** — In the TMS zl Module CLI, the software update commands will accept the "\" character and ignore it as input for the username and filename. Therefore, valid usernames or valid filenames that are made invalid by the addition or insertion of a "\" character in their names are accepted as valid because the "\" characters are simply ignored. The software update functionality in the Web browser interface has the same issue.
- **PR_0000013560** — When a user is in a TMS zl Module CLI session and they copy the **startup-config** file to an FTP server when the ALG for FTP is disabled, the copy command appears to hang. After about 60 seconds, the copy command will timeout and the user session can be recovered.

Example:

1. Open a TMS zl Module CLI session.
2. Disable **alg ftpv4**

```
ProCurve Switch (tms-module-D:config)# no alg ftpv4
```

3. Save the **startup-config**

```
ProCurve Switch (tms-module-D:config)#copy startup-config ftp 192.168.1.1  
backup.cfg user administrator
```

4. If prompted, enter the password for the FTP account.

CLI hangs for sixty seconds.

- **PR_0000014561** — An unexpected `group already exists` error may show up when a user deletes a group and then adds a group with the same name again. The TMS zl Module marks groups for deletion, but the actual deletion may take a few seconds. Simply wait a few seconds before adding a group with the same name as a group that was previously deleted and the error will not appear.

- **PR_0000014762** — In the Web browser interface, when the primary and secondary DNS servers' values are cleared, no error is reported, but the secondary DNS server's value is not cleared.
- **PR_0000014783** — When moving a TMS zl Module from one switch to another, DHCP Relay may not start if there is a mismatch in VLAN configuration between the switches. Specifically, if a VLAN is enabled in DHCP Relay and then the TMS zl Module is moved to another switch which doesn't have that VLAN, the DHCP Relay agent doesn't start up and DHCP Relay will not work. When moving a TMS zl Module, if you wish to maintain the TMS zl Module operation, be sure the VLAN information matches before moving the module to another switch.
- **PR_0000014785** — When executing the TMS zl Module CLI command **sh port-trigger <port-trigger_name>** where the *port-trigger-name* does not exist, an error message is displayed `Error: Operation failed` rather than an error message stating that the port does not exist.
- **PR_0000014794** — There is not a one-to-one correspondence between packets processed or dropped and the log entries that are generated - more log messages than necessary are created. The log is correct, it just has more entries than necessary to describe what happened.
- **PR_0000014823** — When adding a VLAN to a zone, the log displays two entries with the exact same message, but containing a different priority. The message describes the routing interface coming up. For example, if **VLAN 50** is added to a zone, the following two log messages are created:

```
time="2008-12-12 13:14:24" severity=warning pri=4 fw=ProCurve-TMS-zl-Module  
id=routing msg="if_rtrup: UP route for interface vlan50  
10.10.10.1/255.255.255"
```

```
time="2008-12-12 13:14:23" severity=warning pri=5 fw=ProCurve-TMS-zl-Module  
id=routing msg="if_rtrup: UP route for interface vlan50  
10.10.10.1/255.255.255"
```

- **PR_0000015081** — When using the Web browser interface for the software update feature, the **Latest Status** field is not automatically refreshed. Refreshing the browser displays the **Latest Status** correctly but also clears the download form. Although no longer needed by the TMS zl Module to perform the software update, the clearing of the download form removes some information from view.
- **PR_0000015153** — When using the TMS zl Module CLI, two commands provide an **insert-at <position>** extended option: **access-policy** and **nat**. There is no error checking on the position number provided - it is assumed that a policy or rule exists at that location. For example, when using **insert-at 1** there must be at least one policy or rule available. There must be a valid policy or rule at the position number for whatever number is specified. If one does not exist, an error is reported, but the zone information is not included in the error message.

- **PR_0000015448** — In the TMS zl Module CLI, when the attempt is made to modify the protocol or port number in a **connection-settings** command, the CLI displays the following message: `Success: Updated connection timeout: <custom name>`, but when the **show connection-settings timeout** command is issued, the protocol or the port number wasn't changed.

Example:

1. Configure at least one custom connection-settings timeout

```
ProCurve Switch (tms-module-D:config)# connection-settings timeout new-ftp tcp 550 10001
```

2. Update the running Custom Timeout with a different protocol and a different port number

```
ProCurve Switch (tms-module-D:config)#connection-settings timeout new-ftp udp 800 10001
```

3. Review the message displayed in the CLI:

```
Success: Updated connection timeout: new-ftp
```

4. Run the command

```
ProCurve Switch (tms-module-D:config)# show connection-settings timeout
```

The protocol and the port number of the custom connection timeout should be updated, but they are not.

- **PR_0000015462** — The VLAN name is not checked for special characters. If a VLAN name is created with special characters, when the VLAN name is displayed in the Web browser interface, problems can occur in the display of the VLAN name. The workaround is to use alphanumeric VLAN names, avoiding spaces and characters such as: @, #, \$, ^, &, *, (, and). To include a blank space in a VLAN name, enclose the name in single or double quotes ('...' or "...").
- **PR_0000015477** — When adding and removing VLANs via the CLI, additional log messages are created that are not created when using the Web browser interface to add and remove VLANs.
- **PR_0000015522** — There is a difference in how the timezone information is displayed in the TMS zl Module as compared to the switch. The TMS zl Module follows the POSIX standard for displaying the time, for example, 'GMT+6' is displayed to indicate the timezone. However, the switch uses a negative number to set the timezone. The time is correctly displayed in both cases, but the process to set the timezone may cause some confusion.

- **PR_0000016231** — Some log entries for warning logs and information logs have messages that are truncated in the log viewer. The most log messages are not truncated and those that contain enough information that a user can tell what they are about. However, the messages have more information in them than can be displayed.
- **PR_0000016539** — When using the TMS zl Module CLI, the **radius-server help** command gives options that are not available.
- **PR_0000016546** — A TMS zl Module that incorrectly has duplicate IP addresses for its VLANs may cause the TMS zl Module SNMP daemon to restart, which may hide the actual problem from a user. While it is incorrect to have duplicate IP addresses, this may occur, and the SNMP daemon restart may send the administrator down the wrong troubleshooting path.
- **PR_0000016812** — When a user incorrectly logs into a TMS zl Module resulting in an authentication failure, if the TMS zl Module is setup to send traps, it will send an authentication failure trap. However, the trap does not contain the user's IP address or the username.
- **PR_0000016892** — When the local log contains more than 10,000 entries, the oldest entries (after the 1,000th entry) are displayed in a wrong position.

Steps to reproduce:

1. Get more than 10,000 entries in the local log
 2. Either export the local log or, in the Web browser interface, set the number of entries per page to 500 and go to page 6.
- **PR_0000018145** — In the Web browser interface, if a VLAN is added with an invalid IP address in the range 224.0.0.0 - 254.255.255.255, an error is returned stating: `VLAN could not be added. Failed to add VLAN IP address, but the VLAN is actually added, but not associated to any zone.` In the CLI, the error message only states: `Error: Failed to set VLAN IP address:`
 - **PR_0000018197** — The Web browser interface Help incorrectly states the number of VLAN associations supported as 21. It should be 19.
 - **PR_0000000999** — In the Web browser interface, **Firewall > Access Policies**, if a user deletes all the rules in an access policy, the Web browser interface doesn't remove the empty policy until a screen refresh is done. This is a visual issue only, the policy has actually been removed.
 - **PR_0000002379** — In the Web browser interface, when adding a Service Object, if the Service Object already exists, an error message is displayed. The error message refers to an Address Object instead of a Service Object.
 - **PR_0000002387** — In the TMS zl Module CLI, when creating a Service Object, the value of zero cannot be set as a protocol number although zero is a valid protocol number.

- **PR_0000002485** — When there are a large number of firewall access policies, the Web browser interface may take some time to load these policies to display to a user. For example, with approximately 2,000 policies, loading them takes about 15 seconds or less. However, when the number of firewall access policies increased, to around 15,000, the time to load the Web page approaches three minutes.
- **PR_0000005580** — When adding an access policy, the administrator is always asked about a source port, which is not applicable for all protocol selections.
- **PR_0000006312** — In the Web browser interface, an invalid error message is displayed when inserting a policy at the first position when no policies exist.

Example:

1. Go to **Firewall > Access Policies > Unicast** page.
2. Select **Add a Policy...**
3. Set the following fields as specified below.
 - Action = Permit Traffic
 - From: = Internal (this field depends on your management zone that was set by the CLI)
 - To: = Self
 - Service, Source and Destination = Any
 - Insert Position: = 1
4. Click the **Apply** button.

Expected result: The access policy should be added in the first position.

Actual Result: An error message is displayed but the policy is added.

- **PR_0000008074** — When a new named object (for example, an Address Object, Service Object, and so on) is added, a log entry is generated referring to an **IPDB record modified**. This simply means that the IP database that keeps track of these things was modified. See the following example log entry:

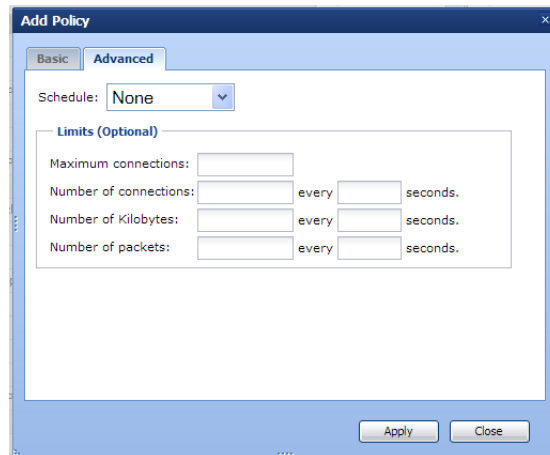
```
time="2008-08-09 18:10:32" severity=info pri=6 fw=ProCurve-TMS-zl-Module  
id=config_configuration ruleid=0 msg="IPDB record modified" srczone=SELF  
dstzone=SELF result=0 throttledcount=0 subfamid=configurationchanges oper-  
ation=0 mtype=config mid=1051 recname=b2222
```

- **PR_0000009711** — When a user authenticates by way of the firewall using RADIUS, they get the correct policy for their group. However, if the policy is changed while the user's session is active, the user is not disconnected automatically to force re-authentication to provide the updated policy. In contrast, a user that is authenticated by way of the Local database is disconnected and must re-authenticate when the policy is updated.

Example:

1. Use username/password to RADIUS Authenticate to the TMS zl Module through the firewall.

2. From a separate management session, delete all access for that user group
 3. The user still has access through firewall
- **PR_0000011874** — On the **Firewall > Access Policy > Unicast** page in the Web browser interface, when adding a policy there is an advanced tab that allows for limit settings.



The valid range for entries in **connections**, **Kilobytes**, **packets**, and **seconds** are not listed. The valid ranges are 1 - 4294967295 for all fields except **Kilobytes**, which is 1 - 4194304.

- **PR_0000012598** — In the Web browser interface, address objects and address groups can be added using the same name. This results in ambiguity when adding an access policy. To prevent such ambiguity, make sure address objects and address groups have unique names. Service objects and service groups also should have unique names.
- **PR_0000015328** — When a DNS object has been created and used in an access policy, if the DNS name cannot be resolved, no further packet processing is done and the packet is dropped. This behavior can cause problems when the DNS server is unavailable. To prevent these problems, minimize the use of DNS objects. If you must use them, be sure to put them towards the end of the list of rules so that other processing can take place on the packet before the attempt to resolve the DNS name is made.
- **PR_0000017344** — In the Web browser interface for the Firewall Access Policy, adding an access policy is done using a dialog. This dialog has drop-down boxes for source and destination zones. These drop-down boxes do not accept **ANY** as a value. However, if you customize the HTTP POST request sent from the browser and modify it to include **ANY** for the zone, it will be accepted.
- **PR_0000018409** — A log entry with **mid=677** is generated for an invalid TCP packet where the flags of RST+ACK are set. This log message indicates that the packet was dropped, but in fact, it was not dropped; it was sent to the TCP peer.

IPS/IDS

- **PR_0000010287** — In the signature file for the TMS zl Module, there are a few mentions of IPv6. This is incorrect. The TMS zl Module is an IPv4 only device.
- **PR_0000018204** — If you filter signatures by severity, then disable a family of signatures, the expected result is that all displayed signatures in that family will be disabled. However, the actual result is that only some of the signatures displayed get disabled. This can be observed by viewing **info** signatures, then disabling the XSS family. When the operation completes, refresh the page, and view **info** signatures. When you inspect the XSS family you will see that not all XSS family **info** signatures are disabled.

VPN

- **PR_0000015755** — When displaying the number of VPN tunnels in the Web browser interface, there may be unnecessary blank pages at the end of the display. All the VPN tunnel information is displayed first, but these unnecessary blank pages appear at the end.
- **PR_0000017972** — In the Web browser interface, in the Help for VPN, the wrong performance numbers are reported.
- **PR_0000038173** — Misleading error messages appear when adding or editing an IKE policy in the Web browser interface (**VPN > Certificates > IPsec Certificates**).
- **PR_0000038217** — When setting up an IPsec policy with a Key Exchange of Manual, it is possible to specify an SPI number that is already in use by another IPsec policy and it would not be detected. Duplicate SPI numbers across IPsec policies are not allowed and an error needs to be displayed.
- **PR_0000038218** — Cannot change a **bypass** or **ignore** policy to **apply** with key exchange method **manual**. Workaround: Delete the policy and add a new one.
- **PR_0000038226** — Changing a **bypass** or **ignore** IPsec policy to **apply** shows an erroneous key exchange method. Workaround: Delete the policy and add a new one.
- **PR_0000038228** — A misleading error occurs when the traffic selector's IP range starts or ends with **255**.
- **PR_0000038229** — IPsec policy advanced settings are displayed incorrectly after the default settings are changed and then edited in the Web browser interface.
- **PR_0000038231** — On the advanced settings screen (**VPN > IPsec > IPsec Policies**) **Enable fragment before IPsec** cannot be disabled.
- **PR_0000038232** — Moving an IPsec policy to another position may not set it in the desired position. Workaround: Delete the policy and add a new one in the correct position.
- **PR_0000038238** — A misleading error occurs when importing an invalid certificate file. Workaround: Import a valid file.

- **PR_0000038240** — Cannot import IPsec Certificates (intermittently fails) from the Web browser interface (**VPN > Certificates > IPsec Certificates**).
- **PR_0000038887** — VPN connections truncate local gateway addresses, preventing a user from seeing all the information for an established tunnel.

High Availability (Active/Standby)

- **PR_0000007372** — From the TMS zl Module CLI, the high-availability command does not accept CIDR notation.

```
ProCurve Switch 5406zl(tms-module-D:config)# high-availability ip 192.168.1.1/24
Invalid input: 192.168.1.1/24
```

- **PR_0000008257** — On the HA configuration page in the Web browser interface, if you change the Multicast IP and then refresh the HA page, you lose your changes. You must save and reboot for the changes to take effect.
- **PR_0000009541** — The switch Web browser interface **config** link directs a user to the HA IP address instead of the TMS zl Module's management IP address.

Example:

There are two TMS zl Modules setup in Active/Standby mode for High Availability

1. Open the switch management Web browser interface
2. Select the **Configuration** tab
3. In the **Device View** page in the Switch Web browser interface press the **Details** link on the TMS Zl Module.

Expected Results: the link should direct the user to the management IP address.

Actual Results: the link directs the user to the High Availability IP address.

- **PR_0000009688** — After an HA link is restored, the TMS zl Module with higher priority does not rejoin the cluster as a Master.

Example:

1. Configure a module in HA as Master (Active) with priority set to 1.
2. Configure a module as Participant (Standby) with priority set to 254.
3. Once both modules are in the cluster, remove the HA link (cable) that connects both switches.

Both devices become Master independently.

4. Re-connect the HA link.

Expected Results: The module with priority set to one (original Mater) becomes Master again.
Actual Results: Device with lower priority joins the cluster as Master and the one with higher priority joins as Participant.

At first glance, this seems to be incorrect, but it is actually done by design. It is assumed that there is something wrong with the module that failed, for example, an intermittent problem. As a result, once the link is rejoined, the module that was Master joins back as a participant (standby) in an attempt to prevent any future issues.

- **PR_0000010844** — When a Participant joins or leaves a cluster, there is very little detail to the log entries describing these important events and these events must be inferred.
- **PR_0000014506** — When an HA configuration is configured for Active/Standby and the Master has IPS enabled and has downloaded the latest signature file, the Participant will not show the correct version of the signature file. The actual signatures are synchronized correctly, but the file name is not.

Example:

Precondition: Master and Participant already on a cluster

1. Download the signatures on the Master.
2. Wait until the Participant reboots and re-joins the cluster.
3. Run **sh ips** command on the Participant.

In the output, the Last Signature Download field appears as None even though the signatures were synchronized.

- **PR_0000014823/0000014916** — When using the TMS zl Module CLI, the **high-availability** command lists a **rebalance** option that is not valid for Active/Standby mode. In the Web browser interface for High Availability, a rebalance button is also present.
- **PR_0000015913** — When using High Availability in Active/Standby mode, if the connection count is high and the connection rate is high, the transfer of TCP state information between the Master and Participant may be too large and it doesn't complete. Once the connection rate or count drops, the state is transferred correctly. However, should a failover from the Master to the Participant occur at the time when TCP state information cannot be sent, there will be an additional failover delay as applications re-establish their TCP state with the Participant (now the Master after the failover).

Monitor Mode Only

- **PR_0000005928** — When in Monitor Mode, a scan of the open ports will reveal TCP port 616 and TCP port 9999 as being open. The only way to block these ports is to setup a firewall access policy to restrict them.

- **PR_000007533** — If the TMS zl Module is in monitor mode, the IDS logs incorrectly show zones **Internal** and **Zone6** in the logs for data and management. These zone references are not correct and should be ignored.
- **PR_0000011929** — When in monitor mode and using the TMS zl Module CLI, if you add an management IP address, the CIDR format of IP-Address/mask is not accepted and you must enter the IP address and Subnet Mask as separate values.
- **PR_0000014582** — In monitor mode, the CLI command **ips help** does not reflect the commands that are actually available in monitor mode as opposed to routing mode.
- **PR_0000015837** — In monitor mode, the management VLAN can be deleted from the switch. In routing Mode, the user is prevented from making this change on the switch.

Example:

Preconditions: monitor mode, management VLAN and management IP address have been set. In this example, the management VLAN is 30.

Delete the management VLAN from the switch CLI.

```
ProCurve Switch (tms-module-D:config)# no vlan 30
```

An error message should be displayed preventing the deletion of the VLAN due to its use by the TMS zl Module. A user is not prevented from performing this action and the VLAN is deleted. As a result, the Web browser interface of the TMS zl Module can't be accessed because the management VLAN has been deleted

- **PR_0000017758** — In monitor mode, when IPS full inspection is turned on and the FTP ALG is turned off, sending an FTP copy of the startup configuration to the network fails with a broken pipe error.



© 2009 Hewlett-Packard Development Company, LP. The information contained herein is subject to change without notice.

June2009
Manual Part Number
'5900-0224