Release Notes *for* Version 06.6.16 of the HP ProCurve Routing Switch 9304M, 9308M, and 6308M-SX, and Switch 6208M-SX Operating Systems

These release notes describe:

- The new operating system enhancement not available in software releases prior to version 06.6.16
- Earlier software operating problems fixed in version 06.6.16.

For release notes describing software releases 06.6.05 and 05.2.16, go to the HP ProCurve website at **http://www.hp.com/go/ProCurve** and click on **Technical Support**, then **Manuals**.

Contents

CLARIFICATION REGARDING DISABLING BGP4, OSPF, OR VRRP 2
CLARIFICATION REGARDING ROUTE ORIGINATION DISABLED BY DEFAULT 2
SOFTWARE RELEASE 06.6.16 3
ALREADY USING A 9304M, 9308M, 6308M-SX, OR 6208M-SX?
HERE'S NEW INFORMATION! 4
NEW FEATURE SUMMARY FOR SOFTWARE RELEASE 06.6.16 4
SOFTWARE IMAGE FILES 5
LOGGING ON 5
ACCESSING A ROUTING SWITCH'S CLI 6
ACCESSING A SWITCH'S CLI 6
ACCESSING THE WEB MANAGEMENT INTERFACE 7
RECOVERING FROM A LOST PASSWORD 7
ENHANCEMENT IN 06.6.16: SECURING MANAGEMENT ACCESS BASED ON VLAN ID 7
SOFTWARE FIXES IN 06.6.16 9

NOTE: Beginning with software release 06.6.05, the software does not have a default read-write SNMP community. If you use the default community name "private" as the password for Web management access, you need to use the CLI to add the read-write community string first.

These notes also contain the following clarifications:

- Clarification regarding what happens when you disable BGP4, OSPF, or VRRP. See "Clarification Regarding Disabling BGP4, OSPF, or VRRP" on page 2.
- Clarification on an OSPF enhancement added in software release 06.6.05. See "Clarification Regarding Route Origination Disabled By Default" on page 2.

Clarification Regarding Disabling BGP4, OSPF, or VRRP

You can easily disable a routing protocol using the CLI or Web management interface. However, be careful when you disable BGP4, OSPF, or VRRP. When you disable these protocols, the routing switch removes all the configuration information for the disabled protocol from the running-config. Moreover, when you save the configuration to the startup-config file after disabling one of these protocols, all the configuration information for the disabled protocol is removed from the startup-config file.

The CLI displays a warning message such as the following:

```
HP9308(config-bgp-router)# no router bgp
router bgp mode now disabled. All bgp config data will be lost when writing to
flash!
```

The Web management interface does not display a warning message.

If you have disabled the protocol but have not yet saved the configuration to the startup-config file, you can restore the configuration information by re-entering the command to enable the protocol (ex: **router bgp**), or by selecting the Web management option to enable the protocol. If you have already saved the configuration to the startup-config file, the information is gone.

If you are testing a BGP4, OSPF, or VRRP configuration and are likely to disable and re-enable the protocol, you might want to make a backup copy of the startup-config file containing the protocol's configuration information. This way, if you remove the configuration information by saving the configuration after disabling the protocol, you can restore the configuration by copying the backup copy of the startup-config file onto the flash memory.

Clarification Regarding Route Origination Disabled By Default

One of the enhancements in software release 06.6.05 was a change in the default behavior for OSPF default route origination. In releases previous to 06.6.05, OSPF default route origination was enabled by default on HP routing switches. The routing switches advertised the default route into the OSPF domain by default.

In software release 06.6.05, OSPF default route origination is disabled by default. Thus, by default HP routing switches do not advertise the default route into the OSPF domain. If you want the routing switch to advertise the OSPF default route, you must explicitly enable default route origination.

When you enable OSPF default route origination, the routing switch advertises the default route into OSPF even if OSPF route redistribution is not enabled, and even if the default route is learned through an IBGP neighbor.

NOTE: In software release 06.6.05 and later, HP routing switches never advertise the OSPF default route, regardless of other configuration parameters, unless you explicitly enable default route origination using the following method.

USING THE CLI

To enable default information originate, enter the following command:

```
HP9308(config-ospf-router)# default-information-originate
```

To again disable the feature, enter the following command:

```
HP9308(config-ospf-router)# no default-information-originate
```

Syntax: [no] default-information-originate [always] [metric <value>] [metric-type <type>]

The **always** parameter advertises the default route regardless of whether the router has a default route. This option is disabled by default.

The **metric** <value> parameter specifies a metric for the default route. If this option is not used, the default metric is used for the route.

The **metric-type** <type> parameter specifies the external link type associated with the default route advertised into the OSPF routing domain. The <type> can be one of the following:

- 1 – Type 1 external route

- 2 – Type 2 external route

If you do not use this option, the default redistribution metric type is used for the route type.

NOTE: If you specify a metric and metric type, the values you specify are used only if the routing switch does not have a default route, but still wants to advertise one because the always option is configured.

USING THE WEB MANAGEMENT INTERFACE

You cannot configure OSPF default information origination using the Web management interface.

Software Release 06.6.16

Software version 06.6.16 and the corresponding 06.*X* product documentation can be downloaded from HP's ProCurve website as described below.

To Download Software Version 06.6.16:

1. Go to HP's ProCurve website at **http://www.hp.com/go/procurve**
2. Click on **Free Software Updates**.
3. Select **Switches download page**.
4. Click on the name of the device for which you are downloading software.

Note: If you are downloading software for a 9304M or 9308M, select the option that matches the type of management module(s) you are using in the device (*with redundant management* or *without redundant management*).

To Download Product Documentation Supporting Software Version 06.*X*:

1. Go to HP's ProCurve website at **http://www.hp.com/go/procurve**
2. Click on **Technical Support**, then **Manuals**.
3. In the resulting display, step through the selections for accessing and viewing the new manuals.
4. On the page listing the manuals, find the new manuals under the heading "**For software version 06.6.05 or greater**".

You will need the Adobe® Acrobat® Reader to view and/or print the manuals. You can also order photocopied, 3-hole punched versions of the new manuals in an 8-1/2 by 11- inch page size and/or the CD-ROM containing PDF files of the manuals. To do so, see the ordering information provided in edition 5 (or later) of the *Read Me First for the HP ProCurve Routing Switches 9304M, 9308M, and 6308M-SX and the HP ProCurve Switch 6208M-SX*. This document is shipped with your HP device and the latest version is also available on the HP ProCurve website. (See steps 1 - 4, above.)

Table 1. Software Download Files for Release 06.6.16

H2R06616.BIN	HP ProCurve Routing Switch 9304M (J4139A) and 9308M (J4138A) *With Redundant Management Module(s)*
HPR06616.BIN	HP ProCurve Routing Switch 9304M (J4139A), 9308M (J4138A), and 6308M-SX (J4840A) *With Non-Redundant Management Module(s)*
HPS06616.BIN	HP ProCurve Switch 6208M-SX (J4841A)

Table 2. Device Compatibility with Software Versions

Device	Supported Software Versions:				
	04791	05084	H2R05216.BIN H2R06605.BIN H2R06616.BIN	HPR05216.BIN HPR06605.BIN HPR06616.BIN	HPS05216.BIN HPS06605.BIN HPS06616.BIN
HP ProCurve Routing Switch 9304M (J4139A) and 9308M (J4138A) *With Redundant Management Module(s)*	*No*	*No*	**Yes**	*No*	*No*
HP ProCurve Routing Switch 9304M (J4139A) and 9308M (J4138A) *With Non-Redundant Management Module*	**Yes**	**Yes**	*No*	**Yes**	*No*
HP ProCurve Routing Switch 6308M-SX (J4840A)	*n/a*	*n/a*	*No*	**Yes**	*No*
HP ProCurve Switch 6208M-SX (J4841A)	*n/a*	*n/a*	*No*	*No*	**Yes**

Note: The flash image files for these software releases differ depending on the product.

If you have a 9304M or 9308M routing switch that was shipped before version 06.6.16 was available, you may want to download this release from HP's ProCurve website. To do so, see "To Download Software Version 06.6.16:" on page 3.

For information on how to update your routing switch software, refer to the chapter titled "Updating Software Images and Configuration Files" in the documentation you received with the device.

Already Using a 9304M, 9308M, 6308M-SX, or 6208M-SX? Here's New Information!

If you received one of the above devices before software release 06.6.16 began shipping, and you are updating the device to release 06.6.16, then you may want to examine the new product manuals that are available beginning with the 06.6.16 release. To view (and freely download) PDF versions of these manuals (chapter-by-chapter files), go to HP's ProCurve website at **http://www.hp.com/go/procurve**, then:

1. Click on **Technical Support**, then **Manual**.
2. In the resulting display, step through the selections for accessing and viewing the new manuals.
3. On the page listing the manuals, find the new manuals under the heading "**For software version 06.6.05 or greater**".

You will need the Adobe® Acrobat® Reader to view and/or print the manuals. You can also order printed versions of either new manual and/or the CD-ROM containing PDF files of both manuals. To do so, see the ordering information provided in edition 5 (or later) of the *Read Me First for the HP ProCurve Routing Switches 9304M, 9308M, and 6308M-SX and the HP ProCurve Switch 6208M-SX*. This document is available on the HP ProCurve website. See "To Download Product Documentation Supporting Software Version 06.X:" on page 3.

New Feature Summary for Software Release 06.6.16

NOTE: Software release 06.6.16 is a maintenance release. See "Software Fixes in 06.6.16" on page 9.

This section summarizes the enhancements in software release 06.6.16.

The enhancement in release 06.6.16 is described in detail in these notes. For details about enhancements in earlier releases, see the release notes for those releases. For release notes describing software releases 06.6.05 and 05.2.16, go to the HP ProCurve website at **http://www.hp.com/go/ProCurve** and click on **Technical Support**, then **Manuals**.

Software release 06.6.16 contains the following system-level enhancement:

Enhancement	Description	See Page
Secure management access based on VLAN ID	You can configure a device to restrict Web, Telnet, SNMP, or TFTP access to devices on ports within a specific port-based VLAN.	7

Software Image Files

To run software release 06.6.16, you need the flash images listed in the following table.

Product	Flash Image
9308M/9304M with Non-Redundant Management Module: • J4140A • J4144A • J4146A	HPR06616.bin
9308M/9304M with Redundant Management Modules: • J4846A • J4845A • J4847A	H2R06616.bin
6308M-SX	HPR06616.bin
6208M-SX	HPS06616.bin (switch-only code)

NOTE: To upgrade redundant management modules in a 9304M or 9308M chassis, use the instructions in the "Using Redundant Management Modules" chapter of *Book 1: Installation and Getting Started Guide*. To get the latest version of this guide, see "To Download Product Documentation Supporting Software Version 06.6.16" on page 3.

NOTE: If you are adding a 1000Base-T module to a 9304M or 9308M chassis you must upgrade to flash image H2R06616 or later (if your are using redundant management modules) or HPR06616 or later (if you are *not using* redundant management modules).

Logging On

You can access an HP device through a direct serial connection to the CLI, through a Telnet connection to the CLI, or through a Web browser.

To access the CLI through a serial connection, attach a straight-through EIA/TIA DB-9 serial cable (M/F) to the management port on the chassis. Then use a terminal emulation application with the following settings to access the CLI:

- Baud: 9600 bps
- Data bits: 8
- Parity: None

- Stop bits: 1
- Flow control: None

NOTE: The serial cable is shipped with your switch or routing switch. If you prefer to build your own cable, see the pinout information in the Installation chapter of *Book 1: Installation and Getting Started Guide*. To get the latest version of this guide, see "To Download Product Documentation Supporting Software Version 06.X:" on page 3.

Accessing a 9304M, 9308M, or 6308M-SX Routing Switch CLI

To access a routing switch's CLI through a Telnet connection, assign an IP address to a router interface attached to the network.

NOTE: This procedure applies only to routing switches. Use the next procedure for switches.

1. Enter the **enable** command at the User EXEC level prompt (for example, `HP9300>`). Then press Enter. (If you are prompted for a password, enter your enable password.)
2. Enter the **erase startup-config** command at the Privileged EXEC level prompt (for example, `HP9300#`), then press Enter. This command erases the factory test configuration if still present.

CAUTION: Use this step only for new systems. If you enter this command on a system you have already configured, the command erases the configuration. If you accidentally do erase the configuration on a configured system, enter the **write memory** command to save the running configuration to the startup-config file.

3. Enter the **configure terminal** command at the Privileged EXEC level prompt. Then press Enter.
4. Enter the following command to access the Interface CONFIG level for the interface:
   int e <*portnum*>, where <*portnum*> is the port number of the interface.
5. Enter the following command to configure the IP address:
   ip address <*ip-addr*> <*ip-mask*>

   NOTE: You also can enter **ip address** <*mask-bits*>.

6. Enter the **write memory** command to save the configuration information to the HP device's flash memory.

NOTE: You will be able to access the routing switch only through this physical interface.

Accessing a 6208M-SX Switch CLI

To access a switch's CLI through a Telnet connection, assign an IP address to the switch as follows.

NOTE: This procedure applies only to switches. Use the procedure above for routing switches.

1. Enter the **enable** command at the User EXEC level prompt (for example, `HP9300>`). Then press Enter. (If you are prompted for a password, enter your enable password.)
2. Enter the **erase startup-config** command at the Privileged EXEC level prompt (for example, `HP9300#`), then press Enter. This command erases the factory test configuration if still present.

CAUTION: Use this step only for new systems. If you enter this command on a system you have already configured, the command erases the configuration. If you accidentally do erase the configuration on a configured system, enter the **write memory** command to save the running configuration to the startup-config file.

3. Enter the **configure terminal** command at the Privileged EXEC level prompt. Then press Enter.
4. Enter the **ip address** <*ip-addr*> <*ip-mask*> command at the device's global CONFIG level prompt (for example, `HP9300(config)#`). Then press Enter.

5. To set a default gateway address (optional), enter the **ip default gateway** <*ip-addr*> command, then press Enter.
6. Enter the **write memory** command to save the configuration information to the HP device's flash memory.

Accessing the Web Management Interface

To access the Web management interface through a Web browser, enter the HP device's IP address in the browser's Location or Address field, then press Enter. When the Login dialog is displayed, enter the default user name and password for read-only or read-write access:

- For read-write access, enter "set" in the User Name field and a valid read-write community string in the Password field. (If this does not work, you have not yet configured the read-write community string using the CLI. Beginning with software release 05.2.16, there is no default read-write community string.) If your device does not yet have an SNMP read-write community string, use the following commands in the CLI to configure one:

```
HP9308# configure terminal
HP9308(config)# snmp-server community <community name> rw
HP9308(config)# exit
```

  where <*community name*> is the SNMP community string you want to use for read/write access.

- For read-only access, enter "get" in the User Name field and "public" in the Password field. (If this does not work, the read-only community name has been changed. Enter the read-only community name configured on the device.)

Recovering from a Lost Password

By default, the CLI does not require passwords. However, if someone has configured a password for the HP device but the password has been lost, you can regain super-user access to the device using the following procedure.

NOTE: Recovery from a lost password requires direct access to the serial port and a system reset.

To recover from a lost password:

1. Start a CLI session over the serial interface to the device.
2. Reboot the device.
3. At the initial boot prompt at system startup, enter **b** to enter the boot monitor mode.
4. Enter **no password** at the prompt. (You cannot abbreviate this command.) This command causes the device to bypass the system password check.
5. Enter **boot system flash primary** at the prompt.
6. After the console prompt reappears, assign a new password.

Enhancement in 06.6.16: Securing Management Access Based on VLAN ID

Software release 06.6.16 allows you to restrict management access to an HP device to ports within a specific port-based VLAN. You can restrict management access individually for the following types of access:

- HTTP (Web management interface)
- Telnet (CLI)
- SNMP (HP TopTools for Hubs & Switches and other SNMP applications)
- TFTP

By default, access is allowed for all the methods listed above on all ports. Once you configure security for a given access method based on VLAN ID, access to the device using that method is restricted to only the ports within the specified VLAN.

VLAN-based access control works in conjunction with other access control methods. For example, suppose you configure an Access Control List (ACL) to permit Telnet access only to specific client IP addresses, and you also configure VLAN-based access control for Telnet access. In this case, the only Telnet clients that can access the device are clients that have one of the IP addresses permitted by the ACL ***and*** are connected to a port that is in a permitted VLAN. Clients who have a permitted IP address but are connected to a port in a VLAN that is not permitted still cannot access the device through Telnet.

Securing HTTP Access

To secure HTTP (Web management) access to clients connected to a specific VLAN, use the following CLI method.

USING THE CLI

To secure HTTP access to a specific VLAN, enter a command such as the following at the global CONFIG level of the CLI:

```
HP9308(config)# web-management enable vlan 10
```

The command in this example configures the device to allow HTTP management access only to clients connected to ports within port-based VLAN 10. Clients connected to ports that are not in VLAN 10 are denied management access.

Syntax: [no] web-management enable vlan <vlan-id>

USING THE WEB MANAGEMENT INTERFACE

You cannot configure VLAN-based access control using the Web management interface.

Securing Telnet Access

To secure HTTP (Web management) access to clients connected to a specific VLAN, use the following CLI method.

USING THE CLI

To secure Telnet access to a specific VLAN, enter a command such as the following at the global CONFIG level of the CLI:

```
HP9308(config)# telnet server enable vlan 10
```

The command in this example configures the device to allow Telnet management access only to clients connected to ports within port-based VLAN 10. Clients connected to ports that are not in VLAN 10 are denied management access.

Syntax: [no] telnet server enable vlan <vlan-id>

USING THE WEB MANAGEMENT INTERFACE

You cannot configure VLAN-based access control using the Web management interface.

Securing SNMP Access

To secure SNMP access to clients connected to a specific VLAN, use the following CLI method.

USING THE CLI

To secure SNMP access to a specific VLAN, enter a command such as the following at the global CONFIG level of the CLI:

```
HP9308(config)# snmp-server enable vlan 40
```

The command in this example configures the device to allow SNMP management access only to clients connected to ports within port-based VLAN 40. Clients connected to ports that are not in VLAN 40 are denied management access.

Syntax: [no] snmp-server enable vlan <vlan-id>

USING THE WEB MANAGEMENT INTERFACE

You cannot configure VLAN-based access control using the Web management interface.

Securing TFTP Access

To secure TFTP access to clients connected to a specific VLAN, use the following CLI method.

USING THE CLI

To secure TFTP access to a specific VLAN, enter a command such as the following at the global CONFIG level of the CLI:

```
HP9308(config)# tftp client enable vlan 40
```

The command in this example configures the device to allow TFTP management access only to clients connected to ports within port-based VLAN 40. Clients connected to ports that are not in VLAN 40 are denied management access.

Syntax: [no] tftp client enable vlan <vlan-id>

USING THE WEB MANAGEMENT INTERFACE

You cannot configure VLAN-based access control using the Web management interface.

Software Fixes in 06.6.16

This section lists the problems that have been fixed in switch and router software releases 06.6.16. For information about fixes in a software release before 06.0.16, see the release notes for that release.

NOTE: Software releases sometimes apply only to specific products. Check the list of products supported by the release to make sure the release applies to your product. Each set of release notes lists the products to which the release applies.

- **ARP table** (9304M and 9308M routing switch only) – In configurations where two 9304M and/or 9308M routing switches were connected together by a trunk group, and the first 9304M or 9308M learned the MAC address of a host connected to the second 9304M or 9308M, the first 9304M or 9308M did not update its ARP table entry for the host, if the host connection was moved from the second 9304M or 9308M to the first 9304M or 9308M .
- **ACLs** (9304M and 9308M routing switch only) – Interfaces on which SRP was running and also ACL entries were configured blocked all outbound TCP packets regardless of the actual filter conditions of the ACL entries.
- **Aging of Layer 4 session entries** (9304M and 9308M routing switch only) – In some cases, a problem in the aging mechanism for Layer 4 session entries could cause the system to reset. This problem generally was associated with ACLs.
- **IP forwarding** – A transit packet with an invalid Router Alert option (with length 0) caused the router to hang.
- **IP forwarding** – The device did not properly send traffic from its IP stack when using an IP default network. This problem did not affect IP transit traffic.
- **IP access policies** (9304M and 9308M only) – When an IP access-policy was configured on an interface, and the IP cache contained a large number of entries, the 9304M or 9308M could be unresponsive for seconds upon learning a new route while flushing IP cache and flow entries.
- **RADIUS** – If multiple users tried to log in to the HP device at the same time, this could cause the HP device to be unable to send RADIUS request packets to the RADIUS server. When this occurred, the problem persisted until the HP device was rebooted.
- **Traceroute** – The HP device did not respond to route traces from some third-party devices to a loopback interface with sub-net mask 255.255.255.255 on an HP device.
- **Trunk ports** – On a pair of trunk ports configured as an IPX interface, if the secondary port in the trunk group became unavailable while it was forwarding traffic for the IPX interface, the traffic did not fail over to the primary port.

- **RIPv1** – RIPv1 did not redistribute static default routes correctly.
- **OSPF** – OSPF protocol update packets whose size was equal to the MTU size were not transmitted properly. This issue did not affect packets of any other size.
- **OSPF** – In some instances, calculation of inter-area routes resulted in regeneration of a summary LSA for routes that actually had not changed since the last summary LSA.
- **OSPF** – If you used the option to set the metric on routes redistributed into OSPF, the software did not apply the new metric. This issue affected static, directly attached, and BGP4 routes redistributed into OSPF.
- **OSPF** – If the routing switch found a lower cost intra-area path for a destination network and the routing switch already had a higher cost intra-area path for the same destination network, the routing switch added the lower cost path as an additional path and treated the two paths as equal cost load sharing paths (with the lower cost). In the current software release, the routing switch adds the lower cost path and discards the higher cost path.
- **BGP4** – If a static route or IGP route to a BGP4 neighbor went away, the BGP4 neighbor session could still remain up, through a BGP4 route to the neighbor learned during the session with the neighbor.
- **BGP4** – In configurations where route redistribution from BGP4 to RIP was enabled, when the software switched from one BGP4 route to another BGP4 route to a given destination, the software withdrew the first route, but then added it again by redistributing it into RIP. The withdrawal of the route caused RIP to give the route a metric of 16 (unreachable), which was followed by another RIP update with the correct metric. When this occurred, some downstream routers held the route down due to the 16 metric.
- **IPX** (9304M or 9308M routing switch only) – In configurations where a stream of IPX traffic (in one interface and out another) was using the same encapsulation type, if an IPX interface with a different encapsulation type was added, the older traffic stream was disrupted, causing the connection to time out. For example, if a device was receiving IPX 802.2 traffic on one interface and forwarding it to another interface using the same encapsulation type, this traffic was disrupted if a third interface using another encapsulation type (example: 802.3) was added.
- **AppleTalk** (9304M or 9308M routing switch only) – The software did not delete cached AppleTalk ARP entries following a Layer 2 topology change.
- **AppleTalk** – The routing switch did not respond to GetMyZone packets, which are used by some AppleTalk devices to obtain their home zones.
- **AppleTalk** – If you deleted a zone, the routing switch did not update zone information to reflect the deletion until you reloaded the software.
- **VRRP** (9304M or 9308M routing switch only) – During heavy traffic loads, the Backup VRRP router sometimes prematurely transitioned to Master, then returned to Backup soon after that due to failing to receive VRRP messages within the dead interval.
- **SRP** – Multiple instances of SRP can be configured without rebooting the routing switch.
- **Multicast** – Removed “router alert option” in IGMP query packets.
- **SNMP and Syslog** – If you disabled a trap, the equivalent Syslog message remained enabled. For example, if you disabled an OSPF trap, the software still sent Syslog messages if the event that initiated the trap occurred, although the software did not send a trap.
- **CLI** – The **show ip** command listed the default value for IP Proxy ARP as disabled but the **show default** command listed the default state for this parameter as enabled. IP Proxy ARP is disabled by default. The **show default** display has been changed to reflect this.
- **CLI** – A **copy** command entered from a Telnet session to copy a file to flash memory appeared to execute successfully, but the **show flash** command listed the file size for the copied file as 0 bytes.

This page is intentionally blank.

HP Part Number: 5969-2351
Edition 1, June 2000