

CUSTOMER RELEASE NOTES

**Vertical Horizon – Patch Release
Gigabit Ethernet Switch
VH-8G
Patch Firmware Version 2.05.09.00
June 16, 2005**

INTRODUCTION:

Enterasys recommends that you thoroughly review this document prior to installing or upgrading this product.

NOTICE: A Patch Release contains a small set of specific feature corrections. It has not been subjected to the same standard of regression testing that a Generally Available Release would be. A Patch Release has been tested only to confirm that the specific feature set is functioning as expected. Unless otherwise stated in the Release Notes, a Patch Release has the same restrictions and limitations as the code upon which it was based. Please read *all* of the Release Notes pertaining to the Generally Available release prior to installation of any Patch in your production network. Please report any undocumented issues you find using the normal technical support procedures found in your product documentation.

The VH-8G is an 8-port Gigabit manageable, standalone switch. The switch provides 8 fixed, 1000Base-SX ports via SC style connectors. Management is built into the switch and is accessible via both in-band and out-of-band management.

Management access is provided in-band via a web interface, Telnet or SNMP, or out of band via the serial console port interface directly or through an attached modem. The imbedded Web agent also provides management capability to any computer on the network via common Http browsers such as Netscape Navigator or Microsoft's Internet Explorer (both browsers should be Version 4.0 or above).

Local Console Management (LCM) allows the user to monitor and configure the VH-8G from a VT-type terminal. LCM can be used to configure features such as SNMP community names and access rights, Port Enable/Disable, firmware downloads, and Device IP address as well as most other parameters. LCM can also provide statistical and diagnostic information about the entire device or an individual port.

Management of the switch is password protected; the same password is used for LCM and for the Web browser interface. Prior to accessing the Management Module via a network connection, a valid IP address, subnet mask, and in some cases a default gateway must be configured using the console interface or the BootP protocol.

The management options provide SNMP, RMON (4 groups: 1, 2, 3, 9), and Web management for system control and statistical monitoring.

The VH-8G switch cannot be used in a stackable configuration; it is a standalone only switch.

FIRMWARE SPECIFICATION:

Status	Version No.	Type	Release Date
Current Version	2.05.09.00	Patch	6/16/2005
Prior Version	2.05.08.01	Patch	6/30/2003
Prior Version	2.05.08	Customer	3/24/2003
Prior Version	2.04.07	Customer	4/23/2001

FIRMWARE CHANGES AND ENHANCEMENTS:

Current Patch Release: 2.05.09.00

The following **known issues** have been fixed in this release of firmware.

Resolved a security vulnerability in prior firmware versions. These firmware revisions contained an internal engineering password used to provide debug access. Knowledge of this password would allow unauthorized access to the switches' internal command line. It is recommended that customers upgrade to this revision.

Debug level commands used for gathering information and making register changes are now restricted to the ADMIN login only.

PRIOR FIRMWARE CHANGES AND ENHANCEMENTS:

The following are known issues or enhancements were outlined in prior releases of firmware. Please refer to the specific release notes of the firmware release for additional information.

Prior Patch Release: 2.05.08.01

The following **known issues** have been fixed in this release of firmware.

Resolved a condition where the timer does not reset after a topology change has been corrected. The system will now reset the 'timesincelasttopologychange' timer after receiving a configuration BPDU with the topology bit flag set to 1.

Resolved a condition where the RMON counters are now retained after resetting them via the system console. This behavior is now consistent with SNMP and WebView.

Prior Firmware Release: 2.05.08

The following **enhancements** have been added in this release of firmware.

The settable parameter configurations for the Vertical Horizon products (VH-8G) may be uploaded (TFTP) from the device and stored for management purposes. The file may be copied (downloaded via TFTP) to the device to restore the saved settings. IP address information will not be overwritten as the file is installed on a device so no loss of management will occur. New, with this firmware revision, is the ability to load the configuration file to other VH-8G devices, with the restrictions below:

- Configuration files can always be saved from, and restored to, the same system.
- On the exact same device, configuration files can be restored to the next higher or next lower firmware revision. This allows configurations to be saved prior to performing code upgrades to products.
- Configurations files can be copied to other systems providing it is running the exact same firmware revision, and it is version 2.05.08 or higher.
- This capability is implemented using TFTP.

Other important notes:

- The management interface IP address parameter information will be maintained on the original system even though a new configuration file is loaded. The IP address information is never overwritten.
- Password information is stored in the saved configuration file. The password information IS written from the saved file into any new device the file is loaded onto. Network managers should change the password information BEFORE uploading and saving the configuration file from a system if this poses any security concern. Configurations copied from one system to another will overwrite the existing password with the one contained in the configuration file. The binary configuration files may not be edited to remove this data as it will corrupt the file checksums.

CUSTOMER RELEASE NOTES

The following **known issues** have been fixed in this release of firmware.

Resolved all known SNMP vulnerability issues have been resolved in this release of firmware. An SNMP trap attack filter was added and padding bytes on all management packets are cleared to prevent eavesdropping on stale buffer data.

Note: During an SNMP attack on this device, using packets directed at the IP address of the switch for prolong periods of time, ICMP and SNMP requests to this device, may be delayed or stopped for 5-15 seconds. Management is restored after the attack ceases.

Resolved a number of minor inconsistencies in the display views have been corrected in this release of firmware as outlined below:

- The Web View GUI properly displays Model name, i.e. VH-8G
- The Web View IGMP Entry is now listed properly in the member port table
- The Web View Port Information screen now correctly reflects the Flow Control Status
- A definition of "ARP Reply Timer" field has been added to Web View help
- The Web View Port Trunk Status is properly displayed

Resolved an issue where the "IfLastChange" MIB has been corrected to properly reflect a port state change.

Resolved an issue where the "ifSpeed" parameter now displays the correct value for the gigabit trunk ports.

Resolved the issue where HP-Openview incorrectly queried the MIB variable "ipNetToMediaPhysAddress" has been corrected.

Resolved the issue where the VH-8G gets into a state where it generates illegal BPDU's (i.e. where the root bridge MAC address is all zeros) has been fixed.

Resolved the condition where IGMP Snooping enabled on the Switch was preventing EIGRP, RIPv2, and VRRP protocols from being transmitted has been fixed.

Resolved an issue where TFTP downloads (code upgrades) will now only reset the VH-8G device **if** the load file is received completely and without errors. The reset occurs after the image is loaded into flash memory. Load re-tries, because of network errors, can now be made without waiting for the device reset to occur.

Resolved an issue to protect the management agent from excessive levels of broadcast traffic from all ports, the VH-8G management agent, when overwhelmed, will drop all broadcast traffic directed to it for periods of time. Under these certain conditions, the switch agent will send unsolicited ARPs (Gratuitous ARPs) to each VLAN configured on the switch. This behavior is not detrimental to network operation and ensures that network management communication to the VH-8G management agent will not be lost for new connections to the agent. The mechanism runs independently of any broadcast control capability on the switch.

Tuning parameters have been added and are stored in NVRAM. If Gratuitous ARP functionality is enabled, refer to the sample configuration screen in these release notes for set up information.

Refer to the Enterasys Support knowledge base: <http://knowledgebase.enterasys.com/support>, document ent12303 for more information regarding Gratuitous ARP configuration and use.

Resolved a condition where slow response or intermittent loss of communication with the management agent has been seen (cause listed above).

Resolved an issue causing a loss of manageability condition (ping, SNMP, telnet requests) when a VRRP master router fails-over to another backup router has been corrected

Prior Firmware Release: 2.04.07

The following **known issue** has been fixed in this release of firmware.

Resolved a condition so that the VH-8G now supports any standards-based console management cable. Version 1.05 microcode must be present in the VH-8G along with firmware version 2.04.07 or higher support all cables.

CUSTOMER RELEASE NOTES

KNOWN RESTRICTIONS AND LIMITATIONS:

When the speed of a Gigabit port is changed from a specific speed to auto-negotiate mode, the user must disconnect and reconnect the cable to cause auto-negotiation to occur.

Gigabit ports used for trunks, or as part of any redundant paths in the network, should always be set to auto-negotiate. If a failure occurs in only one path of the link (i.e. the receive path), the failure to pass the auto-negotiation at both ends of the link will ensure the entire link (both directions) is down, and allow the alternate path to assume the traffic rather than leaving the network with a path only having one way connectivity.

The switch defaults to Shared VLAN (SVL) MAC address learning. As a result, when there are duplicate addresses in different VLANs, packets with these addresses will be forwarded between those VLANs. The user may select IVL mode, to prevent inter-VLAN forwarding of those duplicate addresses.

When a port is in the Spanning Tree Blocking state, incoming packets will continue to be counted in its RMON counters.

When packets originated from the VH management agent are transmitted out a mirror port, they will not have a CRC attached.

When a combination of high and low priority traffic is transmitted from a high speed port to a lower speed port, some high priority packets may be dropped.

When Fast STA is disabled, the configuration count increases by one when a port transitions from a "NO LINK" state to a "BLOCKED" state.

Do not put clients trunk (link aggregation) ports, partial connectivity may result for these clients.

Due to a chip limitation, the VH-8G does not support "Admit Only VLAN-tagged frames."

The Root Port Cost on a Trunk will change back to the Default Port Cost (i.e. 4) after a respan or a reboot of the VH-8G.

If a Static Router port is configured on a multi-port trunk (link aggregation group), it may not be saved following a reboot of the VH-8G. Note: Static Router ports on other ports are not lost after a reboot.

Under high broadcast loads, the VH-8G implements internal mechanisms to limit broadcast and multicast traffic to the Management Agent. This filtering of traffic to the CPU may cause the CPU not to see the IGMP streams for a group for which no "join" messages have been received. The outcome of this event is flooding of the multicast stream until either a "Join" (or "Leave") message is received or until the broadcast and multicast traffic is reduced to a small enough level that the Management Agent can process all of them.

Upon Enabling and Disabling Fast Forwarding and then selecting Apply within WebView, the following incorrect "Pop-Up" Message will be displayed:

"Path Cost is out of Range"

Note: The user will have to acknowledge the "Pop-Up" Message 1-3 times. Even though the message is displayed, Fast Forwarding is "Enabled" and "Disabled" correctly.

In the Local Console within the SNMP Configuration View - IP trap manager settings menu, a blank menu selection will perform a delete function, i.e. the delete option field is shown blank.

Local Console "Reset Counters" Option fails to clear RMON MIB OIDs and WebView RMON Port Statistics.

Note: The user will have to "Reset" the VH-8G in order to clear RMON MIB OIDs and WebView RMON Port Statistics.

A HyperTerminal Session will not open on the VH-8G if it receives 5 positive volts on pin 3 on the console port while the device is booting.

Note: VH-8G will boot properly with no HyperTerminal session open on the console port but attempts to open a HyperTerminal Session upon completion of switch initialization will fail.

If VH-8G HyperTerminal Session already open prior & during the VH-8G boot process, access to the HyperTerminal Session operates as expected.

CUSTOMER RELEASE NOTES

Loading previous versions of code (back-revving) from V 02.05.08 to any previous VH-8G firmware image will change the following configuration settings:

- Aging Time set to 17104898 from 300.
- Default Ingress User Priority for Ports 5-8 set to 1 from 0.

Any problems other than those listed above should be reported to our Technical Support Staff.

GLOBAL SUPPORT:

By Phone: (603) 332-9400

1-800-872-8440 (toll-free in U.S. and Canada)

For the Enterasys Networks Support toll-free number in your country:

<http://www.enterasys.com/support/gtac-all.html>

By Email: Support@enterasys.com

By Web: <http://www.enterasys.com/support>

By Fax: (603) 337-3075

By Mail: Enterasys Networks, Inc.
35 Industrial Way
P.O. Box 5005
Rochester, NH 03866

For information regarding the latest software available, recent release note revisions, or if you require additional assistance, please visit the Enterasys Networks Support web site.