

CUSTOMER RELEASE NOTES**Vertical Horizon – Patch Release
VH-4802
Firmware Version 02.05.05.09
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-4802 is a 48 port dual-speed manageable standalone switch. The switch provides 48 10Base-T/100Base-TX ports, plus two rear-panel slots for optional slide-in dual 100Base-FX, 1000Base-SX or 1000Base-LX modules.

Management access is provided in-band via Telnet or SNMP; or out of band via the serial console port interface (either directly or through an attached modem). An embedded 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-4802 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 an out of band connection or the BootP protocol. The management option provides SNMP, RMON (4 groups: 1, 2, 3, and 9), and Web management for system control and statistical monitoring.

FIRMWARE SPECIFICATION:

| Status | Version No. | Type | Release Date |
|-----------------|-------------|----------------|--------------|
| Current Version | 2.05.05.09 | Customer Patch | 6/16/2005 |
| Prior Version | 2.05.05.07 | Customer Patch | 4/29/2004 |
| Prior Version | 2.05.05.02 | Customer Patch | 10/31/2003 |
| Prior Version | 2.05.05.01 | Customer Patch | 6/20/2003 |
| Prior Version | 2.05.05 | Customer | 1/14/2003 |
| Prior Version | 2.05.00 | Customer | 2/08/2002 |

CUSTOMER RELEASE NOTES

HARDWARE COMPATIBILITY:

ALL

BOOTPROM COMPATIBILITY:

ALL

NETWORK MANAGEMENT SOFTWARE SUPPORT:

ALL

SUPPORTED FUNCTIONALITY:

| Features | Support |
|--|---------|
| 802.1P - Traffic Management | Yes |
| 802.1Q - VLAN tagging and identification (256 VLANs supported) | Yes |
| Spanning Tree support | Yes |
| IGMP Snooping | Yes |
| Address Data Base Maintenance | Yes |
| Local Management via TELNET | Yes |
| RMON Groups 1,2,3,9 | Yes |
| Runtime Address Discovery | Yes |
| BOOTP protocol support | Yes |
| TFTP download from a host support | Yes |
| Broadcast Storm Protection | Yes |
| Trunking | Yes |
| SNMP | Yes |
| Modem support | Yes |
| Imbedded Http Agent | Yes |
| Port Mirroring | Yes |
| Auto-Negotiation | Yes |
| RPU support | Yes |
| Configuration upload/download support | Yes |
| Port Security (MAC Locking) | Yes |

INSTALLATION AND CONFIGURATION NOTES:

None

CUSTOMER RELEASE NOTES

FIRMWARE CHANGES AND ENHANCEMENTS:

Current Patch Release: 2.05.05.09

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. |

KNOWN RESTRICTIONS AND LIMITATIONS:

| |
|---|
| When the speed of a Gigabit port is changed from a specific mode to auto-negotiate mode, the user must disconnect and reconnect the cable to cause auto-negotiation to occur. Gigabit ports should always be set to auto-negotiate mode to insure both ends of a link are aware of failure which might otherwise only affect traffic in a single direction. |
| When Gigabit interfaces are installed and configured for Trunking, they must be alike, i.e., same type of Gigabit interface used at both ends of the Trunk. |
| When a port is in the Spanning Tree Blocking state, incoming packets will continue to be counted in its RMON counters. |
| When packets that originate at the CPU are transmitted out a mirror target port, they will have no CRC. |
| When Fast STA is disabled, the configuration count increases by one when a port transitions from a "NO LINK" state to a "BLOCKED" state. |
| Clients should not be attached to trunk ports. |
| Configuration parameters are not retained when downgrading to a lesser image from version 2.04.01. |

PRIOR FIRMWARE CHANGES AND ENHANCEMENTS:

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

Prior Firmware Release: 2.05.05.07

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

| |
|---|
| Resolved a condition where an HTTP packet with the same source IP address as the switch IP address would cause the switch to stop responding. |
| Resolved a condition where a negative length HTTP packet would cause the switch to stop responding. |
| Resolved a condition where a high rate of HTTP frames would cause SNMP failure to the switch. |
| Resolved a condition where a "negotiate authorization frame" would cause the switch to stop responding. |

CUSTOMER RELEASE NOTES

Prior Firmware Release: 2.05.05.02

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

Resolved a condition where previous versions of code did not allow learning of the MAC address if the port was not in management VLAN. With patch release 2.05.05.02, this is now properly handled.

Prior Firmware Release: 2.05.05.01

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

PRIOR FIRMWARE CHANGES AND ENHANCEMENTS:

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

Prior Firmware Release: 2.05.05

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

Resolved an issue with SNMP vulnerability by adding an SNMP trap attack filter.

Resolved an issue to prevent Local Management from allowing the user to toggle GVRP selection. It is set to disable by default. GVRP was not, and is not a supported feature.

Resolved an issue where uploaded configuration files previously could not be ported from one VH switch to another switch. It has been noticed that the parameter "Broadcast Suppression" still sometimes fails to port. All other parameters port OK.

Resolved an issue where detection was added for using IBM Type 1 configured cabling.

Resolved a condition resulting in a random loss of SNMP, PING, Telnet has been resolved.

Resolved an issue where the VH-4802 gets into a state where it generates illegal BPDUs (i.e., where the root bridge MAC address is all zeros) has been fixed.

Resolved an issue to protect the management agent (loss of management issue) from excessive levels of broadcast traffic from all ports, the VH-4802 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 Arp) to each VLAN configured on the switch. This behavior is not detrimental to network operation and ensures that network management communication to the VH-4802 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 setup information.

Refer to the Enterasys Support knowledgebase: [http://knowledgebase.enterasys.com/support, document ent12303](http://knowledgebase.enterasys.com/support/document/ent12303) for more information regarding Gratuitous Arp configuration and use.

Prior Firmware Release: 2.05.00

| |
|---|
| Resolved a condition that has been occasionally seen in the VH-4802 causing the units to randomly reset. |
| Resolved a condition that has been occasionally seen in the VH-4802 causing <u>all ports</u> to enter a non-forwarding state. All packets that are transmitted into any port(s) on the switch are counted as dropped. |
| Resolved a condition that could be seen in networks with high rates of varied types of broadcast traffic. This caused the units to enter a port lock up state. During this state, <u>some ports</u> would stop forwarding traffic and others would not. |
| Resolved a condition in which a User enters in two additional Local Management user names with passwords and then removes these entries; the User could still get into the LM with one of the user names with the password of the other user name. |
| Resolved a condition in which the "ifName" OID value was not equivalent to the "ifDescr" OID value. (i.e., VH Interface Description). |
| Resolved an issue to add support for a reduced boot up time when the system(s) is warm restarted. When restarting the system, select 'NO POST' from the console for faster system boot up. This enhancement enables the VH-4802 to bypass the internal diagnostics (POST) during a system restart. The boot time is reduced from approximately 210 seconds to 90 seconds. |
| Resolved an issue where HTTP POST packets will no longer cause the switch to lock up and unwanted HTTP POST packets will be dropped. |
| Resolved an issue where Auto-Negotiation on the VHIM1000-S1SX uplink module has been changed to address the link-up issues that could occur when two Vertical Horizon switches containing interconnected VHIM1000-S1SX modules are powered up simultaneously. |
| Resolved an issue where support for the VHIM1000-S1TX 1000Base-T uplink module has been added. |
| Resolved an issue where broadcast Storm Protection (previously Broadcast Strom Control) has been changed to reflect the following: The user-selectable Threshold setting is now between 100 and 141,000 pps in increments of 100. The default is 200 pps. The user-selectable Average Intervals are 200 ms, 500 ms, 1 sec, 5 sec and 10 sec. The default is 1sec. This new algorithm ensures that high rates of broadcast traffic will not hinder the operation on the system(s). |
| Resolved an issue where a new UI for VLAN configuration has been added in this release of firmware. Please refer to the section titled New Local Management Console Menu Items in this release note. |
| Resolved an issue where PING response time has been enhanced. The VH-4802 operating system ensures higher priority tasks such as NVRAM Updates or Address Monitoring (i.e., Spanning Tree) take precedence over PING. This ensures the system(s) will remain operational. |
| Resolved an issue where the transmission rate of Layer 3 packets increases, the rate at which reports are forwarded out the router port decreases. As the rate of Layer 3 packets increases, the forwarding of joins decreases. |
| Resolved an issue where Multicast addresses 01-80-C2-00-00-02 through 01-80-C2-00-00-15 were dropped when Spanning Tree was enabled. |

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

NEW LOCAL MANAGEMENT CONSOLE MENU ITEMS:

Configuring Management Access

Use the Management Configuration menu to define which VLAN(s) has management access to the switch. Parameters shown on this screen are indicated in the following figure and table.

| |
|--|
| <p>Management Configuration</p> <p>Vertical Horizon Local Management – VH-4802 Management Configuration</p> <p>Management VLAN : ALL</p> <p>VLAN : 1</p> <p>Arp reply timer: 1</p> <p><APPLY> <OK> <CANCEL></p> |
|--|

Use <TAB> or arrow keys to move, <Space> to scroll options.

Parameter Description

Management VLAN Select ALL to give all VLANs access to switch management, or ONE to restrict access to a specified VLAN. If you select just one VLAN, you must specify its VLAN ID on the following line. VLAN Specifies the VLAN ID that has access to switch management.

Arp Reply Timer configures the frequency, in seconds, at which Gratuitous Arps are sent out. A value of 99 used to stop sending the Gratuitous Arps completely. Otherwise use a range of 1 – 30 seconds.

COMPLIANCE SUPPORT:

| Compliance Level | Compliant |
|------------------|-----------|
| Year 2000 | YES* |

Known Anomalies: None.

IEEE STANDARDS SUPPORT:

| Standard | Title |
|-------------|--|
| IEEE 802.1D | Transparent Bridging Specifications (ISO/IEC 10038) |
| IEEE 802.1p | Traffic Class Expediting and Dynamic Multicast Filtering |
| IEEE 802.1Q | Virtual Bridged Local Area Networks |
| IEEE 802.2 | Local Area Networks, Logical Link Control (LLC) |
| IEEE 802.3 | CSMA/CD 9 (ISO/IEC 8802-3) |
| IEEE 802.3I | 10Base-T (ISO/IEC 8802-3, clause 14) |
| IEEE 802.3u | 100Base-TX (ISO/IEC 8802-3, clause 25) |
| IEEE 802.3u | 100Base-FX (ISO/IEC 8802-3, clause 26) |
| IEEE 802.3x | Flow Control |
| IEEE 802.3z | 1000Base-SX, 1000Base-LX |

CUSTOMER RELEASE NOTES

IETF STANDARDS MIB SUPPORT:

| RFC No. | Title | Groups Supported |
|---------------------------|---|--|
| 1157 | Simple Network Management Protocol(SNMP) | |
| 1213 | MIB-II | System, Interfaces, IP, ICMP, UDP, Transmission (dot3), and SNMP |
| 1493 | Bridge MIB | Spanning Tree and various managed objects for bridges |
| 2863 (superceded 1573) | Interfaces Evolution MIB | MIB-II Interfaces Group extensions |
| 1643 | Ethernet-like | Various Ethernet specific aspects |
| 1757 | RMON MIB | Statistics, History, Alarm, and Event |
| 2674 | Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering and Virtual LAN Extensions | <p>Groups in the P-BRIDGE MIB</p> <p>-----</p> <pre>dot1dExtBase OBJECT IDENTIFIER ::= { pBridgeMIBObjects 1 } dot1dPriority OBJECT IDENTIFIER ::= { pBridgeMIBObjects 2 }</pre> <p>Groups in the Q-BRIDGE MIB</p> <p>-----</p> <pre>dot1qBase OBJECT IDENTIFIER ::= { qBridgeMIBObjects 1 } dot1qTp OBJECT IDENTIFIER ::= { qBridgeMIBObjects 2 } dot1qStatic OBJECT IDENTIFIER ::= { qBridgeMIBObjects 3 } dot1qVlan OBJECT IDENTIFIER ::= { qBridgeMIBObjects 4 }</pre> |

ENTERASYS PRIVATE ENTERPRISE MIB SUPPORT:

| Title | Version |
|------------|----------|
| ELS100.MIB | 01.00.00 |

Enterasys Private Enterprise MIBs are available in ASN.1 format from the Enterasys web site at: <http://www.enterasys.com/support/mibs/> . Indexed MIB documentation is also available.

SNMP TRAP SUPPORT:

| RFC No. | Title |
|---------------------------|--|
| RFC 1215 | coldStart_trap linkUp_trap authenticationFailure_trap |
| RFC 1493 | ENTERPRISE dot1dBridge NewRoot 1 topologyChange 2 |
| 2863 (superceded 1573) | SnmpTraps linkDown 3 LinkUp 4 |
| RFC 1757 | IETF RMON, ENTERPRISE rmon -- 1.3.6.1.2.1.16 risingAlarm 1 fallingAlarm 2 |

ENTERASYS PRIVATE ENTERPRISE TRAP SUPPORT:

NONE

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.comBy 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.