

**CUSTOMER RELEASE NOTES****Matrix E7 Series  
SmartSwitch 2000/6000 Series  
Firmware Version 5.06.04  
November 2003****INTRODUCTION:**

This document provides specific information for version 5.06.04 of firmware for the 2<sup>nd</sup> and 3<sup>rd</sup> generation modules, which may be installed in either the Matrix E7 or SmartSwitch 6000 chassis, and for the 2<sup>nd</sup> generation SmartSwitch 2000 standalone modules listed below. SecureFast Switching is not supported in this release. The following hardware platforms are supported by this firmware release:

2E253-49R	2H252-25R	2H253-25R	2H258-17R
6E233-49	6H202-24	6H203-24	2H252-25RDC
6H253-13	6H258-17	6H259-17	6H252-17
6H262-18	6H302-48*	6H303-48	6G306-06
6H352-25	6H308-24	6H308-48	6E308-24
6E308-48	6G302-06		

\*There are restrictions on the version of firmware required for 6H302-48 modules with a serial number starting with **3655xxxxxx**. The serial number is visible on the top ejector tab of the switch, or by querying the PIC MIB. For firmware in the 5.x track, version **5.03.05** or higher must be used on 6H302-48 modules with a serial number starting with 3655. For the 4.x firmware track, **4.08.41** or higher must be used on 6H302-48 modules with a serial number starting with 3655.

**It is recommended that one thoroughly review this release note prior to the installation or upgrade of this product. This firmware release incorporates new features and functionality that should be understood before upgrading.**

**FIRMWARE SPECIFICATION:**

Status	Version No.	Type	Release Date
Current Version	5.06.04	Web Release	November 2003
Previous Version	5.05.05	Web Release	April 2003
Previous Version	5.04.09	Web Release	August 2002
Previous Version	5.03.08	Web Patch Release	July 2002
Previous Version	5.03.05	Web Release	April 2002
Previous Version	5.02.03	Web Release	January 2002
Previous Version	5.01.33	Web Release	September 2001

**HARDWARE COMPATIBILITY:**

This version of firmware is supported on all Hardware revisions.

**BOOT PROM COMPATIBILITY:**

This version of firmware supports all Boot PROM versions.

**CUSTOMER RELEASE NOTES****NETWORK MANAGEMENT SOFTWARE SUPPORT:**

<b>NMS Platform</b>	<b>Version No.</b>	<b>Module No.</b>
NetSight Atlas Console	1.2	N/A
NetSight Atlas Console Lite	1.2	N/A
NetSight Atlas Inventory Manager	1.2	N/A
NetSight Atlas Policy Manager	1.6	N/A

If you install this image, you may not have control of all of the latest features of this product until the next version(s) of network management software. Please review the software release notes for your specific network management platform for details.

**SUPPORTED FUNCTIONALITY:**

<b>Features Summary</b>
802.1X Port Based Network Access Control with RADIUS
MAC Locking and MAC Authentication
Port Web Authentication
Per VLAN Spanning Tree (PVST)
IEEE 802.1w Rapid Reconfiguration of Spanning Tree
SMON
3 <sup>rd</sup> Generation Module Proxy Function for Matrix E7 modules
Multi-Layer Frame Classification
IGMP v1/v2 Support
IEEE 802.1D/Q bridging
Support for the following HSIMs: HSIM-A6DP*      HSIM-F6 HSIM-FE6      HSIM-G09* HSIM-G01*      HSIM-W84 HSIM-W6      HSIM-W85 HSIM-SSA710*      HSIM-W87 HSIM-SSR600*
Support for the following VHSIMs: VHSIM-G6 VHSIM-G02 VHSIM-A6DP* VHSIM2-A6DP
Port Mirroring
RMON (9 groups)
IEEE 802.3ad Link aggregation
Web Management (WebView)
Rate Limiting

\*These modules are not supported when installed in a 6H352-25.

**CUSTOMER RELEASE NOTES****INSTALLATION AND CONFIGURATION NOTES:**

In general, the product will be shipped to you pre-configured with this version of firmware. If you would like to upgrade an existing product, please follow the TFTP download instructions that are included in your User's Guide. TFTP download instructions are also available on the Enterasys Networks' Support web site at:

<http://www.enterasys.com/support/techtips/tk0020-9.html>

Product manuals are available on the Enterasys Networks web site: <http://www.enterasys.com/support/manuals>

If you are downloading this firmware to a module or modules operating in Distributed Chassis Management mode within a SmartSwitch 6000\*, and you wish to use the chassis IP address, you must be connected to one of the front panel ports of the module you are downloading. In order to download to the chassis IP address, the community name string must include the slot number. For example, to download a module in slot one, a community name of *public.1* would be used (assuming the super-user community name was *public*). Non-Runtime downloads to the chassis IP address are not allowed. Please consult your user's guide for more details on performing firmware downloads.

Modules running this firmware version default to Distributed Chassis Management mode when installed into a SmartSwitch 6000\*. An individual IP address does not need to be assigned to each module if a chassis IP address has been assigned. The management mode field in the General Configuration Screen of Local Management allows a user to select whether a module will operate in Distributed or Standalone mode. Changing this value will cause the module to reboot.

*\* Distributed Chassis Management (DCM) is not supported on the Matrix E7 chassis.*

**Module Generations and Chassis Definitions**

Part #	Description
6C107	7-slot Matrix E7 chassis
6C105	5-slot SmartSwitch 6000 chassis
6X1XX	1 <sup>st</sup> generation module, SmartSwitch 6000 family
6X2XX	2 <sup>nd</sup> generation module, SmartSwitch 6000 family
6X3XX	3 <sup>rd</sup> generation module, SmartSwitch 6000/Matrix E7 family
2X2XX	2 <sup>nd</sup> generation standalone switch, SmartSwitch 2000 family

Note: where X is a wildcard

The second and third generation modules default to an 802.1Q operational mode. In order for the modules to maintain backward compatibility with first generation SmartSwitch 6000 modules, which default to an 802.1D operational mode, the backplane ports do not insert an 802.1Q Frame Tag when forwarding traffic to other modules. If 802.1Q VLANs are configured on modules, then the backplane ports will need to be configured by the user as 802.1Q tagged ports for all second generation modules. The first generation modules automatically configure their backplane ports as 802.1Q when changed from the default operational mode to the 802.1Q VLAN mode.

**CUSTOMER RELEASE NOTES****SmartTrunk**

This version of firmware supports SmartTrunk, Enterasys' Link Aggregation feature. Below is a matrix that details the other SmartSwitch platforms and the firmware versions required to operate properly with this version of firmware.

Product Line	Firmware Version Required
First Generation SmartSwitch 2000/6000	4.05.09 or higher
SmartSwitch 9000 9X5XX series	1.01.10 or higher
SmartSwitch 9000 9X4XX series	1.11.08 or higher
SmartSwitch Router (SSR-2000, 8000, and 8600)	2.0 or higher

**SmartTrunk with Non-Enterasys Products**

SmartTrunk has been successfully tested with some other vendor's Link Aggregation methods. It is usually necessary to disable the SmartTrunk link protocol for proper operation. This is configurable in the SmartTrunk Local Management screen. When the SmartTrunk link protocol is disabled, some of the automated configuration protection is lost. Users must be very careful to observe the SmartTrunk configuration rules detailed in the *SmartTrunk User's Guide*. Failure to follow these configuration rules could result in unstable network operation. This guide is available at: <http://www.enterasys.com/support/manuals>.

**SecureFast**

This image does not support SecureFast switching.

**Cabletron Discovery Protocol**

By default the SmartSwitch products periodically transmit multicast CDP frames, these frames are used by network management products, and other switches to discover the topology of the network. CDP frames are sent by the switches using a multicast destination address of 01-00-1d-00-00-00. This feature can be disabled using the CDP command in Local Management.

**System Interface Numbering**

The System interfaces are numbered by MIB II as shown:

- 1 - Front Panel switch port 1 interface
- 2 - Front Panel switch port 2 interface
- 3 - Front Panel switch port 3 interface
- ...
- n - Last Front Panel switch port 'n' interface
- n+1 - FTM1 slot/port 1 switch interface
- n+2 - FTM1 slot/port 2 switch interface
- n+6 - FTM1 slot/port 6 switch interface
- n+7 - Host in-band management interface
- n+8 - SmartTrunk group 1
- ...
- n+13 - SmartTrunk group 6

**CUSTOMER RELEASE NOTES****Source Address Table**

The default size of Source Address Table (SAT) has been changed from 16,000 entries to 8,000 entries. The SAT size can be changed back to 16000 entries; however, the number of classification entries allowed is reduced. With the SAT size set to 8000 entries, up to 500 VLAN classifications can be created, and up to 500 priority classifications can be created. With the SAT size set to 16000 entries, up to 200 VLAN classifications can be created, and up to 200 priority classifications can be configured. For more detailed information about SAT size and classifications, refer to the user's guide <http://www.enterasys.com/support/manuals/2-6.html>

**Matrix E7 Proxy Function**

The 3<sup>rd</sup> generation modules (6X3XX) provide a function called "proxy". This function provides 1<sup>st</sup> and 2<sup>nd</sup> generation modules (which have only 4 backplane ports that connect to slots 1-5) with the ability to communicate with 3<sup>rd</sup> generation modules installed in slots 6 and 7, by way of an intermediate (proxy) 3<sup>rd</sup> generation module installed in one of the first 5 slots.

A packet entering a port on a 1<sup>st</sup> or 2<sup>nd</sup> generation module in one of the first 5 slots is transmitted to the FTM1 backplane connection to the 3<sup>rd</sup> generation "proxy" module in one of the first five slots. This proxy module can then forward that packet out its appropriate backplane port to either slot 6 or 7.

The lowest numbered slot containing a 3<sup>rd</sup> generation module will always be the "proxy" module. The function moves dynamically if a new lower slot 3<sup>rd</sup> generation module is installed or removed.

Since the "proxy" function does consume switching resources, switching performance will be reduced on the module. For this reason, it is not recommended that an uplink module (like the 6G306-06) perform the "proxy" function in order to avoid performance degradation of the uplink. This is avoided by simply installing uplink modules in the higher numbered slots and using other 3<sup>rd</sup> generation modules in a lower numbered slot to perform the function.

**ATM Specific**

In order for the HSIM-A6DP, VHSIM-A6DP or VHSIM2-A6DP to operate with this version of firmware, the optional memory upgrade kit must be installed in the SmartSwitch 2000/6000. The Enterasys Networks' part number for this kit is SS-16M-DRAM-UGK.

This version of firmware supports the ATM Forum's standards for LAN Emulation version 1.0 and 2.0 as well as UNI 3.0, 3.1, and 4.0 Signaling, and Traffic Management 4.0™. The VHSIM-A6DP, VHSIM2-A6DP, and HSIM-A6DP modules are 802.3 LAN Emulation (LEC) devices and will operate in an 802.3 Emulated LAN using an MTU of 1516 bytes or 1580 bytes.

The VHSIM-A6DP, VHSIM2-A6DP and HSIM-A6DP support 32 LECs when operating in 802.1Q mode.

For SVC operation, LAN Emulation Services must be installed on the ATM Network. At a minimum, there must be an 802.3 LAN Emulation Server (LES) and a Broadcast and Unknown Server (BUS). Additionally, there should be a LAN Emulation Configuration Server (LECS) on the ATM network. If there is no LECS on the ATM network, the ATM address of the LES must be manually entered on the VHSIM-A6DP, VHSIM2-A6DP or HSIM-A6DP through Local Management.

On power-up, the VHSIM-A6DP, VHSIM2-A6DP, and HSIM-A6DP will automatically join a default ELAN provided by ATM Services. The VHSIM-A6DP, VHSIM2-A6DP and HSIM-A6DP will contact the LECS using the Configured ATM address of the LECS. If an LECS ATM Address has not been configured (via Local Management), the VHSIM-A6DP, VHSIM2-A6DP and HSIM-A6DP will use the ATM Address provided by Interim Local Management Interface (ILMI) to set up a connection to the LAN Emulation Configuration Server (LECS). If there is no response via ILMI, the VHSIM-A6DP, VHSIM2-A6DP, and HSIM-A6DP will set up a connection to the well-known ATM

**CUSTOMER RELEASE NOTES**

address of the LECS. If a connection is not successful to the well-known ATM address, the VHSIM-A6DP, VHSIM2-A6DP, and HSIM-A6DP will use the well-known VC of VPI=0, VCI=17 to connect to the LECS.

This firmware image supports Permanent Virtual Circuits via Local Management or the IETF AtoM MIB (RFC 2515). When PVCs are used, LAN traffic is encapsulated over ATM using RFC 1483 VC-based Multiplexing or LLC Encapsulation for Bridged Protocols.

**HSIM-A6DP Specific**

This version of firmware supports up to 2040 SVCs on the HSIM-A6DP using LANE 1.0/2.0 and UNI 3.0/3.1/4.0 signaling. In 802.1Q mode, 64 PVCs are allowed. Each PVC is treated as a bridge port.

This firmware image provides support for Bandwidth Allocation over PVCs. When creating PVCs via Local Management, the user can specify a peak bandwidth allowed (in Mbps) to be transmitted on each PVC. This feature is available for PVCs only. SVCs are not allowed when using this feature.

This version of firmware provides support for the HSIM-A6DP Traffic Management Daughter-card (HSIM-TM-UGK and HSIM-A6DP-TM). When the TM card is installed, the HSIM-A6DP supports the following ATM Forum Traffic Management 4.0 traffic classes:

- UBR
- ABR (Explicit Rate and Relative Rate)
- nrt-VBR
- CBR

This version of firmware provides support for up to 64 Traffic Descriptors, which can be assigned to any of the aforementioned classes. A single Traffic Descriptor can be used for each PVC on the HSIM-A6DP. Traffic Descriptors (up to eight) are assigned to a LEC or virtual port based on 802.1p priority and transmit queue mapping. Traffic Management will carry priority across the ATM fabric for the given QoS level.

**VHSIM-A6DP and VHSIM2-A6DP Specific**

This version of firmware supports up to 8192 SVCs on the VHSIM-A6DP using LANE 1.0/2.0 and UNI 3.0/3.1/4.0 signaling. The number of PVCs allowed in 802.1Q mode is 64. Each PVC is treated as a bridge port.

This version of firmware provides support for the following ATM Forum Traffic Management 4.0 traffic classes:

- UBR
- nrt-VBR
- CBR

This version of firmware provides support for up to 64 Traffic Descriptors, which can be assigned to any of the aforementioned classes. A single Traffic Descriptor can be used for each PVC on the VHSIM-A6DP. Traffic Descriptors (up to eight) are assigned to a LEC or virtual port based on 802.1p priority and transmit queue mapping. Traffic Management will carry priority across the ATM fabric for the given QoS level. Please refer to the user's guide for proper utilization of this feature.

**Fast Ethernet VHSIMs**

For the following VHSIM-G6 module to operate, the minimum firmware revision 1.03.07 must be installed and running on the SmartSwitch 2000/6000 prior to installing the VHSIM-G6. If this firmware is not running prior to installing the VHSIM, the switch module may not boot-up.



**CUSTOMER RELEASE NOTES****IEEE 802.1X Port Based Network Access Control**

Using the physical access characteristics of IEEE 802 LAN infrastructures, the 802.1X standard provides a mechanism by which administrators can securely authenticate and grant appropriate access to users directly attached to switch ports. When configured in conjunction with NetSight Policy Manager and RADIUS access server(s), Enterasys switches can dynamically administer user-based policy that is specifically tailored to the end user's needs. Please refer to the *SmartSwitch 2200/Matrix E7 Series Security Local Management Supplement* for additional information and configuration requirements. Additional information related to Enterasys Networks' User Personalized Network architecture can be found at <http://www.enterasys.com/upn/>

**RADIUS Management Authentication**

Enterasys' RADIUS management authentication is a standard-based process in which access to critical management functions (LM screens via COM port and TELNET) are processed through external RADIUS Authentication services. Authentication via RADIUS will use Password Authentication Protocol (PAP) and require username and password credentials to gain access to management resources. In the event no external RADIUS server is present or configured, the switches will revert to legacy password protection. Accounting services for access receipt is not available in this release. Please refer to the Local Management user's guide for information specific to administration of RADIUS client services.

**Access Control Lists (ACL) for Management Port Security**

This firmware release incorporates the ability to define in Local Management a list or range of IP addresses that are authorized to access management. By introducing such a function, the admission of non-authorized nodes accessing the switch and making potentially harmful changes to configuration parameters is negated. The definition of the addresses can be as granular as a single IP workstation to a range of IP addresses within a given subnet. When used in conjunction with RADIUS Authentication, switches operating with this firmware revision offer additional security measures for the management host.

**Per VLAN Spanning Tree (PVST)**

The 802.1Q-1998 standard specifies a single 802.1D-Spanning Tree running across all VLANs. This was done primarily to expedite the ratification of the standard. Some of the benefits of configuring multiple VLANs are sacrificed with this compromise. The ability to run a Spanning Tree domain per VLAN is a powerful enabler in the deployment of VLANs as a topology management tool. PVST presents several significant benefits to end users and network managers:

1. Multiple, load sharing, links between switches optimize the most efficient utilization of bandwidth.
2. Topology re-spans and disturbances are confined to a single VLAN domain. Global interruption is averted, as Spanning Tree domains on any particular VLAN will not impact the state of another VLAN's Spanning Tree topology state.
3. The scalability of topologies can be extended much greater than single 802.1D Spanning Tree domains. The limits on the number of hops in a single Spanning Tree currently limits the geographical scope even though connectivity is restricted by VLANs.

**Remote Network Monitoring MIB Extensions for Switched Networks (SMON, RFC 2613)**

SMON is an IETF standard outlining the MIB necessary for gathering and compiling remotely monitored switch based technologies as opposed to shared segment technologies. The SMON capabilities incorporated in this release of firmware permit the statistical gathering of VLAN information.

**IEEE 802.1w - Rapid Reconfiguration of Spanning Tree**

The convergence times of IEEE 802.1D environments have been expedited through developments in IEEE Spanning Tree rapid reconfiguration. This technology is based on and compatible with traditional Spanning Tree topologies and addresses the limitations imposed on port state by a timer-based process. Anticipating certain network failures, Rapid Reconfiguration ensures the end-user is insulated from dropped sessions or resource

**CUSTOMER RELEASE NOTES**

inaccessibility through accelerated and anticipatory Spanning Tree states (state-based). Physical connectivity, in the event of failure, can occur in less than five seconds compared to the forty-five to fifty second delays.

**IEEE 802.3ad Link Aggregation**

This version of firmware supports dynamic link aggregation via the IEEE 802.3ad specification. Link aggregation, through the use of the *Link Aggregation Control Protocol* (LACP) can be used for automatic communication of trunking capabilities between systems and automatic configuration of links between a switch and its link partner.

**IEEE 802.1t**

This version of firmware supports the IEEE 802.1t standard. 802.1t expands the allowable range of Spanning Tree path costs to accommodate higher speed technologies such as 10 gigabit Ethernet. By default the switch uses the path costs defined in 802.1D 1998. To enable 802.1t path costs, use the `stpLegacyPathCost` network tools command. It is recommended that a consistent path cost scheme be used throughout the network.

**FIRMWARE CHANGES AND ENHANCEMENTS:****5.06.04**

Added the ability to allow the same MAC address to be locked on multiple ports.

Added support for RADIUS\_NAS\_port\_type.

Added the ability to allow an administrator to disable RADIUS authentication for remote management.

Added the ability to allow the switch to send an SNMP trap each time a new source address is learned.

MIB II sysName, sysLocation, and sysContact all now return a null string by default.

Added Link Flap feature. Link flap will disable a port for a set period of time when the frequency of link state changes exceeds a user-defined interval. The feature is configured using the linkflap\_detect command in Local Management Network Tools.

Added support for undecoded RADIUS filter IDs.

Added the ability to automatically disable a switch port when it receives a BPDU. The feature is configured in Local Management Network Tools.

Added a Network Tools command to allow the ability to hide the "SecureHarbour" logo when using Port Web Authentication.

Added a MAC Authentication Configuration screen in Local Management.

Added a RADIUS Management Option to the RADIUS Configuration screen in Local Management.

Added SecureSpan feature. The feature is configured using the securespan command in Local Management Network Tools.

Added Node/Alias speed-up enhancement. Note that if the Compass tool part of NetSight Atlas Console is used, NetSight Atlas Console 1.3 is required to take advantage of this enhancement.

Added ifName enhancement. For example, the ifName for Fast Ethernet Port 5 of switch in slot 3 will be displayed as "fe.3.5".

Added Local Management Network Tools command igmpv3\_drop enable/disable. This allows the switch administrator to allow IGMPv3 multicast frames to be either flooded or filtered.

Fixed an issue with IEEE 802.1X where the EAP-Success message was sent by the authenticator (switch) to the supplicant (client) before the user policy was completely mapped on the physical port.

Fixed an issue where users continually logging in and out using Web based authentication could cause the switch to stop allowing users to login.

Fixed an issue where the user name and password screen still appears after an access violation.

Fixed an issue where policy was not being enforced properly if multiple policy roles were applied to different ports.

Fixed an issue where RMON history was reporting erroneous information.



**CUSTOMER RELEASE NOTES**

Fixed an issue where Spanning Tree was blocking ATM ports in a different LEC.
Fixed an issue where if a VLAN port assignment is changed on a LEC virtual port, the switch would not add the virtual port to the egress list of the new VLAN.
Fixed an issue where if "switch 8" was disabled in local management it could not be re-enabled.
Fixed an issue where passwords with the character . would not work.
Fixed a VHSIM-A6DP/VHSIM2-A6DP VC FIFO issue that could cause the switch to drop connections.
Fixed a reset issue that would log a DMS APP error in the message log.
Fixed an issue where incorrect SNMP traps were being generated when a GPIM was removed.
Fixed an issue where ctTimedResetStatus could only be successfully queried if the Super User community string was used.
The Local Management Network Tools StpStandby command has been removed, as this same functionality is provided by 802.1w. In previous version resetting a switch with stpStandby enabled could result in the ports on the switch being disabled.
Fixed a reset issue that would result in a 'No Room for HG Port State' message to be logged in the message log.
Fixed an issue where ctAliasConfigurationInterfaceEnableState could not be set.
Fixed an issue where an uploaded configuration file would increase in size each time it was uploaded or downloaded.
Fixed an issue where Rate Limit Low Mode was not correctly reflected in the Local Management Rate Limiting Configuration Screen.
Fixed an issue where users could not be authenticated using the PEAP Protocol.
Fixed an issue where configuring more than 48 rate limiters could cause the switch to reset. This could be seen by applying the NetSight Atlas Policy Manager "demo.pmd".
<b>5.05.05</b>
Added Local Management and WebView interface to modify STP bridge priority.
Added Policy and MAC locking commands to network tools.
Added MAC locking enhancements (Static MAC locking, multiple dynamic and static MAC locks, move dynamic MAC locks to static).
Added firmware support for GPIM-02 with 6G306-06 only.
In previous versions, host control frames (BPDU, GVRP, CDP, IGMP, EAPoL) were not transmitted out the destination ports of a port mirror. This issue has been corrected.
In previous versions, the total multicast streams supported was limited to 32. The multicast pool size is now configurable via the IGMP/VLAN screen.
In previous versions, ports which received OSPF and VRRP packets would send IGMP router add events causing multicast traffic to be erroneously forwarded out those ports. This issue has been corrected.
In previous versions, a configuration backup using the virtual IP address of an HP cluster would fail. This issue has been corrected.
In previous versions, a CDP memory corruption error potentially could have resulted in a 6H302-48 reset. This issue has been corrected.
In previous versions, intermittent loss of backplane connectivity between 6H302-48 modules in slots 3 and 5 in a Matrix E7 chassis was observed. This issue has been corrected.
In previous versions, on aggregated links, CDP packets were sourced with the physical port information. This has been changed so, on aggregated links, CDP packets are sourced with the logical port information.
The D-Trunk functionality has been modified to match the 4.08.XX firmware version behavior.

**CUSTOMER RELEASE NOTES****5.04.09**

MAC address authentication and MAC address locking are now supported. These features enable administrators to allow access to the network based on a device's MAC address. For detailed information on using these features, refer to the User's Guide located on the Enterasys website.

<http://www.enterasys.com/support/manuals/>

Ports on the switch can now be configured as "Trunk" or "Hybrid" ports. This feature simplifies manual configuration of VLAN egress lists.

Mirroring traffic from a single port to multiple ports is now supported. Mirroring traffic from multiple ports to a single port is also now supported. Up to 128 port mirroring (any combination) instances can be configured.

ACL "wildcards" are now supported for host port ACLs. Up to sixteen IP ranges can now be defined.

Up to six rate limiters can now be configured per port. Previously up to four rate limiters per port were allowed.

IEEE 802.3ad parameters can now be configured via WebView.

Node/Alias functionality has been enhanced to allow the administrator to enable and disable learning on individual ports via SNMP using the ctron-alias-mib. The number of learned alias entries can also be configured via SNMP.

Support for IEEE 802.1t has been added. The switch can now be configured to use the path costs defined in IEEE 802.1D 1998, or the path costs defined in 802.1t. By default the switch supports the IEEE 802.1D 1998 path costs.

Spanning Tree Topology Change Notifications can now be suppressed on a per port basis. The "suppress\_topology\_traps" command in Network Tools is used to enable and disable this feature.

Frame Classification rules are now available as a pool of 1024 rules available per switch for priority and VLAN classifications. In previous versions of firmware up to 512 VLAN classifications and 512 priority classifications were available.

A condition where certain IP addresses could not be configured as the IGMP querier has been corrected.

A condition where the LEC function on an HSIM/VHSIM-A6DP would stop operating has been corrected.

A condition where disabling PWA did not actually disable the function has been corrected.

A condition where the ports of a 6G306-06 could not be manually configured has been corrected.

A condition where a switch reset would occur under heavy load has been corrected.

A condition where ATM ports, not on the default VLAN, were not getting added to the default Spanning Tree, while running in non-PVST mode has been corrected.

A condition where deleting link aggregation ports via WebView could cause re-created link aggregation ports to stay in blocking mode has been corrected.

A condition where rapid toggling of the Port Authorization screen could cause the module to reset has been corrected.

A condition where RMON history utilization was not being reported correctly on an HSIM-FE6 port has been corrected.

**5.03.08**

A reset condition caused by polling the MIB object ctCDPneighborMAC has been corrected.

A condition where port parameters could not be manually configured on the 1000Base-SX, 1000Base-LX, and 1000Base-ELX interfaces has been corrected.

A condition where the "B" port of an FPIM-01 was not recognized has been corrected.

The option to select TOS=PID in the Priority Classification local management screen has been removed. In order to write the TOS value to equal the PID value, the values need to be explicitly defined.

A condition where the switch "listens" to TCP or UDP port 7 echo requests has been fixed. The switch no longer "listens" to port 7 echo requests.

A condition where WebView would incorrectly display the current status of the SmartTrunk protocol setting has been corrected.

A condition where RMON would incorrectly count 1518 byte packets as oversized has been corrected.

## CUSTOMER RELEASE NOTES

A condition where SNMP management was lost after upgrading from firmware 4.08.xx to 5.02.x and higher has been corrected.

A condition where PVCs configured on an HSI-M-A6DP were not restored after reset has been corrected.

A condition where dynamic VLANs (GVRP) were not being propagated correctly through a device acting as the proxy bridge in a Matrix E7 has been corrected.

In previous firmware versions, certain 192.168.x.x IP addresses could not be used. This issue has been corrected.

A reset issue that logged an "IPLFIFO" message in the message log has been fixed.

### 5.03.05

Support has been added for the 6G302-06. For firmware in the 5.x track, this version or higher must be used. For the 4.x firmware track, 4.08.43 or higher must be used on the 6G302-06.

Support has been added for a new hardware version of the 6H302-48. This new module can be identified by the first four digits of the serial number located on the top ejector tab of the switch, or by querying the PIC MIB. The serial number of the new module will start with 3655. Example: **3655**xxxxxxx. For firmware in the 5.x track, this version or higher must be used. For the 4.x firmware track, 4.08.41 or higher must be used on the 6H302-48.

A number of SNMP host vulnerabilities have been fixed. The original issue is referenced at [http://www.enterasys.com/support/snmp/snmp\\_statement2.html](http://www.enterasys.com/support/snmp/snmp_statement2.html)

PVST port configuration labeling is now correct in Local Management.

A GVRP memory leak, that could cause resets, has been fixed.

A reset caused by using port mirroring over ATM interfaces has been fixed.

An issue where SmartTrunk links wouldn't operate correctly on the HSI-M-FE6 when upgraded from 5.01.34 to 5.02.03 has been corrected.

In previous firmware versions, certain 192.168.x.x IP addresses could not be used. This issue has been corrected.

A reset issue that logged an "IPLFIFO" message in the message log has been fixed.

### 5.02.03

*New Feature* - 802.1X Port Based Network Access through EAPOL.

A reset condition when applying rate limiting to ports has been fixed.

Querying the dot1dStpProtocolSpecification MIB now yields a correct response.

The SecureHarbour DNS name can now be greater than 24 characters (but less than 32 characters).

An issue preventing the application of IPX classification rules has been addressed.

When using an HSI-M-FE6 with FEPIM FE100TX's, tagged packets greater than 1468 bytes are no longer dropped.

The IGMP switch querier IP address can now be set back to 0.0.0.0.

### 5.01.33

*New Feature* - IEEE 802.1w Rapid Reconfiguration of Spanning Tree.

*New Feature* - IEEE 802.3ad Link Aggregation.

*New Feature* - Port Based Web Authentication through RADIUS challenge.

*New Enhancement* - Rate Limiting can now be defined to a more granular level using the rate\_limit\_mode command in local management. The new low range allows the selection of rates as low as 50Kbps to 400Mbps in addition to the default 100Kbps to 1Gbps.

*New Enhancement* - Added gigabit\_oversize command to network tools.

*New Enhancement* - Added PVST port configuration screen.

*New Enhancement* - Added show mac command to network tools.

*New Enhancement* - WebView and LM Module Password screens now contain a new field called "Restrict NVRAM Passwords from upload/download". When this feature is enabled, the passwords in NVRAM do not get uploaded and will not be used if they are in a download configuration file. When disabled, the NVRAM passwords will be uploaded and if they are downloaded they will be used.

**CUSTOMER RELEASE NOTES**

GVRP can now be disabled on a global basis through local management.  
Power supply and chassis information is now available in the Matrix E7.  
Message age timers now correctly increment across bridge hops.  
HSRP router packets are now correctly forwarded with IGMP snooping enabled.

**KNOWN RESTRICTIONS AND LIMITATIONS:**

When enabling PVST, ports manually added to VLANs may not be configured properly if the VLAN configuration is saved prior to enabling PVST. It is recommended to enable PVST prior to saving created VLANs.  
GVRP state configuration is not supported via WebView.  
Port loop back detection is not supported on 100BaseFX ports (HSIM-FE6 w/FE100-FX, 6H308-48).  
GVRP accepts GVRP updates on GVRP disable ports. The workaround is to globally disable GVRP.  
Using Matrix E7 modules as IGMP queriers may cause an undesired result where responses to queries are not answered with a report message. If the querier and clients are not located in the same chassis, then the IGMP reports will not be transmitted properly. If the querier is another device such as a router, and not a Matrix E7 module, IGMP packets are processed properly.  
IP address 192.168.x.x is reserved for Port Web Authentication. While Port Web Authentication is enabled, you will not be able to use this IP address.  
All ports included in a SmartTrunk group must be manually set to Full Duplex.  
An issue in which tagged packets will not be redirected across the backplane will be resolved in a future release of firmware.  
If the etsysPwaSystemAuthHostName (Secure Harbour name) is set to 16 or more characters, and DNS is not enabled on the end-station, then the request will not be resolved. This is a limitation of the WINS protocol. However if the etsysPwaSystemAuthHostName is set to 16 or more characters and DNS is enabled on the end-station, then the request should get resolved by DNS.  
RADIUS Authentication over ATM is not supported.  
The HSIM-A6DP, HSIM-G01, HSIM-G09, HSIM-SSA710, HSIM-SSR600, and VHSIM-A6DP are not supported in the 6H352-25.  
Rate Limiting is not supported over ATM interfaces or WAN VC interfaces (i.e., HSIM-W87/-W85) in this release of firmware.  
When using 802.1Q VLANs with multiple LECs, and with PVST disabled, Spanning Tree Algorithm must be disabled on ATM. This can be done via the Local Management "Network Tools" option using the atm\_stp\_state command.  
MPOA and ATM Lane Services (LECS, LES, BUS) are not supported in this version of firmware.  
The SmartSwitch cannot perform Layer 3/4 Classification on frames received by the HSIM-A6DP, VHSIM-A6DP or VHSIM2-A6DP. This means that inbound ATM frames cannot be classified into an 802.1Q VLAN based on the received frame's protocol type. Also, inbound ATM frames cannot be assigned an 802.1p Priority value based on a frame's protocol type, Layer 3 or Layer 4 information.  
VLAN IPX classifications using the custom field to specify a socket number does not work in this release.  
Each ATM LEC assigned to an 802.1Q VLAN must be assigned a unique Filtering Database Identifier (FID).  
GVRP must be disabled on the following types of interfaces: 802.1Q Trunk Ports, 802.1d Trunk Ports, SmartTrunk Ports and all ATM ports.  
IEEE 802.1Q VLAN tagging is not supported on the VHSIM-A6DP.  
GVRP should be disabled on ATM ports implementing a VHSIM-A6DP. This module does not support tagged frames.  
SMON statistics cannot be gathered on an ATM port.  
GVRP must be manually disabled on a port on which PVST is enabled.

**CUSTOMER RELEASE NOTES**

You must have GVRP enabled globally and on the ports whose PVIDs have been assigned the VLAN associated with the Dynamic\_egress command.

SecureFast Switching is not supported in this release.

NVRAM must be cleared on a 6H302-48 module after upgrading from version 4.02.10 to this release because of interface numbering changes between firmware revisions.

1<sup>st</sup> and 2<sup>nd</sup> generation modules (6X1XX & 6X2XX series) are restricted to installation into slots 1-5 of the Matrix E7. In addition, if backplane communication from these modules in slots 1-5 to 3<sup>rd</sup> generation modules within slots 6 and 7 is desired, a 3<sup>rd</sup> generation module (6X3XX) is required to be installed within the first 5 slots to perform the proxy function. See "Matrix E7 Proxy Function" on page 5 of these notes.

The Matrix E7 chassis does not support Distributed Chassis Management.

Port Redirect cannot be used to redirect frames between modules that use the proxy function within the Matrix E7 for their connectivity. Specifically, frames cannot be redirected from 1<sup>st</sup> or 2<sup>nd</sup> generation modules in slots 1-5 to a 3<sup>rd</sup> generation module in slots 6-7, and vice-versa. Note that frames may be redirected between any two 3<sup>rd</sup> generation modules in the chassis.

Using local management to configure 100 Mb/s Full Duplex via "Save to all ports" command on a module with a VHSIM-G6 or VHSIM-G02 installed, may cause constant Spanning Tree topology changes to occur. This will only occur on devices with a VHSIM-G6 or VHSIM-G02 installed. This issue can be avoided by configuring the ports individually.

BOOTP firmware download will not function over an 802.1Q tagged port.

Hot swapping a 3<sup>rd</sup> generation module into a lower numbered slot, than the current Matrix E7 proxy module, will cause the proxy function to move to the newly inserted module. This will cause a temporary loss of connectivity for 1<sup>st</sup> and 2<sup>nd</sup> generation modules communicating to slots 6 and 7. This does not happen with removal of the current proxy module causing the proxy function to move to the next 3<sup>rd</sup> generation module in a higher slot number.

There can be power redundancy issues when installing 6H302-48 or 6H303-48 modules in a SmartSwitch 6000 chassis. The 6C205-1 power supply provides 60 Amps and the 6C205-3 provides 90 Amps. The recommended maximum using the 6C205-1 is two modules (6H30x-48) and four when using the 6C205-3. Please contact Technical Support for assistance in determining which configurations have power redundancy and those that do not. The redundancy LEDs on the power supplies indicate the status of power redundancy. When both LEDs are green, the chassis has redundant power. The Matrix E7 does not have these power redundancy issues.

User-configured VrrpPort settings in Local Management may be lost after downloading this image and resetting the switch. The settings must be manually reentered.

By default only one port is active on the VHSIM-G6 and 6H262-18. To activate the second port you must use the "gigabit\_port\_mode" option in the Network Tools Local Management screen. When the second port is activated, the switch will reset, and the contents of NVRAM with the exception of IP Address and Subnet Mask will be lost.

If the device is running boot code version 2.01.00 or lower and power-up sequence is interrupted, or if optional hardware is installed or removed, the device may run an extended diagnostics sequence. During the extended diagnostics, the CPU LED color will be solid amber. This sequence may take between five to forty minutes to complete depending on the hardware model.

The SmartSwitch host (SNMP management) port must not be configured as an 802.1Q tagged Port. If configured as an 802.1Q tagged Port, the device may reset. If the user wishes to make the host port accessible from some or all 802.1Q VLANs, then the 802.1D untagged Port option must be used.

If an optional HSIM or VHSIM is installed or removed, the device will restore all configuration settings to the factory defaults. The only customer configuration settings that will be saved are the IP Address, Subnet Mask and the Operational Mode.



**CUSTOMER RELEASE NOTES**

When upgrading from firmware version 2.00.17 to this version of firmware, the speed and duplex settings may not be properly restored from NVRAM. In the event this occurs, you will need to reconfigure the speed and duplex settings if something other than the default setting is required. This issue only affects devices running firmware version 2.00.17.
If HSI-M-F6 ports are configured to operate in full duplex mode, the Local Management Ring Map screen may not operate correctly.
The HSI-M-F6 should not be configured as an 802.1Q tagged port.
The HSI-M-F6 does not support 802.1Q tagged frames which exceed the maximum Ethernet frame length (1522 bytes). Frames larger than 1522 bytes will be discarded by the switch.
The HSI-M-F6 was developed in the early stages of the 802.1Q standards process. The Ethernet & FDDI translation and frame tagging rules were not fully defined at development time. Changes made during the standardization process, result in the HSI-M-F6 using a proprietary method of frame tagging on FDDI. The implementation used on the HSI-M-F6 is fully functional between other HSI-M-F6 devices.
The user-configurable parameters available in the IGMP Local Management screen should be set to match the parameters on the device acting as the IGMP Querier if one exists. This version of firmware does have the ability to act as an IP querier.
Runtime firmware downloads will not work if the TFTP server is using one of the following RFC 1918 reserved addresses: 10.0.0.0, 172.16.0.0, 192.168.0.0
All modules installed in a Matrix E7 must have consistent Spanning Tree settings, i.e., all modules configured for Spanning Tree enabled or all modules configured for Spanning Tree disabled. This restriction does not apply to individual ports just the entire module. Also the same Spanning Tree algorithm (IEEE or DEC) must be used for all modules installed in a Matrix E7.
Backplane ports must not be administratively disabled on modules installed in a Matrix E7, when there is a device providing a Proxy bridge service in the chassis. If backplane ports are disabled, unreliable Spanning Tree operation could occur. For details on Proxy Bridge, refer to the "Matrix E7 Proxy Function" in the "Installation and Configuration Notes" section of this document.
A BootP firmware image download should not be performed to a device that is providing a proxy bridge service. If a download is performed on the proxy device, the proxy will stop bridging, and the other modules in the chassis will not assume the proxy function. An online (runtime) download can be performed on any module including the proxy without affecting proxy function.
When operating in Per VLAN Spanning Tree (PVST) mode no other switch or bridge should be operating in DEC bridging mode. Please refer to the user's guide for design guidelines.
The maximum number of PVST instances for a single switch is twenty.
GVRP assumes a single Spanning Tree per domain. As a result GVRP cannot be run in PVST regions of the network topology.
802.1D switches will emit BPDUs that appear to be in the PVST of the default VLAN.
When interconnecting an 802.1Q environment to a PVST environment, the connection should be made through a trunk. This will permit the 802.1Q Spanning Tree to merge with the IEEE Spanning Tree of the PVST cloud. It will also permit the PVST BPDUs to tunnel through the 802.1Q environment.
When downloading a configuration file to a switch, the file used must have been originally uploaded from the same SmartSwitch type (i.e., a file from a 6H202-24 can only be downloaded to a 6H202-24).
In PVST topologies that include an X-Pedition router (formally SSR), the command <i>set special-encap</i> must be evoked in the router's command line interface and configuration to ensure proper interoperability.
When aggregating ports with IEEE802.3ad there is a maximum of 6 aggregators per module.
Ports cannot be trunked via SmartTrunking or IEEE802.3ad across multiple modules in a chassis.
All ports within an IEEE802.3ad aggregation must be configured to full duplex. Ports manually set to half duplex or of differing interface speeds will not trunk.
User authentication will fail if the policy name contains a : (colon) or ; (semi-colon).



**CUSTOMER RELEASE NOTES**

Dynamic Egress functionality is designed to only work in the default Spanning Tree.

Every PVC or LEC interface is considered a bridge port. These ports are designed to support only one Spanning Tree state. Each bridge port created by a PVC or LEC is restricted to only one Spanning Tree instance. A virtual port can only be associated with one instance. This prevents implementations that trunk multiple VLANs over a single PVC or LEC. The solution is to map a PVC/LEC per PVID for each VLAN.

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

**COMPLIANCE SUPPORT:**

Compliance Level	Compliant
Year 2000	YES

Known Anomalies: None.

**STANDARD MIB SUPPORT:**

RFC No.	Title
RFC 1190	Path MTU Discovery
RFC 1213	MIB II
RFC 1354	FIB
RFC 1493	Bridge MIB
RFC 1573	Evolution of MIBII Interfaces
RFC 1595	SONET MIB
RFC 2515	AtoM MIB
RFC 1757	RMON MIB
RFC 2613	SMON MIB dataSourceCaps smonStats smonVlanStatsControlTable smonVlanIdStatsTable
RFC 2674	IETF Q MIB
RFC 2869	RADIUS Extensions
	IEEE8021-PAE-MIB
	IEEE8023-LAG-MIB
	IEEE8021-RSTP-MIB

## CUSTOMER RELEASE NOTES

### PRIVATE ENTERPRISE MIB SUPPORT:

Title and Version No.		
<b>Event-action mib</b> version 1.03.01	<b>ctmib2-ext-mib</b> version 1.05.01	<b>sys-res-mib</b> version 1.00.02
<b>container mib</b> version 1.02.00	<b>ctdownload</b> version 1.06.01	<b>ctpic-mib</b> version 1.02.01
<b>ctbridge-mib</b> version 1.06.01	<b>fast-ethernet-mib</b> version 1.02.01	<b>trap-mib</b> version 1.01.03
<b>ctenvir-mib</b> version 1.05.01	<b>ctbroadcast-mib</b> version 1.00.01	<b>ctsmt-mib</b> version 1.03.02
<b>ctip-mib</b> version 1.02.01	<b>cttranslat-mib</b> version 1.01.06	<b>ctatm-mib</b> version 1.03.00
<b>community-mib</b> version 1.02.02	<b>ctrouter-mib</b> version 1.01.00	<b>ctEthernetParameters</b> ver 1.00.00
<b>Ctups-mib</b> version 1.03.00	<b>ctIFRemap2-mib</b> ver 2.00.02	
<b>ct-vlan-classify-mib</b> version 1.00.00	<b>ctTxQarb-mib</b> ver 1.00.01	<b>ct-priority-classify-mib</b> ver 1.00.00
<b>Ctron-cdp-mib</b> version 2.00.05	<b>ctWebView-mib</b> Version 1.00.00	<b>ctRatePolicing-mib</b> version 1.00.00
<b>ct-smarttrunk-mib.txt</b> version 1.00.01	<b>ctron-oids-mib</b> version 1.1	<b>ctron-alias-mib</b> version 1.00.00
<b>enterasys-oids-mib</b> version 1.00.00	<b>enterasys-policy-profile-mib</b> version 1.00.08	<b>enterasys-RADIUS-auth-client-encryp-MIB</b> version 1.1
<b>enterasys-PWA-MIB</b> version 1.1	<b>enterasys-RADIUS-auth-client-MIB</b> version 1.1	<b>ctron-igmp-mib</b> version 1.1
<b>ctron-smarttrunk-mib</b> version 1.0	<b>ct-if-ext-mib</b> version 1.3	<b>ctron-WebView-mib</b> version 1.1
<b>enterasys-mac-locking-mib</b> version 1.9		

Cabletron and 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
1157	WARM START LINK UP LINK DOWN AUTHENTICATION FAILURE
1493	NEW ROOT TOPOLOGY CHANGE

**CUSTOMER RELEASE NOTES****PRIVATE ENTERPRISE TRAP SUPPORT:**

Title	
0x1A2 interfacePortLinkUp	0x40D fddiMACDuplicateMACAddress
0x1A3 interfacePortLinkDown	0x44E aPCLineFailRecovery
0x3EB ctBroadcastThresholdReached	0x450 aPCLowBatteryRecovery
0x4B0 contLogicalChangesTrap	0x451 aPCAbnormalCondition
0x4B1 contPhysicalChangesTrap	0x708 wgPsInstalled
0x44F aPCLowBattery	0x709 wgPsRemoved
0x542 aPCAbnormConditionRecovery	0x70A wgPsNormal
0x453 aPCShuttingDown	0x70B wgPsFail
0x44D aPCLineFail	0x70C wgPsRedundant
0x400 fddiPortConnectStateChange	0x70D wgPsNotRedundant
0x403 fddiPortAction	0x70E wgBoardInserted
0x404 fddiPortLerAlarm	0x70F wgBoardRemoved
0x408 fddiMACRMTState	0x2EE0 activePortInATMRedundancyFailed
0x409 fddiMACCurrentPath	0x2EE1 aTMRedundantPortActivated
0x40A fddi SMTCFstate	0x2EE2 aTMRedundantPortTestFailed
0x40B fddiRingTopology	0x2EE3 aTMRedundPrimaryPortSkipped
0x40C fddiMACFrameErrorRatio	0x2F12 atmLecStatus
etsysMACLockingMACViolation	

**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](mailto: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.