50 Minuteman Road
Andover, MA 01810 (USA)
Tel: (978) 684-1000

CUSTOMER RELEASE NOTES

Enterasys Matrix™ E1 Series
WS & GWS & GDS
Firmware Version 3.07.32.0002
July 2009

INTRODUCTION:

This document provides specific information for firmware version 3.07.32.0002 for the Enterasys Matrix E1 WS, GWS, and GDS.

1H582-51	1H582-25	1G582-09	1G587-09

Enterasys recommends that you thoroughly review this release note prior to installing or upgrading this product. There may be a more up-to-date version of this Release Note. Please go to the Enterasys web site to ensure that this is the latest revision of the Release Note (http://www.enterasys.com/support/).

FIRMWARE SPECIFICATION:

Status	Version No.	Type	Release Date
Current Version	3.07.32.0002	Customer Release	July 2009
Previous Version	3.07.31.0000	Customer Release	October 2008
Previous Version	3.07.30.0001	Customer Release	June 2008
Previous Version	3.07.29.0000	Customer Release	January 2008
Previous Version	3.07.28.0001	Customer Release	September 2007
Previous Version	3.07.26	Customer Release	June 2007
Previous Version	3.07.23	Customer Release	February 2007
Previous Version	3.07.21	Customer Release	December 2006
Previous Version	3.07.20	Customer Release	October 2006
Previous Version	3.07.14	Customer Release	May 2006
Previous Version	3.07.12	Customer Release	April 2006
Previous Version	3.07.03	Customer Release	February 2006
Previous Version	3.07.02	Customer Release	December 2005
Previous Version	3.05.12	Customer Release	November 2005
Previous Version	3.05.11	Customer Release	October 2005
Previous Version	3.05.09	Customer Release	July 2005
Previous Version	3.05.06	Customer Release	July 2005
Previous Version	3.05.05	Customer Release	April 2005
Previous Version	3.04.04	Customer Release	February 2005
Previous Version	3.03.08	Customer Release	December 2004
Previous Version	3.02.22	Customer Release	October 2004
Previous Version	3.02.08	Customer Release	May 2004
Previous Version	3.00.14	Customer Release	November 2003
Previous Version	2.06.01	Customer Release	October 2003
Previous Version	2.05.03	Customer Release	August 2003
Previous Version	2.04.12	Customer Release	May 2003
Previous Version	2.03.07	Customer Release	February 2003

Status	Version No.	Type	Release Date
Previous Version	2.02.14	Customer Release	December 2002
Previous Version	2.02.12	Customer Release	November 2002
Previous Version	2.01.10	Customer Release	September 2002
Previous Version	2.01.09	Customer Release	September 2002
Previous Version	2.00.20	Customer Release	June 2002
Previous Version	1.01.11	Customer Release	March 2002
Previous Version	1.01.05	Customer Release	March 2002
Previous Version	1.00.10	Customer Release	December 2001
Previous Version	1.00.05	Initial Customer Release	November 2001

NOTE: In order to successfully upgrade to 3.02.XX, the unit must be at a firmware version 2.00.20 or higher. If the unit is not at 2.00.20 or higher, the Matrix E1 upgrade tool can be used. The tool is located at http://secure.enterasys.com/support/tools.html.

NOTE: Version 1.01.05 was supported on the 1G582-09 only.

HARDWARE COMPATIBILITY:

This version of firmware is supported on all hardware revisions. See the table below for the minimum firmware and boot requirements.

Part	Description	Minimum System Firmware Version	Minimum Boot Firmware Version
1G587-09	6 port Mini-GBIC standalone with 3 uplink slots	2.06.01	2.00.00
1H582-25	24 port 10/100Base-T standalone with 1 uplink slot	2.05.03	1.03.00
1H-8FX	8 port 100Base-FX uplink module	2.01.10	1.01.00 * 1.00.05 *
1G-2MGBIC	2 port Mini-GBIC gigabit uplink module	2.00.20	1.00.03
1G582-09	6 port 1000Base-T standalone with 3 uplink slots	1.01.05	1.00.05
1G-2TX	2 port 10/100/1000 Base-TX uplink module	1.00.10	1.00.03
1G-2GBIC	2 port GBIC gigabit uplink module	1.00.10	1.00.03
1H-16TX	16 port 10/100Base-T uplink module	1.00.10	1.00.03
1H582-51	48 port 10/100Base-T standalone with 3 uplink slots	1.00.05	1.00.01

*Boot code version 1.01.00 is only required on the 1H582-51, version 1.00.05 is required on the 1G582-09 in order to support the 1H-8FX. In order to upgrade to boot code 1.01.00 on a 1H582-51 via network download, the unit must first be running firmware version 2.01.XX or higher. In order to upgrade to boot code 1.02.00 on a 1H582-51 via network download, the unit must first be running firmware version 2.03.XX or higher. Reference http://knowledgebase.enterasys.com/esupport/, ent8577 for other Matrix E1 upgrade considerations and procedures.

BOOTPROM COMPATIBILITY:

This version of firmware is compatible with all boot prom versions.

NETWORK MANAGEMENT SOFTWARE SUPPORT:

NMS Platform	Version No.
NetSight Console	3.1.3
NetSight Automated Security Manager	3.1.3
NetSight Inventory Manager	3.1.3
NetSight Policy Manager	3.1.3
NetSight Router Services Manager	3.1.3
Enterasys Sentinel Trusted Access Manager	3.1.3

If you install this firmware version, you may not have control of all 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:

Features	Features
802.3ad - Link Aggregation	Web-based user authentication (PWA+)
802.1s - Multiple Spanning Tree Protocol	RADIUS Accounting
Span Guard	Jumbo Frame (switch only)
Multiple local user account management	ACL editor functionality
Denial of Service prevention	SNTP
Outbound Traceroute	Audit trail logging
Auto-configuration	DNS Client
DVMRP - Multicast Routing	IGMP VLAN registration
Text-based Configuration Upload/Download	Telnet Client
Syslog	MAC-based Authentication
802.1w - Rapid Spanning Tree	Q-tag override command
Node/Alias table	SSHv2 (Server/Client)
IP Routing	802.1X Authentication
RIP v1/v2	OSPF
VRRP	RADIUS Client
DHCP Relay	MAC Port Locking
RAD (Remote Address Discovery)	ICMP Route Discovery
Extended ACLs	TOS Rewrite
802.1p – Traffic Management	Priority Classification L2-L4
802.1Q – VLAN tagging and identification	4 Transmit Queues per port
802.1D	802.3x Flow Control
802.1t	GVRP
CLI Management	Port Mirroring
Telnet Support	Port Trunking
IGMP v1/v2 Snooping	RMON (4 groups)
Strict and Weighted Round Robin Queuing	Runtime Download
Broadcast Suppression	GPIM support: GPIM-01, GPIM-02, GPIM-08, GPIM-09
Auto Negotiation	MGBIC support: MGBIC-LC01, MGBIC-MT01, MGBIC-LC09, MGBIC-08, MGBIC-02, MGBIC-LC03

Features	Features
VLAN Classification	Inbound Rate Limiting
WebView	Directed Broadcast
SNMPv1, SNMPv2c, SNMPv3	Convergence End Point (CEP) support for discovery of IP Phones.
Flow Setup Throttling	Enterasys Discovery Protocol (EDP)
Dynamic VLAN Assignment (RFC 3580)	Multicast Server Load Balancing

INSTALLATION AND CONFIGURATION NOTES:

Please refer to http://secure.enterasys.com/download/#switches for the latest firmware updates to the Matrix E1. In general, the Matrix E1 product will be shipped to you pre-configured with this version of firmware. If you would like to upgrade an existing Matrix E1 product, please follow the TFTP download instructions that are included in your Configuration Guide.

TFTP download instructions are also available on the Enterasys Knowledgebase. From http://knowledgebase.enterasys.com, click "Search by ID", then enter document ID ent8577.

Soft copies of the Configuration Guide are available at no cost to the user on the Enterasys Networks web site, http://secure.enterasys.com/support/manuals/. To order hard copies of the Configuration Guide, contact your Enterasys representative.

DOWNGRADING TO PREVIOUS VERSIONS

Firmware versions 3.07.14 and later support up to four active RADIUS servers of each type (that is, up to four authentication servers and four accounting servers). Firmware versions previous to 3.07.14 supported only up to two active RADIUS servers of each type.

If, after installing firmware version 3.07.14 or later, you wish to downgrade to a firmware version earlier than 3.07.14, you must ensure that at most, only two active RADIUS servers of each type are configured before you download the firmware image and reset the device.

Additional steps are required if you wish to downgrade from firmware version 3.05.09 or later to a firmware version earlier than 3.05.09.

Downgrading to a firmware version earlier than 3.05.09

1.) Save the device configuration to a TFTP server
2.) Clear the configuration from the E1
3.) Download firmware version earlier than 3.05.09 onto the E1 and reset
4.) Reload the previous configuration

FIRMWARE CHANGES AND ENHANCEMENTS:

Changes and Enhancements in 3.07.32.0002:
A display issue where certain host MAC addresses were reported as being on port fe.0.1 has been corrected.
An issue where the EAPOL attributes in a RADIUS Accept message could get corrupted has been corrected.
An issue where enabling RADIUS caused instability when no active RADIUS servers were configured has been corrected.
An issue where CDP neighbors are reported incorrectly via an SNMPGET has been corrected.
An issue where frames received on a VRRP backup were not forwarded correctly to the VRRP master has been corrected.
Configurations beyond the maximum allowed classification entries via SNMP will now report an error.

Changes and Enhancements in 3.07.31.0000:
An issue where the show nodealias port CLI command did not show all entries for the port has been corrected.
An issue where in some cases the first frame of an IP multicast session was not forwarded has been corrected.
DHCP IpHelper will now forward all replies rather than just the initial one.
The spanguardtrapenable CLI setting is now properly restored in all cases from NVRAM.
An issue with the SNMP "AT" and "ipNetToMediaTable" MIBs looping has been corrected.

Changes and Enhancements in 3.07.30.0001:
An issue where priority tagged frames were not properly forwarded when policy was applied to a port has been corrected.
An issue where MAC authentication could incorrectly attempt to authenticate multicast MAC addresses on port 1 has been corrected.
OSPF 2-WAY traps are now sent only on a transition in or out of the 2-WAY state.
PWA enhanced mode login redirect functionality has been made more robust.
An issue where the EAPOL attributes in a RADIUS Accept message could get corrupted has been corrected.

Changes and Enhancements in 3.07.29.0000:
An enhancement has been made to ssh logins to allow non-alphanumeric characters at the login prompt.
A performance enhancement was made to improve VRRP recovery time when the router is under a heavy and sustained load during a failover.
An issue where receipt of a malformed CDP frames could cause the device to reset has been corrected.
Port Web Authentication (PWA) has been enhanced to be compatible with the Windows VISTA Operating System.
A timing issue which caused the switch to think it has missed a bpdu and issue a TCN has been corrected.
Consistency checking for the Filter Database has been improved.
An issue where at times, SSH sessions would not be properly closed has been corrected.
An issue where the E1 with applied policy to a port was incorrectly preventing VRRP protocol frames from being forwarded has been corrected.
An issue where OSPF table MIB reads could report incorrect information has been corrected.
A change was made to correct cases where configured SNMP V3 notifyFilter entries were not persistent.

An issue that could cause a reset when RADIUS accounting is enabled has been corrected.
An issue where manipulation of a port's autonegotiation parameters via Webview would cause a reset has been corrected.
Via the CLI, the user is now queried for the RADIUS Mgmt-Auth state after RADIUS is enabled.

Changes and Enhancements in 3.07.28.0001:
An issue that would prevent pinging to the critical IP when its associated interface was down has been corrected.
The ability to process or discard IGMP frames whose IP address is outside the range of a routed interface is now configurable.
An issue where multicast frames were not forwarded after a port link down / up has been resolved.
An issue where VRRP frames included incorrect MAC address information when MD5 Authentication was enabled for VRRP has been corrected.
An issue where the E1 with applied policy to a port was incorrectly preventing VRRP protocol frames from being forwarded has been corrected.
An issue with RADIUS Authentication that could, in rare cases, cause a reset has been corrected.

Changes and Enhancements in 3.07.26:
An issue where classification Rules to permit LLC DSAP\SSAP frames did not function properly has been corrected.
An issue where memory corruption could occur if an adjacent router advertised 240 or more interfaces has been corrected.
An issue where OSPF may fail to converge properly, when adjacent routers are forcibly rebooted every two minutes for a period of hours, has been resolved.
A restriction to limit the user login name, via standard telnet or console, to alpha-numeric characters has been lifted.
The E1 now supports new daylight savings time start and stop dates.

Changes and Enhancements in 3.07.23:
Convergence End-Point (CEP) functionality was augmented to recognize additional models of Cisco IP Phones.
The E1 now correctly displays the non-default configuration entries for the trust-ext and cos-ext attributes of ciscoDP. Additionally these values can now be reset to the default value.
An issue where the vlan config fails to restore after a power cycle when a large number of vlans are configured has been corrected.
An issue where the switch show config command could hang in the displaying non-default ciscodp entries has been corrected.
A rare issue where the MAC Auth database gets corrupted and may force a switch reset has been corrected.
The set banner and set newaddrtrap commands are no longer allowed to be manipulated by Read-Only users.

Changes and Enhancements in 3.07.21:
The E1 host now correctly responds to the same VLAN that a command comes from. Previously in some multiple VLAN scenarios where the E1 switch was routing between VLANs, the E1 host would reply to its assigned VLAN instead of the VLAN that the command came from.

Changes and Enhancements in 3.07.20:
An issue where the removal of a node alias entry could cause a reset has been corrected.

Changes and Enhancements in 3.07.20:
An issue where the use of the LLS option in OSPF could lead to a reset has been corrected.

Changes and Enhancements in 3.07.14
set radius server command (or MIB settings) has been modified to support the configuration of up to four active RADIUS servers. The previous limitation was two.
A problem where POST test was causing configuration corruption has been resolved.

Changes and Enhancements in 3.07.12
set summertime and show summertime commands have been added to set and display daylight savings time settings.
The Calling-Station-Id attribute has been added to RADIUS accounting.
A problem where IGMP groups could fail to correctly forward traffic has been corrected.
A problem where the IM upload/download was not setting some commands has been corrected.
A problem where non-virtual DA MACs to Matrix E1 Router gateway were being dropped has been corrected.
A problem with the CLI looping on "show ip arp" command has been corrected.
A problem where the E1 would not respond properly to received topology change notifications has been corrected.
A problem with removing a classification rule residing on multiple policies has been corrected.
A problem where a high traffic load to the host was degrading performance when programming route entries has been corrected.
A problem where port 1 was incorrectly forwarding frames has been corrected.
A problem where in rare cases, arp entries were not properly updated has been corrected.
A problem where "write file" is commented out in the text config has been corrected.
A problem where configuration downloads incorrectly restored settings from a previous download has been corrected.
A problem where CiscoDP packets were not being forwarded has been corrected.
A problem where the radius mgmt-auth setting would not be properly configured after a reset has been corrected.
A problem with the ifXEntry MIB indexing incorrectly has been corrected.

Changes and Enhancements in 3.07.03
A problem causing a lockup condition when the system uptime reaches 497 days has been corrected.
An issue has been corrected where in rare instances, a VRRP backup entry can be incorrectly programmed causing connectivity loss.

Changes and Enhancements in 3.07.02
A problem with the display of SNMP community names has been corrected.
A problem with OSPF choosing a non optimal route has been corrected.
A problem with OSPF choosing the wrong next hop has been corrected.
A problem where static VLANs could become incorrectly configured after a reboot, which could suppress the transmission of unlearned frames, has been corrected.
A problem with an OSPF trap sending the wrong OID has been corrected.

Changes and Enhancements in 3.07.02
The CLI has been enhanced to show the last downloaded image when a download has been performed but the switch has not subsequently been rebooted.
The CLI has been enhanced to allow the port configuration and display of manual speed and duplex settings prior to disabling auto-negotiation.
Added support for Layer 2 load balancing (multicast enhancements).
A problem with memory corruption that could cause resets when CDP is enabled has been corrected.

Changes and Enhancements in 3.05.12
A problem where static VLANs could become incorrectly configured after a reboot, which could suppress the transmission of unlearned frames, has been corrected.

Changes and Enhancements in 3.05.11
EAPOL authentication packets are now set to flood by default.
A problem with resets occurring when all node/alias entries are deleted, has been corrected.
A problem with configuration activation and clear community commands causing management to hang, has been corrected.
A problem with the PWA logout page not loading properly if the host is configured in a different VLAN than the client, has been corrected.
A problem with the ctChassisPowerTable MIB returning power supply is not redundant when a redundant power supply is in use, has been corrected.
A problem where IP ACL allows ping but not telnet, has been corrected.

Changes and Enhancements in 3.05.09
WebView has been enhanced to include additional configuration and manageability for Span Guard, MSTP, and Port Negotiation and speed settings.
Span Guard traps are now supported.
Banner message length has been increased to 1200 characters.
The gratuitous ARP command structure has been enhanced.
A problem with communication when MAC Locking is enabled has been corrected.
A problem with connectivity to a host on an unauthenticated EAP port has been corrected.
A problem with clearing VLAN Authorization commands during configuration file processing has been corrected.

Changes and Enhancements in 3.05.06
A problem with the value in the RIP packet, next hop field has been corrected.
A problem with the counting of stations when using MAC Locking has been corrected.
A problem with port numbers when using MIB queries has been corrected.
A problem with host connectivity when policy is applied has been corrected.
The LSA Type 1 message count was increased from 100 to 200.

Changes and Enhancements in 3.05.05
A problem causing the reception of constant pause frames caused degraded performance has been corrected.

Changes and Enhancements in 3.05.05
A problem where flow limit thresholds, in some cases, were not counting all flows has been corrected.
A problem that prevented some password commands from executing properly during a configuration download has been corrected.
Certain alias table entries are now more human readable.
Syslog messages no longer have milliseconds in the time format.
A problem causing IP helper functionality for user-defined ports to not properly forward frames has been corrected.
A problem causing IGMP open functionality to not function properly has been corrected.
A problem where setting the admin password caused unexpected results when done via a RADIUS authenticated session has been corrected.
Added support for dynamic VLAN assignment (RFC 3580) and policy interaction.

Changes and Enhancements in 3.04.04
Added unknown (unicast) destination frame suppression functionality.
Added functionality to disable MAC address aging in the filter database.
Added functionality to automatically transfer dynamically-learned MAC addresses to static addresses.
A problem with MAC locking delaying the recognition of newly-discovered users has been corrected.
A problem with the RADIUS application shared secret not being correctly accepted and stored has been corrected.
A problem requiring the user to re-enter certain OSPF parameters after issuing an explicit clear command has been corrected.
A problem that could incorrectly apply a deny ACL to a valid flow, even if a specific permit rule existed for the given flow, has been corrected.
A problem affecting the interaction between MAC authentication and MAC locking has been corrected.
A problem where the ‘set LACP disable‘ command in a configuration file would cause LACP to be enabled if downloaded to a switch in which LACP was already disabled, has been corrected.

Changes and Enhancements in 3.03.08
A problem when upgrading from older versions to 3.02.22 with IS-IS packets has been corrected.
A problem when using proxy ARP and the default gateway feature has been corrected.
A problem where configuring an ACL with “permit any any” caused slowness has been corrected.
A problem when changing the Router IDs and not reaching a full adjacency status has been corrected.
A problem with the PWA logout page not closing properly when the switch host and user are not in the same VLAN has been corrected.
A problem where VRRP packets are passed between VLANs has been corrected.
A problem where IP Dest drop rules were dropping EAP packets has been corrected.

Changes and Enhancements in 3.02.24
A problem with resets and erratic behavior with the 03.02.22 image has been corrected.
A problem with performance degradation when ACLs and policies were not applied in tandem has been corrected.
A problem with not being able to correctly flush ARP entries on active trunk ports has been corrected.
A problem with not being able to display the PWA logout page correctly when the host VLAN does not match the port VLAN has been corrected.

Changes and Enhancements in 3.02.22
A problem when making a TFTP copy request where the switch changes the capitalization to lower case resulting in Unix server failures has been corrected.
A problem with the switch sending ping replies incorrectly to an IP address whose MAC has changed when using the a constant ping has been corrected.
A problem with the switch dropping ping packets shortly after the interface's ARP cache has been cleared has been corrected.
A problem with the WebView causing resets when WebView is not in use has been corrected.
A problem with VRRP packets being forwarded between VLANs has been corrected.
A problem with being unable to ping the WebView page with routing enabled has been corrected.
A problem with large numbers of broadcasts being reported as unicasts has been corrected.
A problem when changing an SNMPv3 User to include MD5 and Privacy DES and traps not being sent has been corrected.
A problem with the RAD function assigning a random default gateway has been corrected.
A problem with configuring a 24 bit mask and a ".1" in the last octet has been corrected.
A problem running a "Nessus" DOS attack against the switch has been corrected.
A problem learning the virtual MAC during a VRRP topology change has been corrected.
A problem using priority classification in conjunction when routing to another interface has been corrected.
A problem when using DHCP relay with the switch sending out two discover and two request packets to the server has been corrected.
A problem with timeouts when using MAC authentication with a role applied to the port has been corrected.
A problem with MAC address mobility within a VLAN without a Link Down event has been corrected.
A problem with the configuration file when using the "system lockout" command has been corrected.
A problem with LACP caused by moving MAC addressed to different ports has been corrected.
A problem booting the device as a router from the network where the boot would hang at the SNTP section of the config file has been corrected.
A problem causing a reset when querying via SNMP and\or logging has been corrected.
A problem with the "show dns" command not responding properly when upgrading to 3.02.08 has been corrected.
A problem with routing functionality being affect by receiving short ICMP frames has been corrected.
A problem where an "ACL hit" with ping causes a loss of contact to the switch via ping has been corrected.
A problem with the etherHistoryIndex (port.instance) not incrementing the instance field correctly has been corrected.
A problem with the switch forwarding IEEE unreserved MAC addresses while in the blocking state has been corrected.
A problem with the configuration file when using the "system lockout" command has been corrected.
A number of Enhanced PWA issues have been corrected pertaining to improper redirection.
A problem with downloaded configuration files not functioning properly has been corrected.

Changes and Enhancements in 3.02.08
Added Convergence End Point (CEP) support to automatically discover IP Phones. IP Phone Discovery support in this firmware version includes Cisco, Siemens, and H.323 based phones.
A problem where upon boot up of the unit, 1-5 short frames may egress a gig port has been corrected.
A problem where a unit may reset after a router configuration change or show command has been corrected.
A problem where clearing the node/alias table would reset the unit has been corrected.

Changes and Enhancements in 3.02.08
A problem where multiple policies would not function correctly when applied to the unit has been corrected.
A problem where a link would show 100% utilization with a certain configuration has been corrected.
A problem where the calling station-id field in an EAP packet had an incorrect MAC address has been changed. This field is no longer populated.
A problem where the box would drop multicast packets with a TTL of 1 when switched in the same VLAN has been corrected.
A problem when a user deletes an interface with an active DVMRP stream on it and the unit would reset has been corrected.
When a device is in PWA mode and user access port mode is active/discard with a default role assigned to the port, before the user has authenticated, the port passes traffic based on the settings of the default role. When the port mode is set to active/discard, it should not pass traffic until authentication has occurred. This has been corrected.
Flow Setup Throttling support has been added to this release. Flow Setup Throttling provides additional network protection against various types of network attacks by monitoring the setup of flows on the network and applying thresholds to those flows to alert the network manager and\or take proactive action to reduce and\or eliminate the thread to the network.
Network Management notification via SNMP traps is now supported when new MAC addresses are learned on the device. This capability can be enabled\disabled via CLI and/or SNMP.
The RMON Statistics group is now persistent and will allow up to a total of 192 entries. The RMON History group will now allow up to a total of 288 entries. Previously only 192 entries were allowed.
An issue involving loss of SNMP management support has been corrected. This was due to the improper processing of SNAP encapsulated BPDUs which resulted in rapid bridge topology changes.
An issue involving the support of two ACLs on different interfaces with constant pings being sent has been corrected.
The RADIUS support for entering a device's MAC address into the calling station ID field is now supported.
An issue where logging in as RO allowed the user to view RW level access information in the configuration file has been corrected in this release.
A problem with the Forwarding Database getting out of synch and requiring a "clear arp" to correct the problem, has been corrected.
A problem when configuring two ACLs on a particular port causing packet corruption has been corrected.
The device previously had difficulty handling SNAP Encapsulated BPDU packets and as a result would cause loss of communication to the device's management entity. This has been corrected.
A problem with setting a path cost to a value of 34000 and the affect on the device configuration file has been corrected.
A problem using MAC Authentication where the user is authenticated but in 60 seconds their port reverts back to its previous state has been corrected.
A problem where configuring an ACL on one interface causing packets to be "soft forwarded" on other interfaces, has been corrected.
A problem with Multiple Telnet sessions causing problems with the CLI has been corrected.
An issue with viewing RW information when logged in as RO has been corrected.
An issue with uploading failures for configuration files which have a subset of previously loaded configuration files has been corrected.
An issue with TFTP configuration downloads that affected logging values has been corrected.
An issue with MIBII statistics for the virtual interfaces on the device, has been corrected.
A problem with the CLI display being truncated when the "set SNMP notifyprofile FL-profile targetparam FL-params nonvolatile" is used has been corrected.
A problem with an SNMP "getnext" causing loss of management access to the device has been corrected.
An issue with the "clear node alias port" command causing a reset has been corrected.

Changes and Enhancements in 3.02.08
A problem with the “banner” command causing a system lock up with a “show Config” command has been corrected.
An issue with large numbers of ICMP redirects causing management connectivity loss has been corrected in this firmware version.
An issue involving entering a wrong password when using SSH to connect to the product has been corrected.
An issue with large numbers of outgoing telnet sessions causing the system to lock up over time has been corrected.

Please refer to http://www.enterasys.com/download/download.cgi?lib=e1 and choose the “archive” link to view information on changes previous to the information listed in this document.

KNOWN RESTRICTIONS AND LIMITATIONS:

When downgrading from firmware versions 3.07.14 or later to a firmware version earlier than 3.07.14, only a maximum of two active RADIUS authentication servers and two active RADIUS accounting servers may be configured on the device.
Firmware versions 3.05.09 and later enforce support of a maximum of 1024 VLANs. To downgrade to a firmware version earlier than 3.05.09, you must save and clear the device configuration prior to the downgrade, and then restore the device configuration after the downgrade.
ACLs cannot be applied to multicast traffic. This limitation will not be lifted in future firmware versions.
The “drop VLAN tagged frames” rule is not supported by the Matrix E1. Previous versions would not return a “set failed” when setting the function via NetSight Policy Manager. This version will now return a failure.
BPDUs will no longer be sent from the switch if VLAN 1 is set to disable.
When an individual FE port running spanning tree is changed from an enabled state to a disabled state and then back to enabled (basically a toggle of the port’s status) BPDUs are then not sent out when the port is re-enabled.
If an MGBIC-02 is installed, the device may display erroneous link status LED with no cable connected. Data transfer is not affected.
XMODEM upgrade of the firmware image 3.00.14 or higher requires bootcode of 1.04.00 for the 1H582-25 and 1H582-51. The 3.00.14 firmware may be upgraded via TFTP without upgrading the boot code to 1.04.00.
Jumbo Frames are not supported when the device is configured as a router.
It is recommended that GVRP (if used) be disabled on all edge ports in order to reduce processing overhead. This is especially beneficial when more than 100 VLANs are configured in the network and\or Multiple Spanning Tree instances are configured.
Upon upgrade to version 2.04.x or higher from a previous image, an “admin” user account is created. The admin password will be the same as the previous rw password until changed by the admin user.
Prior to version 2.04.12, port advertise ability values may have become corrupted. If advertise ability is configured to not advertise flow control, upon upgrade to version 2.04.12 or higher, flow control will be advertised. If desired, flow control advertise ability should be disabled after upgrade to 2.04.12 or higher.
Prior to version 2.04.12, port advertise ability values may have become corrupted. Upon upgrade to 2.04.12 or higher, port advertised ability values will be returned to the default values. If desired, port advertise ability values should be re-configured. Manual settings for port speed, duplex, and flow control will remain intact.
The SNTP client will not respond to subnet broadcasts. Unicast mode and broadcast mode are fully supported.
The Matrix E1 will respond to ICMP requests from VLANs of which it is not a member.
When configuring port trunking with 10/100 ports, the ports in the trunk group must reside on the same block of 8 10/100 ports.
In order to upgrade to boot code 1.01.00 on a 1H582-51 via network download, the unit must first be running firmware version 2.01.x or higher.
In order to upgrade to boot code 1.02.00 on a 1H582-51 via network download, the unit must first be running firmware version 2.03.x or higher.
When configuring RIP authentication, multiple keys are not supported.
RIP route distribution filtering is not supported.
Multicast group memberships will be flushed when a port in the trunk group that is part of the multicast group is disconnected. The groups will be relearned; this may cause a temporary pause in the multicast application.
It is recommended to pre-configure trunk ports prior to installation of this product. By the nature of port trunking, a temporary data loop condition may result when the links are transitioned to trunk ports.
OSPF Auto Virtual links are not supported in this firmware version.
OSPF authentication can be enabled only on a per area basis.
If an OSPF area is created as a regular area then changed to a stub area, the Matrix E1 will need to be reset in order to properly filter the routes from the stub area.
Router configuration is not available via WebView.

Hot swapping of uplink modules is not supported. The system must be powered down before uplink modules can be installed or removed.
Support for Enterasys PVST is not planned for the Matrix E1. The Matrix E1 supports the standard 802.1s for multiple spanning trees.
The 1G582-09 does not support boot code upgrade via network download.
WebView does not support the configuration of GVRP, CDP, or Dynamic Egress in this firmware version.
The ability to rewrite the TOS/DSCP for SNAP, 802.3 and 802.2 IP frames is not supported in this firmware version. TOS/DSCP rewrite does operate properly for Ether II IP frames.
When port mirroring between two Gigabit Ethernet ports, it has been occasionally observed that if the data rates exceed 850Mb/s, the switch may not properly learn new addresses, and flooding could occur temporarily.
The port speed for the 1G-2TX and 1G582-09 cannot be configured manually for 1000 Mbps.
Spanning tree must be enabled on ports using IBM type 1 cabling to provide Loopback detection.
The “Show VLAN Port Info” commands are listed in the documentation but are not supported in this version.

For the most up-to-date information concerning known issues, go to the **Global Knowledgebase** section at http://www.enterasys.com/support/. For the latest copy of this release note, go to http://www.enterasys.com/services/support/downloads/. To report an issue not listed in this document or in the **Global Knowledgebase**, contact our Technical Support Staff.

STANDARD MIB SUPPORT:

RFC No.	Title
RFC 1213	MIBII
RFC 1493	Bridge MIB
RFC 1757	RMON MIB
RFC 2271	SNMP-FRAMEWORK-MIB
RFC 2272	SNMP-MPD-MIB
RFC 2273	SNMPv3 Applications
RFC 2574	SNMP-USER-BASED-SM-MIB
RFC 2575	SNMP-VIEW-BASED-ACM-MIB
RFC 2576	SNMP-COMMUNITY-MIB
RFC 2620	RADIUS Accounting MIB
RFC 2665	802.3 MAU MIB
RFC 2668	Ethernet-like Interface Type MIB
RFC 2674	802.1p\Q MIB
RFC 2737	Entity MIB (physical branch only)
RFC 2863	IF-MIB
RFC 2933	IGMP MIB
NA	IEEE 8021-PAE-MIB
NA	IEEE8023 LAG MIB

ENTERASYS NETWORKS PRIVATE ENTERPRISE MIB SUPPORT:

Title and Version	Title and Version
Ctenviron-mib	Ct-priority-classify-mib
Ct-vlan-classify-mib	Ctron-cdp-mib
Ctbroadcast-mib	Ctron-timed-reset-mib
Ctdownload	Ctron-rate-policing-mib
Enterasys-radius-auth-client-encrypt-mib	Ctron-alias-mib
Enterasys-mac-locking-mib	System-resource-mib
Ctron-q-bridge-mib-ext-mib	Enterasys-policy-profile-mib
Enterasys-mac-authentication-mib	ctif-ext-mib
Enterasys-configuration-management-mib	Enterasys-mstp-mib
Enterasys-pwa-mib	enterasys-radius-acct-client-ext-mib
enterasys-syslog-client-mib	enterasys-ieee8023-lag-mib-ext-mib
enterasys-diagnostic-message-mib	etsysVlanAuthorizationMIB
etsysPolicyRFC3580Map	

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

SNMP TRAP SUPPORT:

RFC No.	Title
RFC 1213	ColdStart Link Up Link Down Authentication Failure
RFC 1493	New Root Topology Change
RFC 1757	RisingAlarm FallingAlarm

ENTERASYS NETWORKS' PRIVATE ENTERPRISE TRAP SUPPORT:

Title	
wgPsRedundant	wgPsNotRedundant
wgPsNormal	wgPsFail
etsysMACLockingMACViolation	etsysIetfBridgeDot1dBasePortNewLearnedAddrTrap

RADIUS Authentication and Authorization Attributes

Attribute	RFC Source
Called-Station-Id	RFC 2865, RFC 3580
Calling-Station-Id	RFC 2865, RFC 3580
Class	RFC 2865
EAP-Message	RFC 3579
Event-Timestamp	RFC 2869

Attribute	RFC Source
Filter-Id	RFC 2865, RFC 3580
Framed-IPv6-Pool	Not Supported
Framed-MTU	RFC 2865, RFC 3580
Framed-Pool	Not Supported
Idle-Timeout	RFC 2865, RFC 3580
Message-Authenticator	RFC 3579
NAS-Identifier	RFC 2865, RFC 3580
NAS-IP-Address	RFC 2865, RFC 3580
NAS-IPv6-Address	Not Supported
NAS-Port	RFC 2865, RFC 3580
NAS-Port-Id	RFC 2865, RFC 3580
NAS-Port-Type	RFC 2865, RFC 3580
Password-Retry	Not Supported
Service-Type	RFC 2865, RFC 3580
Session-Timeout	RFC 2865
State	RFC 2865
Termination-Action	RFC 2865, RFC 3580
Tunnel Attributes	RFC 2867, RFC 2868, RFC 3580
User-Name	RFC 2865, RFC 3580
Vendor-Specific	Not Supported

RADIUS Accounting Attributes

Attribute	RFC Source
Acct-Authentic	RFC 2866
Acct-Delay-Time	RFC 2866
Acct-Input-Octets	RFC 2866
Acct-Input-Packets	RFC 2866
Acct-Interim-Interval	RFC 2866
Acct-Output-Octets	RFC 2866
Acct-Output-Packets	RFC 2866
Acct-Session-Id	RFC 2866
Acct-Session-Time	RFC 2866
Acct-Status-Type	RFC 2866
Acct-Terminate-Cause	RFC 2866
Calling-Station-Id	RFC 2865

GLOBAL SUPPORT:

By Phone: 978-684-1000
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/services/support/contact/

By Email: support@enterasys.com

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

By Fax: 978-684-1499

By Mail: Enterasys Networks, Inc.
50 Minuteman Road
Andover, MA 01810 (USA)

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.