145 Rio Robles
San Jose, CA 95134
+1 877-801-7082

Customer Release Notes

B-Series B3

Firmware Version 6.61.16.0002
April 2016

INTRODUCTION:

This document provides specific information for version 6.61.16.0002 of firmware for the following B3 products:

B3G124-48	B3G124-48P	B3G124-24	B3G124-24P

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

For the latest firmware versions, visit the download site at:
http://support.extremenetworks.com/

FIRMWARE SPECIFICATION:

Status	Version No.	Type	Release Date
Current Version	6.61.16.0002	Maintenance Release	April 2016
Previous Version	6.61.15.0003	Maintenance Release	September 2015
Previous Version	6.61.14.0006	Maintenance Release	May 2015
Previous Version	6.61.13.0006	Maintenance Release	November 2014
Previous Version	6.61.12.0005	Maintenance Release	April 2014
Previous Version	6.61.11.0006	Maintenance Release	December 2013
Previous Version	6.61.10.0008	Maintenance Release	September 2013
Previous Version	6.61.09.0012	Maintenance Release	August 2013
Previous Version	6.61.08.0013	Maintenance Release	April 2013
Previous Version	6.61.07.0010	Maintenance Release	October 2012
Previous Version	6.61.06.0009	Maintenance Release	August 2012
Previous Version	6.61.05.0009	Maintenance Release	July 2012
Previous Version	6.61.03.0004	Maintenance Release	April 2012
Previous Version	6.61.02.0007	Feature Release	March 2012
Previous Version	6.42.11.0006	Maintenance Release	February 2012
Previous Version	6.42.10.0016	Maintenance Release	December 2011
Previous Version	6.42.09.0005	Maintenance Release	August 2011
Previous Version	6.42.08.0007	Maintenance Release	July 2011
Previous Version	6.42.07.0010	Maintenance Release	May 2011
Previous Version	6.42.06.0008	Maintenance Release	April 2011

Status	Version No.	Type	Release Date
Previous Version	6.42.05.0001	Maintenance Release	March 2011
Previous Version	6.42.03.0004	Maintenance Release	January 2011
Previous Version	6.42.02.0006	Maintenance Release	December 2010
Previous Version	6.42.01.0064	Maintenance Release	November 2010
Previous Version	6.03.08.0012	Maintenance Release	October 2010
Previous Version	6.03.06.0008	Maintenance Release	August 2010
Previous Version	6.03.05.0004	Maintenance Release	June 2010
Previous Version	6.03.04.0004	Maintenance Release	April 2010
Previous Version	6.03.03.0008	Maintenance Release	February 2010
Previous Version	6.03.02.0006	Maintenance Release	November 2009
Previous Version	6.03.01.0008	Maintenance Release	September 2009
Previous Version	6.03.00.0022	Feature Release	June 2009
Previous Version	1.02.06.0004	Maintenance Release	June 2009
Previous Version	1.02.05.0004	Maintenance Release	April 2009
Previous Version	1.02.04.0005	Maintenance Release	March 2009
Previous Version	1.02.03.0012	Maintenance Release	January 2009
Previous Version	1.02.02.0009	Maintenance Release	November 2008
Previous Version	1.02.01.0004	Feature Release	September 2008
Previous Version	1.01.06.0007	Maintenance Release	August 2008
Previous Version	1.01.06.0006	Maintenance Release	August 2008
Previous Version	1.01.05.0004	Maintenance Release	July 2008
Previous Version	1.01.04.0001	Maintenance Release	June 2008
Previous Version	1.01.03.0003	Maintenance Release	May 2008
Previous Version	1.01.02.0007	Maintenance Release	March 2008
Previous Version	1.01.01.0051	Maintenance Release	March 2008
Previous Version	1.01.01.0049	Maintenance Release	February 2008
Previous Version	1.01.01.0047	Maintenance Release	January 2008
Previous Version	1.01.01.0040	Maintenance Release	December 2007
Previous Version	1.01.01.0039	Feature Release	December 2007
Previous Version	1.00.86	Customer Release	August 2007
Previous Version	1.00.74	Customer Release	March 2007
Previous Version	1.00.34	Customer Release	January 2007
Previous Version	1.00.31	Customer Release	December 2006
Previous Version	1.00.30	Customer Release	December 2006
Previous Version	1.00.29	Initial Release	November 2006

HARDWARE COMPATIBILITY:

This version of firmware is not compatible with the B2 platforms. If you mix a B3 in a stack with B2 switches, you must download the B2 image 4.02 and apply it to all members of the stack.

BOOTPROM COMPATIBILITY:

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

NETWORK MANAGEMENT SOFTWARE SUPPORT:

Network Management Suite (NMS)	Version No.
NMS Automated Security Manager	6.2
NMS Console	6.2
NMS Inventory Manager	6.2
NMS Policy Manager	6.2
NMS NAC Manager	6.2

If you install this image, 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.

PLUGGABLE PORTS SUPPORTED:

MGBICs	Description
MGBIC-LC01	1000Base-SX, IEEE 802.3 MM, 850 nm Short Wave Length, 220/550M, LC SFP
MGBIC-LC03	1000Base-SX-LX/LH, MM, 1310 nm Long Wave Length, 2 KM, LC SFP
MGBIC-LC07	Extended 1000Base-LX, IEEE 802.3 SM, 1550 nm Long Wave Length, 110KM, LC SFP.
MGBIC-LC09	1000Base-LX, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 KM, LC SFP
MGBIC-MT01	1000Base-SX, IEEE 802.3 MM, 850 nm Short Wave Length, 220/550 M, MTRJ SFP
MGBIC-02	1000Base-T, IEEE 802.3 Cat5, Copper Twisted Pair, 100 M, RJ45 SFP
MGBIC-08	1000Base-LX/LH, IEEE 802.3 SM, 1550 nm Long Wave Length, 80 KM, LC SFP
MGBIC-BX10-D	1000Base-BX10-D Single Fiber SM, Bidirectional, 1490nm Tx / 1310nm Rx, 10 km, Simplex LC SFP (must be paired with MGBIC-BX10-U)
MGBIC-BX10-U	1000Base-BX10-U, 1 Gb, Single Fiber SM, Bidirectional 1310nm Tx / 1490nm Rx, 10 km, Simplex LC SFP (must be paired with MGBIC-BX10-D)
MGBIC-BX40-U	1 Gb, 1000Base-BX40-U Single Fiber SM, Bidirectional, 1310nm Tx / 1490nm Rx, 40 Km, Simplex LC SFP (must be paired with MGBIC-BX40-D)
MGBIC-BX40-D	1 Gb, 1000Base-BX40-D Single Fiber SM, Bidirectional, 1490nm Tx / 1310nm Rx, 40 Km, Simplex LC SFP (must be paired with MGBIC-BX40-U)
MGBIC-BX120-D	1 Gb, 1000Base-BX120-D Single Fiber SM, Bidirectional, 1590nm Tx / 1490nm Rx, 120 Km, Simplex LC SFP (must be paired with MGBIC-BX120-U)
MGBIC-BX120-U	1 Gb, 1000Base-BX120-U Single Fiber SM, Bidirectional, 1490nm Tx / 1590nm Rx, 120 Km, Simplex LC SFP (must be paired with MGBIC-BX120-D)

NOTE: Installing third party or unknown pluggable ports may cause the device to malfunction and will void your warranty.

PRODUCT FEATURES:

What's New in 6.61

Spanning Tree Diagnostic MIB - Support for the Enterasys Spanning Tree Diagnostic MIB.
MSTP Multisource Detection - Checks for a change in the source MAC address of received BPDUs. Once detected this information is used to change the Spanning Tree point-to-point status of LAN on the given port.
MAC Locking clearonlinkchange – Support for the optional ability to maintain first arrival MAC addresses on a port with a change in link status.
MAC Locking Threshold Notification – Support for notification when the MAC address tables threshold is reached.
Time Based Reset – Support for the ability to add time and date to the reset command.
Flexible Link Aggregation Groups – Support for configurable group limits.
Service Access Control Lists (SACL) - Provide security for switch management features, by ensuring that only known and trusted devices are allowed to remotely manage the switch via TCP/IP. A Service ACL may be applied to a specific host service (i.e. Telnet, SNMP, SSH, HTTP).
Access Control Lists – Added support for IPv6 and MAC based ACLs. Added queue assignment action to ACLs Note: ACLs are not supported simultaneously with Policy.
Increased Password Security – Supports new password options including: complexity, history, and aging. Passwords can be encrypted using a FIPS 1402 approved algorithm.
Login Banner – Added support for a login banner with required user acceptance, in addition to the post login Message of the Day banner. **Warning:** Configuration files containing login banners should not be used on pre-6.61 images
VLAN Classification – Added support for standalone "VLAN Association" application, for subnet, protocol and MAC based VLAN classification.
Password Reset Button Enhancements – Now supports ability to disable/enable the password reset button. The default admin login account will now be restored, as well as the default password.
OpenSSL FIPS Object Cryptographic Module – This module replaces previous software libraries used for encryption. This module is FIPS 140-2 validated when run in the C2 security profile.
IPsec for RADIUS transactions – Secures RADIUS transactions, including encryption of passwords passed via RADIUS.
Command Logging – Support for command logging added.
SNTP Server-Client Authentication - Authentication ensures that any response received from an SNTP time server has come from the intended reference.
Console Disconnect – Support added for Console disconnect through the use of VT100 terminal emulation.
VLAN 4094 – VLAN 4094 is no longer reserved for stacking. **Note:** 6.61 will not stack with previous images.
Mixed Strict and WRR Port Transmit Queue settings – Extended the "port txq" command to support mixing one or more queues in strict priority with queues running in WRR.
Security Log – Added support for an undeletable security log that can only be read by the administrator.
Secure directory – Created a secure directory that can only be accessed by a super-user. This directory contains no files by default but may be used to load and store configuration files.

Existing Product Features	
Multi-user authentication per port (up to 3 policy users per port)*	IP Forward-Protocol command
Multiport LAG to single port LAG automatic failover	ARP Spoof Protection
DHCP Spoof Protection	High-Temperature Alerts
Control mdi/mdix port settings via CLI to prevent network loops	Show support command
TDR-based cable status check detects cable breaks and disconnections	24 Gbps Full Duplex (48 Gbps bidirectional) closed-loop stacking
Enterasys Policy (role-based L2/L3/L4 access control, QoS, and rate limiting)*	Selectable MAC Hashing Algorithms
802.1D	Auto-Negotiation
802.1Q - VLAN Tagging	8 Priority Queues per Port (user mapping to 6 queues)
802.1p - Traffic Management	Session-Timeout and Termination-Action RADIUS Attributes Support
802.3x Flow Control	Ability to Set Port Advertised Ability via CLI
802.3ad – Dynamic and Static Creation for Link Aggregation	Multi-method Authentication*
802.1s – Multiple Spanning Tree Protocol (up to 4 instances)	Multiple RFC3580 Users per port (up to 3)
802.1w – Rapid Spanning Tree	User + IP Phone Authentication*
RFC-3580 t based on 802.1X, PWA or MAC Authentication	L2 Policy Rules*
Spanning Tree Backup Root	COS based Inbound Rate Limiter per Policy User*
Spanning Tree Loop Protect	DHCP Server
LLDP/LLDP-MED	Web Authentication (PWA)*
Legacy Path Cost	Web Redirect – PWA+ and URL redirection*
Spanning Tree Pass Through	802.1X Authentication
SpanGuard	Non-Strict 802.1X Default RFC 3580 With Auth Failure
Link Flap Detection	RADIUS Client
Per Port Broadcast Suppression	Turn Off RADIUS Authentication (RADIUS Realm)
Port Mirroring (Single instance)	Queuing Control Strict and Weighted Round Robin
Protected Port (Private VLAN)	MAC Authentication / MAC Authentication Masking
Cabletron Discovery Protocol (CDP)	MAC Authentication Retained After Age Out
Cisco Discovery Protocol (CDP) v1/2	RADIUS Accounting for MAC Authentication
Cisco IP Phone Discovery	EAP pass-through
GVRP	VLAN marking of mirrored traffic – Edge only
IGMP v1/v2/v3 and IGMP Snooping	Dynamic and Static MAC Locking
Syslog	Dynamic Egress
Text-based Configuration Upload/Download	SSHv2 Support
CLI Management	WebView
Telnet Support	SSL Interface to WebView

Existing Product Features	
IPv4/IPv6 Dual Host Management Support (SNMP,Telnet,SFTP,SCP,SSH,RADIUS)	RMON (4 groups)
Discard VLAN Tagged Frames	RMON View in the CLI With Persistent Sets
Jumbo Frame (up to 9K)	RMON Packet Capture/Filtering Sampling
Priority Classification L3-L4*	SNMPv1, SNMPv2c, SNMPv3
VLAN-to-Policy Mapping on a per Port Basis*	Simple Network Time Protocol (SNTP)
Node/Alias Table	User selectable code points for Voice over IP via DiffServ
ToS Rewrite*	Alias Port Naming
DiffServ	Ability to Set Time and Date via the MIB
Packets can be dropped, shaped, marked (with an IP DSCP or IP precedence value), or sent unchanged to the switching process.	Configurable Login Banner
Basic IPv4 Routing (static, RIP v1/v2, IRDP)	CPU/Memory utilization monitoring via SNMP
Multiple IP Helpers per Interface (up to 6)	SMON MIB support for Port Mirroring
ACLs	sFlow
CoS MIB based Flood Control (broadcast, multicast, and unknown unicast)	ACLs per VLAN
Hybrid Policy Mode*	Host Protect
VLAN-to-Policy Mapping*	AES-128 support with SNMPv3
LLDP-MED Network-Policy TLV	Selectable management interfaces
TACACS+	Copy & Paste
Extended ACLs	Power Supply & Fan Monitoring via SNMPv3
Secure Copy / Secure FTP	New MAC Trap
Display 802.3 pause counters	Serviceability enhancements
Support for 5M cables	Tx Queue Monitoring

*With purchase of the optional Policy license.

INSTALLATION AND CONFIGURATION NOTES:

WARNING:

- Direct firmware upgrades to 6.61 from 6.03 (and previous) images may result in the loss of some configuration. It is recommended to upgrade to 6.42 prior to loading 6.61. Alternatively the configuration may be saved to a file and reloaded after upgrade.
- 6.61.05.009 contains new boot PROM code that will be programmed into the PROM the first time the image is booted. This process should take less than 3 minutes and the switch will reboot itself once PROM programming is complete. Do not remove power during this process. If the process of programming is interrupted it may leave the switch in an unrecoverable state.
- A 6.61 (or later) stack will not detect a switch that is added to the stack if it is running any code release prior to 6.61. Any switch added to a 6.61 (or later) stack MUST be individually upgraded to 6.61 (at a minimum) PRIOR to attempting to add the switch to the stack
- Configuration files containing a login banner may suspend operation of images prior to 6.61. This state can only be corrected by clearing the configuration through the boot PROM. Use extreme caution when using a configuration file. Login banners will automatically be removed from the configuration when back revving to pre- 6.61 images.

Note:

- The STK-RPS-500PS should NOT be used with the B3. If you do connect a STK-RPS-500PS to a B3 PoE switch, the STK-RPS-500PS will automatically become the PRIMARY power supply for the switch - this is due to the logic in the switches for selecting the power supply with the higher voltage as the primary supply. The internal power supply on the switch will NOT act as a backup to the RPS since the over-voltage protection of the internal power supply will kick in when it senses the additional voltage (6 volts higher) of the RPS. The only way to get the internal power supply out of the over-voltage protection mode is to remove power to the switch and reboot the switch.
- If VLAN 4094 is provisioned in firmware 6.61, it must be removed prior to backreving to firmware 6.42 as VLAN 4094 is not supported in release 6.42. Failure to remove VLAN 4094 could potentially cause issues loading certain Layer 3 parameters.
- As a best practice, Extreme Networks recommends that prior to upgrading or downgrading the firmware on your switch, you save the existing working configuration of the system by using the **show config outfile** configs/<*filename*> command. Please note that you will need a copy of your previous configuration if you need to back-rev from 6.61.xx.xxxx to the previous firmware version.

The B3 most likely will not be shipped to you pre-configured with the latest version of software. It is strongly recommended that you upgrade to the latest firmware version BEFORE deploying any new switches. Please refer to http://support.extremenetworks.com/ for the latest firmware updates to the B-Series B3 and follow the TFTP download instructions that are included in your B3 Configuration Guide.

Soft copies of the B3 Configuration Guide are available at no cost on the Extreme Networks web site, http://support.extremenetworks.com/

The B3 family of stackable switches is managed by a single IP address for a stack of up to 8 switches.

In order to download the new software to a stack of B3 switches, simply follow the instructions to upgrade a switch with new software. The system will then automatically download the new software to all the members in the stack controlled by that stack manager.

Policy Capacities

Policy roles (profiles) per system	15
Number of users per port	Tunnel Mode = 3, Policy Mode = 3, Hybrid Mode = 3
Number of unique rules per system	768
L3/L4 rules	512
EtherType rules	128
MAC rules	128
Number of rules per single role	100
Number of masks	No Limit
COS rate limiting (IRL)	Yes
Role-based rate limiting	Yes
Rule-based rate limiting	No
Priority-based rate limiting	No
Fixed rule precedence	Yes
VLAN to policy mapping**	Assign VLAN traffic to use a specific policy
Rule Types	
EtherType*	VLAN/cos/drop/forward***
MAC dest / MAC source	Cos/drop/forward
IP Protocol	Cos/drop/forward
IP dest socket / IP source socket	Cos/drop/forward
IP TOS	Cos/drop/forward

TCP dest port / TCP source port	Cos/drop/forward
UDP dest port / UDP source port	Cos/drop/forward
ICMP Type	No

* The EtherType to VLAN mapping rule is supported only when ‘numusers’ (number of users allowed to authenticate on a port) is set to 1.

** The VLAN to policy mapping rule is supported only when ‘numusers’ (number of users allowed to authenticate on a port) is set to 2 or greater.

*** When configuring EtherType to VLAN rules, there is a maximum of 7 VLAN rules per profile

Diffserv Limits (System Limits, not per Port)

Max number of Classes	25
Max number of Rules per Class	6
Max number of Rules	150
Max number of Policies	12
Max number of Policy Instances	120
Max number of Instances per Policy	10
Max number of Policy Attributes	120
Max number of Attributes per Policy Instance	1
Max number of Ports	120

Router Capacities

The following table defines the router capacities:

Feature	Capacity
ARP Dynamic	2024
ARP Static	512
Route Table	2500
Static Routes	64
RIP Routes	2500
IP Interfaces	24
Secondary IP addresses per Interface	31
IP Helper Address	6 per interface
Access Rules (inbound only)	100
Access Rules – Per ACL	9
IGMP Groups	256

sFlow Capacities

Feature	Capacity
Number of sFlow pollers	unlimited
Number of sFlow samplers	32

FIRMWARE CHANGES AND ENHANCEMENTS:

Changes and Enhancements in 6.61.16.0002
19644 Corrected an issue in port mac locking that could result in a ““nim_events.c(213)” reset event
19511 Corrected a potential loss of management and eventual reset condition seen when monitoring the etsysResourceUtilizationMIB.
19608 Corrected a potential reset condition when attempting to save a prompt (“set prompt”), of 50 or more characters.
19649 Corrected an issue in the display of radius server configuration that could erroneously be detected as a configuration change.
19656 Corrected a memory utilization issue with RW user accounts that resulted in the message “System memory is too low to complete new cli tree operation”.
19652 Corrected an issue with processing LLDP packets that could result in a reset with the message “ Last switch reset was caused by buff.c(546):”
19643 Corrected a reset condition resulting in the message “dot1s_task(0xac24038) + broad_l3_mcast.(2766):Error 0xFFFFFFFC”.
19320 Corrected an issue where the SNTP server table is restored in reverse order from entry Configuration.

Changes and Enhancements in 6.61.15.0003
19553 Corrected a potential reset condition when processing jumbo 802.1x and 802.1s control frames
19484 Corrected a logic error with handling of an apostrophe as the second character of a system login. This error previously resulted in the incorrect storage of the password.
19588 Corrected a reset issue in the LLDP application, which produced the log entry, “reset caused by buff.c(546)”
19557 Corrected an issue where LC-04 and LC-05 MGBICs are recognized properly but will not provide link.
18590 Addressed an issue in the IGMP snooping application that could result in a reset with the error message, “nim_events.c(213): Error code 0x0000BADD”
19528 Corrected an issue in the TFTP application that may have resulted in corrupted file transfers.
19450 Corrected an issue in the output of the "show vlan portinfo vlan" command, where some egress ports may not be displayed.
19581 Addressed an issue in host packet processing that could result in a reset with the error message, “edb_bxs.c(1314) 286 %% Last switch reset caused by Fault(0x00000E00) SRR0(0x01554000)”
19583 Corrected a memory loss issue in SNMP trap processing that could result in a reset.
19579 Corrected an issue where the “set length" command was not persistent.
19578 Corrected a reset caused by the lack of the memory nessary to support multiple simultaneous user accounts.
19586 Corrected an issue where the snmpEngineTime (1.3.6.1.6.3.10.2.1.3) MIB value rolled over after 497 days of system uptime instead of the maximum allowed 24855 days.

Changes and Enhancements in 6.61.14.0006
Modified Spanning Tree loop protect behavior to disable a protected port when in a state where multiple BPDU sources have been detected.

Changes and Enhancements in 6.61.14.0006
19534 Corrected an SNMP issue within the ctChasPowerTable where power supply redundancy may be incorrectly returned.
19440 Added support for ifMauType dot3MauType10GigBaseSR, dot3MauType10GigBaseER, and dot3MauType10GigBaseLR.
19267 Corrected an issue that could prevent SFPs from linking on bootup if auto-negotiation is disabled.
19276 Corrected an issue where ports could erroneously be removed from link aggregations. This could result in users MAC addresses being learned on incorrect ports.
19332 Corrected a reset issue in the SNMP Task that resulted in the message “edb_bxs.c(1314) 73 %% Last switch reset caused by Fault(0x00000300) SRR0(0x01104270) ESR(0x00800000) MSR(0x00000200) DEAR(0x0000000C) IMISS(0x01104270)”.
19377 Corrected an issue that prevented the disabling of an admin login account from being persistent.
19334 Corrected a potential reset condition that resulted in the message “Task IGMP(0xc73a978) is suspended with error 2”.
19241 Corrected an issue where erroneous POE traps “etsysPseChassisPowerNonRedundant” and “etsysPseChassisPowerRedundant” were transmitted.
19318 Corrected an issue where the “set length” command was not persistent.
19366 Corrected an issue where the output of “show lldp port remote-info” was missing remote-info POE Device-Type information.
19372 Added support for the ability to separately configure RADIUS and RADIUS accounting parameters.
19282 Corrected an issue that could cause the CLI to lock.
19437 Corrected a reset issue concerning the LLDP POE tx-tlv option which resulted in the message “NIM B3 reset 0x0000BADD caused by nim_t :Task ID:0x0a6dcd20”.
19434 Corrected a reset issue which resulted in the message “Nim_T reset due to TASK 0x0a758ec0”.
19383 Corrected a potential method of corrupting the startup configuration file. This may previously have resulted in the continuous rebooting of the system on power up.

Changes and Enhancements in 6.61.13.0006
18907 Corrected an issue that prevented clearing SNMP community name public, using the NetSight Configuration Template.
19300 Corrected a message queuing issue with the resulting log entry, “RADIUS: Msg Queue is full! Event”.
19305 Corrected an issue where the LLDP protocol was not processed on unauthenticated ports.
19311 Corrected an issue that may prevent a gratuitous ARP from being transmitted from a newly elected master after a stack master switch failover.
19196 Addressed an issue which allowed corrupted DHCP packets, to be looped back on dhcpsnooping trusted ports.
18907 Corrected an issue that prevented clearing the SNMP community name public using NetSight.
18587 Corrected an issue where SSH sessions were misidentified as Telnet sessions, in syslog messages.
19288 Corrected an issue that prevented Cisco Voice Gateway dot1x authentication.
19271 Corrected a potential reset “Fault(0x00000D00)”, caused by a memory leak in SNMP processing.

Changes and Enhancements in 6.61.13.0006
19287 Corrected a reset condition generated when an invalid index was used in the CTRON chassis MIB.
19257 Corrected an issue with Policy CoS rate limiter implementation that could cause loss of Spanning Tree BPDUs.
18943 Corrected an issue with MGBIC-LC04 support, that may have resulted in the failure to link on system boot.
18499 Corrected an issue that prevented identification of Avago MGBIC-LC04s.
18870 Corrected a potential reset condition in the “snoopTask” task, which produced the log entry, “sal.c(1197): Error code 0x00000000”.
18880 Corrected an issue where Initiating a Secure Copy (SCP) file transfer could result in loss of management.
18990 Corrected an issue where the Spanguard application will lock a port on receiving an LLDP packet with a destination MAC of 01:80:C2:00:00:00.
19249 Modified the logging behavior of SNTP to prevent excessive changed system time messages, “sntp_client.c(2109) 62 %% SNTP has changed system time”.
16086 Attempt to recover from a L2 table DMA error that previously resulted in a reset with a log entry of: “soc_l2x_thread DMA failed too many times”. On an L2 Table DMA failure we will now walk the table to find the corrupted entry and remove it. The expected warning message is: “warning soc_l2x_thread: Bad L2 table entry found. Recovering”.
19163 Corrected a potential reset condition in the “ipMapForwardingTask” task, which produced the log entry, “sal.c(1184): Error code 0x00000000”.

Changes and Enhancements in 6.61.12.0005
19033 Corrected an issue in TACACS command accounting, where the receipt of an unknown TACAC reply packet caused the CLI to become unresponsive.
19076 Modified the SNTP protocol to insure that the UDP source port will not be equal to the UDP destination port.
18793 Patched updates to SSH to address the following Common Vulnerabilities and Exposures (CVEs): CVE-2006-4925, CVE-2012-0814, and CVE-2008-1657. Note: Scan tools that report potential vulnerabilities based on SSH version may still report these.
18455 Addressed an issue in the SSH application that could result in a reset with the error message, “Fault (0x00000E00) Task EDB BXS”.
18490 Corrected an issue in Spanning Tree Loop Protection on aggregated ports, which could cause the port to inadvertently become locked.
18711 Addressed an issue in the IGMP application that could result in a reset with the error message, “nim_events.c(216) 593 %% NIM: Timeout event(UP) on unit(1) slot(0) port(46)(intIfNum(46)) for components(IGMP_SNOOPING)”
18861 Added support for the ctAliasEntryClearAll object of the Ctron Alias MIB.
18864 Corrected an issue with timed resets, where the current configuration would be saved automatically even if the SNMP persistmode was set to manual.
18891 Corrected an issue in the output of “Show spantree stats active”, which displayed the incorrect role for the physical ports that are currently a member of an aggregation.
18931 Syslog messages will now be generated on SNMP user authtication failure.

Changes and Enhancements in 6.61.11.0006
18691 Corrected an issue in the implementation of the Enterasys Resource Utilization MIB, where setting etsysResource1minThreshold to zero, did not prevent etsysResourceLoad1minThresholdExceeded notifications.
18761 Corrected an issue where etsysMACLockingMACViolation traps could erroneously be generated.
18466 Corrected one potential cause of a reset that would result in the error message “reset caused by prefix.c(1941): Error code 0x00000000 IGMP”.

Changes and Enhancements in 6.61.10.0008
18584 Addressed an issue in MAC Locking application that could result in a reset with the error message, “nim_events.c(213): Error code 0x0000BADD”
18569 Corrected an issue with the interaction of MAC Locking and 802.1x, which could prevent client network access.
17978 Corrected an issue with TACACS+ management authentication, where local authentication was not allowed when TACACS+ server was unreachable.
18383 Addressed a reset memory corruption issue that could result in a system reset.
18483 Corrected an issue with the “show reset” command which prevented the display of scheduled resets.
18494 Corrected an issue with the MIB object etsysConfigMgmtChangeDelayTime that prevented the use of scheduled resets.
18550 Added password support for the “! “ character. Previously its use would result in an additional space being added to the end of the password string on reset.
18596 The "clear snmp community <name>" command will now remove the community name when using the encrypted community name. The command will not work without specifying one or the other.
18421 Corrected an issue where the Policy application allowed 802.1x supplicant EAP packets to be leaked to other ports.

Changes and Enhancements in 6.61.09.0012
17514 Corrected an issue that prevented DiffServ application policies from being applied to hardware. Previously a “set diffserv service add” command resulted in the message, “Could not attach the Policy”.
16911 Corrected the output of the “show logging default” command to display the correct severity value.
18449 Corrected the timestamp of Radius Accounting packets to account for day light savings.
17297 Addressed a potential SSH session lockup when attempting to perform a “show support” command.
17263 Corrected the format of lldpStatsRemTablesInserts in the LLDP MIB.
17116 Corrected the inability to append to a configuration file that has flow control disabled.
17957 Addressed an issue where a port could stop learning MAC addresses if the policy maptable response was set to both (i.e. Hybrid authentication mode).
18012 Added support for the etsysRadiusAcctClientMIB
18194 Corrected the inability to access the network from a port in “force-auth”, with multiauth mode set to strict, and maclocking firstarrival set to 1.

Changes and Enhancements in 6.61.09.0012
18231 Corrected an issue where the VLAN returned by RADIUS as a result of an RFC 3580 VLAN Authorization, fails to be applied to the user, when the MultiAuth mode is strict.
18275 Packets with an invalid destination mac address (All zero's) are now dropped.
18281 Corrected an issue where “sys-des” option was not persistent in LLDP commands.
18369 Corrected an issue where Dynamic ARP Inspection (DAI) was not functioning on VLAN authenticated ports.
18378 Corrected an issue with the Spanning Tree Diagnostic MIB, which prevented operation with NetSight flexviews.
18432 Corrected an that issue resulted in the message “Policy_dist: Mac-vlan error adding macAuth user”, and prevented adding the authenticating users VLAN attribute from being applied correctly to hardware.
18458 Corrected an issue where enabling MSCHAPv2 for management authentication, prevented user authentication via RADIUS.
18461 Corrected a display issue where “show multiauth session”, still showed MAC authenticated users, when the port was down.

Changes and Enhancements in 6.61.08.0013
16442 Corrected an issue with DHCP relay agent that could prevent completion of the DHCP process.
16911 Corrected incorrect values displayed in the output of the “show logging default” command.
17038 Corrected an issue with failing to timeout TACACS+ transactions. Loss of contact with the TACACS server could have resulted in loss of switch management.
17046 Addressed potential loss of configuration when upgrading image from 6.3
17081 Adapted disputed BPDU algorithm to support Cisco 2950 MSTP/RSTP behavior, which previously prevented spanning tree convergence.
17497 The timing of a reset configured by the "reset at" command now takes into account the offset configured through the “set summertime enable” command.
18021 Corrected an issue with enabling VLAN authenticated, Wake-On-LAN devices.
17949 Corrected a display issue with the “show mac port” command being case sensitive.
17884 The output of the "show port status" command displayed the an MGBIC-08 as 1000-lx. It is now displayed as 1000-lx/lh.
17137 The output of the "show port status" command displayed an MGBIC-LC03 as 1000-sx. It is now displayed as 1000-lx/lhmm.
17875 Addressed a VLAN egress issue where a port’s statically applied egress could be cleared by removal of policy applied egress.
17797 Addressed a display issue with output of “show spantree nonforwardingreason” so it accurately reports the non-forwarding reason.
17717 Corrected an issue where “show config outfile” would display corrupted file names, when TACACS was used to authenticate the command.
17673 Corrected issue with calculating profile use counts. Previous the output of “show policy profile all”, could incorrectly display an applied profile as not as being in use.
17498 Corrected an issue with the processing of large LLDP PDUs that previously resulted in a system reset.

Changes and Enhancements in 6.61.08.0013
17485 Corrected an issue in TACACS+ authentication that could hang SSH and Telnet sessions.
17482 Added SNMP support for ifdescr (1.3.6.1.2.1.2.2.1.2) for SFP ports. Previously Netsight shows installed MGBIC-BX## as not installed.
17479 Resolved an issue with link up/down messages not displaying on the local console.
17478 Corrected an issue with memory utilization associated with saving configuration files. This issue could result in memory exhaustion resulting in a reset.
17286 Corrected an issue with VLAN Authorization (RFC 3580), where RADIUS VLANID tunnel attributes greater than 999 were not accepted.
18129 Corrected an issue with archiving configurations using NetSight Inventory Manager
18198 With the introduction of IPv6 ACLs, Policy and ACLs were prevented from being configured simultaneously. Policy configuration is now prevented only in “ipv6mode”. These features use the same hardware resources and administrators are not guaranteed to reach published resource limits.

Changes and Enhancements in 6.61.07.0010
15668/16748/17266 Addressed an issue with IGMP snooping which resulted in loss of management with error “MRT: assertion (0) failed at line 1893 file ../../../../src/application/ip_mcast/vendor/igmp2/prefix.c error at an aprox rate of 10 entries/s” or “edb_bxs.c(1226) 110 %% Last switch reset caused by prefix.c(1941): Error code 0x00000000, after xx second”.
16602 Addressed a RADIUS authentication issue which could cause a reset with error “edb_bxs.c(1226) 204 %% Last switch reset caused by Fault(0x00000e00) SRR0(0x00e9d490) ESR(0x00000000) MSR(0x00001200) DEAR(0x31303203) IMISS(0x00e9d490)” while processing a RADIUS response packet.
16742 Fixed a semaphore deadlock in POE with the following error “broad_poe.c(5001) 182 % PoE timeout while in reset and recovery mode”.
16864 Resolved an issue associated with SNMP configuration with error at boot up “The following commands in "startup-config.cfg" failed:”.
17017/17027 Resolved a code exception in SNMP task with reset “BOOT[141143864]: edb_bxs.c(1226) 108 %% Last switch reset caused by Fault(0x00001100) SRR0(0x01162ae8) SRR1(0x4000b030) MSR(0x00001030) DMISS(0xc914d6d0) IMISS(0x00000000)”.
17035 Addressed an issue with Service ACLs which could cause the switch to block SNTP packets. This fix will allow users to configure the SNTP service type and define PERMIT/DENY rules for SNTP traffic.
17072 Addressed an issue introduced in firmware 6.61.02 which caused DiffServ to stop functioning.
17124 Addressed an issue whereby setting a lengthy login banner when TACACS+ was enabled caused an exception and reset “Fault(0x00000300) SRR0(0x00e6e83c) SRR1(0x2000b032) MSR(0x00001030) DMISS(0x2000b032) IMISS(0x00000000)”.
17127 Resolved an issue with DiffServ in which configuring DSCP AF41, AF42 or AF43 could cause a reset loop.
17134 Device config no longer displays "passive-interface vlan “for each configured interface when “passive-interface default” command was entered.
17256 Addressed a reset associated with issuing the “clear snmp community” command when the switch security mode was set to c2.
17344 Corrected an issue which could prevent the switch to drop certain malformed packets with an invalid destination MAC address.

Changes and Enhancements in 6.61.07.0010
17362 & 17619 Addressed an issue which prevented DHCP to function properly on trusted ports when DHCP snooping was enabled.
17530 & 17773 Addressed an issue in LLDP with reset and error similar to "Last switch reset caused by Fault(0x00001100) SRR0(0x0126BB0C) SRR1(0x4002B030) DMISS(0x19DFE888) IMISS(0x00000000) DAR(0x00000000) DSISR(0x00000000)".

Changes and Enhancements in 6.61.06.0009
To increase the ability to detect memory corruption, protected code space has been created. Any attempt to overwrite operation code space results in an exception that logs the location of the offending operation and resets the switch.
A hardware based watchdog timer has been enabled to increase error recoverability. If the switch enters a hung state where it no longer services the timer, the watchdog will reset the switch without manual interaction.
4616 With this release we have added support for the Interface Name and System Description optional data tuples to CDP.
9783 Added the "all <port#>" option to the "clear maclock" command to clear static maclock entries on a single or range of ports.
13396 Addressed an issue which could cause the VLAN egress configuration settings to be ignored during port bring-up following a stack reset.
14359 Corrected an issue whereby the “show rmon stats” command output displayed incorrect value for oversized packet counters.
14938 Corrected an issue whereby under certain circumstances the SNTP client could stop processing requests.
15192 Resolved an issue whereby the ifTableLastChange MIB object (1.3.6.1.4.1.9.9.27) returned incorrect data.
15283 Addressed an issue whereby the entPhysicalIsFRU MIB object (1.3.6.1.2.1.47.1.1.1.1.16) returned incorrect data when object class was of type "module".
15428 The SNMPv3 User Credentials are now persistent across stack resets.
15685 Resolved an issue which could cause user configured VLAN egress to be removed from saved config on member units.
15997/17051/17117 Addressed an issue whereby IGMP group membership reports were erroneously flooded across the associated VLAN. This could potentially interrupt multicast traffic such as FOG to some clients.
16330 Resolved a CLI issue which caused mdi and mdix strings to be interchanged in “show port mdix all” and “show config port” output. This resulted in the wrong cable type connection to be displayed.
16354 When authenticating a user on an auth-opt port and using RFC3580 dynamic VLAN assignment, the port may get into a state where users are no longer able to authenticate on the port. This has been resolved.
16376 DHCP discovery packets are now serviced at a higher priority COS queue. Previously DHCP requests were dropped when L2 multicast traffic was switched at high rate to the host.
16411 Corrected the OID value for chHotTemp object (. 1.3.6.1.4.1.52.11004) in the xtraps MIB group. This issue only affected SNMPv2 and v3.
16488 Addressed an issue with configuring Ether type policy rules via Netsight Policy Manager. Out of range values were accepted and the resulting classification rules could not be removed via the CLI.

Changes and Enhancements in 6.61.06.0009
16521 Addressed an issue with Syslog message format by removing extra spaces between timestamp and host's IP address.
16591 Addressed a policy issue whereby deny actions were assigned higher precedence over permit rules. This caused a deny-all policy at the role level to disregard subsequent permit rules and drop all inbound traffic to the port.
16630 Resolved an issue whereby continuous SSH sessions to the switch caused the session to hang. Telnet, console and SNMP management were unaffected.
16639 Addressed an issue which could remove static DHCP binding for a client's MAC address when the client renewed its DHCP lease.
16647 Corrected an issue with IGMP snooping which caused multicast traffic to flood out ports once the IGMP group membership interval time expired.
16750 Resolved an issue with the "set policy rule < profile-index > ipdestsocket "command whereby policy was applied to traffic which did not match the specified destination IP address. This resulted in packet loss due to erroneous traffic classification.
16778 Addressed an issue where user defined passwords with embedded spaces revert to default settings upon reboot. As best practice, password strings containing spaces should be enclosed in quotes.
16997 Addressed an issue which prevented users to define password strings starting with "!".
17009 Addressed an issue associated with the command line parsing buffer which prevented service-ACLs to be displayed in certain show command outputs. This issue was seen when screen length was set to a non-zero value.
17048 Resolved a code exception in SNMP with reset "BOOT[141143864]: edb_bxs.c(1226) 108 %% Last switch reset caused by Fault(0x00001100) SRR0(0x01162ae8) SRR1(0x4000b030) MSR(0x00001030) DMISS(0xc914d6d0) IMISS(0x00000000)".
17083 Addressed an issue whereby logging to the switch via webview could cause a reset with a message similar to "edb_bxs_api.c(786) 202 %% Last switch reset caused by Fault(0x00000300) SRR0(0x01113A40) SRR1(0x0000B030) DMISS(0x13350104) IMISS(0x00000000) DAR(0x00000000) DSISR(0x0A000000)".
17120 Removed informational debug messages similar to "SIM[88867688]: broad_hpc_drv.c(2686) 19017 % bcm_port_update: u=0 p=20 link=1 rv=-15" from the CLI output.
17130 The MGBIC-BX120 SFP transceiver modules are now supported in CLI display output.
17149 If a login banner is configured on the switch and a console cable is attached, no response is sent to the screen when the <enter> key is hit. This has been addressed.

Changes and Enhancements in 6.61.05.0009
17069 Resolved an issue which could prevent PoE delivery to some ports following an upgrade to firmware 6.61.02 or 6.61.03.
17073 The bootrom is now upgraded ONLY on a system reboot following a firmware upgrade. This addressed an issue which could prevent units from booting up after upgrade to firmware 6.61.02 or 6.61.03.

Changes and Enhancements in 6.61.03.0004
16951 Addressed an issue with hybrid policy authentication in which the authenticated user's MAC address was not learned.

Changes and Enhancements in 6.61.03.0004
16958 Addressed an issue with the TCP MIB in which a continuous GetNext on the tcpListenerProcess OID would loop.
16982 Addressed an issue with high CPU utilization when setting an SNTP interface to an interface that is not up.
16993 Addressed a reset condition when large numbers of VLAN egress rules are pushed from policy manager.

Changes and Enhancements in 6.61.02.0007
Added the capability to detect unidirectional stacking communication failures. This mode of failure may have resulted in units being in a permanently detached state. On detection, the failing unit will automatically reset and rejoin the stack.
13946 Addressed an issue which prevented GVRP from automatically propagating VLANs assigned to ports via vlan authentication.
15007 Addressed a loss of link issue with the following error “SIM[83729768]: broad_hpc_drv.c(2689) 80 %% Port ge21: bcm_port_update failed: Operation failed”.
15974 Resolved a buffer allocation issue which could cause the switch to stop generating console and syslog messages.
16041 Addressed an issue associated with transmit queue monitoring whereby an oversubscribed front-panel port could potentially cause spanning tree topology change and reconvergence when flow control was enabled.
16155 Addressed a flow control issue where packet based backpressure limits were reached with packets sent to the host. This could inadvertently activate flow control on an undersubscribed uplink port.
16294 Addressed an issue which prevented forbidden precedence in policy to override 802.1Q VLAN egress on a port when default role and dot1q applied to the same VLAN. Additionally, the precedence order was corrected to “Forbidden”, “Untagged” and “Tagged”.
16486 Addressed a CLI display issue with Transmit Queue Monitoring which could cause oversubscribed ports to appear stalled when flow control was engaged.
16624 Addressed a persistency issue associated with the “set length” command following a switch movemanagement.
16815 Resolved a multiauth issue which prevented a user to authenticate via multiple authentication methods using the same vlan assignment.
16826 Corrected an issue which prevented Service ACLs to work over routed interfaces.
16862 Addressed a stack management issue which could prevent newly added switches with a "code version mismatch" from rebooting with the "reset <Unit ID>" command.

Changes and Enhancements in 6.42.11.0006
14077 & 16236 Addressed an issue which resulted in high CPU utilization when the switch received Kiss-o’-death packets from an SNTP server.
16067 Addressed an issue whereby the following CLI messages were scrolled continuously on the console “SIM[149535472]: timer.c(995) 1001 %% XX_Call() failure in _checkTimers for queue 0 thread 0xfc8ad00. A timer has fired but the message queue that holds the event has filled”.
16135 Addressed a buffer management issue which limited the number of LLDP-MED endpoint connections to the switch. Previously only 6 connections were allowed.
16156 & 16760 Addressed an issue where a stack could fail to reform after powering down the master unit.

Changes and Enhancements in 6.42.11.0006
16157 Addressed an issue which caused LAG ports to enter Ingress Back Pressure (IBP). This issue could cause LACP and STP BPDU control packets to be dropped when oversubscribing a LAG with Flow Control (FC) disabled.
16291 Corrected an issue with the LLDP service routine which prevented LLDP-MED endpoints to register with the switch after a warm boot. This issue was not seen when the switch was cold started.
16447 Addressed an issue where the user defined MDI/MDIX port setting was reversed after moving the management unit.

Changes and Enhancements in 6.42.10.0016
Added the capability to detect unidirectional stacking communication failures. This mode of failure may have resulted in units being in a permanently detached state. On detection, the failing unit will automatically reset and rejoin the stack.
14038 An informational level Syslog message is now generated when the manager unit is removed from the stack. Previously “unit leave” messages were sent for member units only. Note that a unit leave message will not be generated on move management or stack renumbering commands.
15593 Addressed an issue associated with LLDP and LLDP-MED which resulted in a reset with an exception message in the lldpXMedRemCapCurrentGet task.
15599 Addressed an issue where an extra line was inserted in the CLI output display. This was seen when screen length was set to non-default and ENTER was pressed to advance the output one line at a time.
15874 The “clear dhcp conflict logging” CLI command now disables DHCP conflict logging.
15876 Addressed an issue where login authentication failed to switch from SSH to local when the RADIUS server was unreachable.
15893 Resolved an issue whereby the member of a single-port LAG was not properly added to the egress list of the LAG’s VLAN if the port was down while the LAG was being configured.
15916 Resolved an issue whereby RMON failed to capture packets when capture type in the channel entry was set to “failed”.
15933 Corrected an issue in CDP which could result in an error “NIM[164832176]: nim_intf_map_api.c(420) 1083 % internal interface number 21021 out of range" when the "show neighbors" command was executed.
15983 Addressed an issue with unlocking MAC addresses in a MAC locked port after a link down. This issue prevented locking the first MAC arriving on a port after a link up when the first arrival value was set to 1.
16027 Addressed an issue with diffserv policy using the VLAN class match which resulted in the following error message, “UPN[113003432]: broad_policy.c(1367) 168 % Error creating port policy 17 for intf 134217728, code Operation failed & Could not attach the Policy.”
16039 Addressed an issue whereby sFlow datagrams were transmitted with invalid packet type when selectable management was configured.
16077 Addressed a system hang and reset which was accompanied by messages similar to “broad_hpc_drv.c(2689) 30 %% _soc_xgs3_mem_dma: L2_ENTRY.ipipe0 failed(NAK), unit 1” and “hwutils.c(4178) 39 %% MPC85xx DMA/PCI register dump“.
16089 Addressed an issue whereby client RADIUS requests were sent to all configured RADIUS servers even when the primary server was reachable.
16107 Addressed an issue where DAI was silently dropping ARP packets which exceeded 64 bytes in size. This resulted in loss of contact with some devices such as Cisco Analog Telephone Adaptor (ATA) products when DAI was enabled.
16156 Addressed an issue where stack members could potentially leave the stack when the management unit was powered off.

Changes and Enhancements in 6.42.09.0005
6672 The “clear spantree adminpathcost” CLI command now works when using wildcards for the port-string option field.
13573 Corrected a memory access issue associated with SSH which could potentially result in a device reset. This issue was previously seen when using SFTP to transfer files to an OpenSSH 3.8p1 server.
14359 Corrected an issue whereby the “show rmon stats” command output displayed incorrect value for oversized packet counters.
14494 Corrected an issue associated with RSTP which prevented the alternate port from failing over to the root bridge when the root port failed.
14796 Addressed an issue where setting the CLI screen length to a non-zero value could cause the “clear snmp” command to not appear in the “show config” output.
14910 Addressed an issue where the “set port advertise” command was removed from the config following an upgrade to firmware 6.42.
14989 Addressed a CLI issue which could potentially cause a reset when the output of the “show config” command exceeded 9K lines.
15052 Resolved an issue whereby the “show lldp port remote-info” command would not display the correct POE Power source of remote devices.
15054 Resolved an issue whereby the switch would flood unicast DHCP release packets across the VLAN when the path to the network DHCP server was known.
15177 Corrected an issue where uploading a file to a Secure Copy (SCP) server could potentially cause a CLI session lockup and reset with the following errors “0x8798140 (TransferTask): task 0x8798140 has had a failure and has been stopped” and “0x8798140 (TransferTask): fatal kernel task-level exception!”.
15189 With this release UDP ports 7700 and 7800 are no longer used during the TFTP image download operation.
15224 Resolved a display issue associated with the “show neighbors” command where the device ID in the Cisco DP neighbor discovery field was truncated.
15246 Addressed an issue with the “set snmp group” command where group names delimited by spaces were not saved in the config correctly.
15297 Addressed an issue associated with the switch port state machine which could potentially cause device ports to lockup.
15308 Resolved an issue which could prevent Spanning Tree from failing over to the alternate port after multiple failovers when automatic edge port detection was disabled on edge ports.
15315 Resolved a problem where the “show vlan portinfo vlan” command displayed port information for all configured VLANs not just the one specified in the command.
15400 Addressed a persistency issue associated with the “set radius server” command when the specified server secret password started with the exclamation mark (!).
15550 Addressed an issue where the etsysMACLocking traps were generated with incorrect MIB object name causing them to appear as Enterprise Specific traps.
15584 Resolved an issue where the etsysResourceProcessName (1.3.6.1.4.1.5624.1.2.49.1.2.1.1.2) MIB in etsysResourceUtilizationMIB module returned an incorrect process name.
15596 Addressed an issue where the Multiauth numusers value was set to default if the policy maptable response type was changed; consequently all instances of “set multiauth port numusers” command were removed from the config.
15841 Addressed an issue where the user defined MDI/MDIX mode was reversed when issuing the "Set port mdix" command.
15848 Corrected an issue whereby users could potentially fail to send a DHCP request after being assigned a new profile. This issue was caused by a small delay in moving users to the new authenticated VLAN.

Changes and Enhancements in 6.42.09.0005
15859 Corrected an issue with the premature closure of the RADIUS UDP socket. This issue could have prevented user authentication when the server response was routed through the unit and was not received from the RADIUS server within 1 second.
15888 Addressed an issue with the move management switch functionality which could cause loss of access to the new management unit following an administrative move.

Changes and Enhancements in 6.42.08.0007
14716/15019/15350/15357 Addressed a DHCP snooping issue whereby DHCP packets forwarded over LAG ports to the CPU were sent back to the source causing a loop and high CPU utilization.
15523 Resolved an issue with high CPU load caused by excessive interrupts generated when an unpowered RPS was attached to the device.
15711 Resolved an issue whereby connecting a Redundant Power Supply (RPS) to an operational switch could cause loss of PoE power delivery to attached devices.

Changes and Enhancements in 6.42.07.0010
15348 Addressed a user connectivity issue where a user could internally be learned on a Spanning Tree discarding port, if an IGMP message sourced by the user is seen on that port.
15395 Addressed stacking stability issues associated with changing POE detection mode. In stacks with high POE port counts, setting the inline detection mode to ieee, could cause long delays in stack formation at boot time. Changing the detection mode (auto or ieee) at run time could also result in units leaving the stack for periods of time. The stacking instability was accompanied by large numbers of ATP timeout warning messages on the console (example “ATP: TX timeout, seq 55327. cli 778. to 3 tx cnt 6.")
15452 Corrected an issue which could potentially prevent MAC address notification traps from being generated and cause a CLI lockup.

Changes and Enhancements in 6.42.06.0008
13100 Resolved an issue whereby executing the “show config outfile" command followed by “show support” could cause a device reset.
14582 Corrected a formatting issue associated with the "show dhcpsnooping port" command output display.
14639 The "movemanagement" command is now supported over SSH sessions.
14733 When upgrading from firmware 1.02.05 to higher revisions, the port inlinepower admin state will now persist when preceded by the "set port linepower admin off" command in the config file.
14776 Corrected an issue whereby read-write and read-only SSH users were unable to log back onto the switch once locked out.
14817 Resolved an issue whereby SNMPv3 inform requests were not sent when the device was in router mode.
14903 Corrected an issue whereby the egress ports on GVRP-generated VLANs were removed after LACP was disabled on the associated LAG port.
14954 & 15182 Addressed an issue which could affect re-learning the ARP table on a switched interface after issuing the “clear arp-cache” command.
14996 Resolved a CLI buffering issue which resulted in the following error message “Max number of lines in the scroll buffer reached. Output will be truncated.” This was seen when using a non-default CLI screen length in a stacked environment.

Changes and Enhancements in 6.42.06.0008
15013 Addressed a potential TCP vulnerability identified in US-CERT VU#723308.
15060 Cisco discovery protocol announcements now contain the IP address of the routed interface on which the PDUs are sent.
15084 With this release the output of “show txqmonitor” and “show txqmonitor flowcontrol” commands are now gathered in the “show support” CLI command.
15085 Corrected a stack management issue which could result in loss of config on a newly-designated manager following a move management or leave operation.
15086 Resolved an issue with potential loss of management following a switch movemanagement when accessing the switch across a LAG port.
15114 Resolved an issue in the CPLD status handler task which could result in high CPU utilization when an RPS was detected.
15203 Resolved an issue whereby the Spanning Tree instance assigned to a VLAN by MSTP would not persist across stack resets with COS enabled. This could cause loss of network connectivity.
15251 Issuing the “config configure” command will attempt to disable all device ports prior to executing the configuration file. In certain cases some ports could remain up, resulting in a network loop and loss of management to the switch. This has been resolved.

Changes and Enhancements in 6.42.05.0001
15171 Corrected an issue with the premature closure of the RADIUS UDP socket. This issue could have prevented user authentication in cases where a response was not received from the RADIUS server within 1 second.

Changes and Enhancements in 6.42.03.0004
13278 Resolved an SSH issue which prevented users from logging onto the switch using the Ponderosa SSH Client application.
13979 Resolved a Multiauth issue whereby the switch continued to send MAC authentication requests after the supplicant successfully authenticated via 802.1X, which could potentially cause a reset.
14224 Authenticated users that remained quiet for periods of time after authenticating failed to reauthenticate once the session timed out. This has been corrected.
14447 Monitoring SSH sessions to the switch via the Xymon Monitor (aka hobbitmon) bbtest-net program will no longer cause the sessions to hang.
14567 The “show vlan portinfo” command output now displays the correct egress list. This was only a display issue on dynamic VLANs.
14599 Users are now able to enforce policy to members of a stack via NetSight Policy Manager.
14739 The LLDP auto-negotiation TLV definition now advertises correct port capability.
14740 Resolved a problem whereby accessing the system via SSH failed with the following message “Connection refused”. This issue was only seen when device config was loaded via TFTP or NetSight Inventory Manager.
14757 sFlow Receivers are no longer persistent and will not be displayed in the running-config. Receivers can be viewed using the “show sflow receivers” command. This will prevent receiver timers from making configurations appear to change in Inventory Manager.
14921 Routed interfaces will not be enabled without egress. Policy applied egress was previously not considered in the calculation.
14926 Corrected an issue with 802.1x where a client table entry was lost with each authentication. This would eventually result in clients being unable to authenticate.

Changes and Enhancements in 6.42.02.0006
14485 Resolved an issue with loop protect whereby breaking links on a LAG could potentially stop traffic across its member ports shortly after connection was re-established.
14846 The host protect feature now properly rate limits the traffic.
14882 Upgrading from firmware 1.02 to 6.42.01 without an interim upgrade to 6.03.08 caused PoE power-delivery failures. Upgrading from firmware 1.02 to 6.42.02 does not require any interim upgrade.
14895 Corrected a reset condition when the “set system hostprotect enable” command was applied via NetSight onto a system with host protect disabled.
14900 Corrected a potential reset condition with a message similar to “edb_bxs_api.c(779) 22 %% Last switch reset caused by nim_events.c(213): Error code 0x0000badd, after 328456 second”.

Changes and Enhancements in 6.42.01.0046
When upgrading PoE switches from firmware 01.02 to 6.42.01, you must first upgrade to firmware 6.03.08 then to 6.42.01.
12796 Resolved an issue whereby some MGBIC-LC03 LX SFP modules would display as type SX in the "show port status" command output.
12989 Resolved an issue whereby the SNTP client running in broadcast mode could potentially fail if the server was unavailable at the time client went operational.
13113 When restoring a saved configuration file, Spanning Tree settings are now loaded in correct order.
13153 Corrected an issue where loss of management could ensue when a Telnet session with an active TFTP transfer is terminated.
13367 Resolved an issue whereby login authentication via TACACS+ failed to switch over according to authentication precedence rules when the TACACS+ server was unavailable.
13392 Resolved an issue whereby static ARP entries were displayed in the configuration file after being administratively removed.
13674 Resolved an issue with IGMP snooping filters whereby the device could drop some SMB packets in transit, causing the file transfer to fail.
13792 Corrected an issue which resulted in the daylight savings times function to fail when the dates to start and stop DST spanned over a year.
13844 Resolved an issue whereby the switch could potentially respond with NAS-Port-Type RADIUS attribute of Virtual instead of Async when users attempted to login to console.
13851 The “set length” command is now persistent after a reset.
13941 The daylight savings time function (Summer Time) now works properly when SNTP is enabled.
13980 The value of port utilization percentage is now calculated and displayed correctly in the “show rmon history” command output.
14003 Resolved an issue whereby Syslog messages were not generated for SSH login events.
14022 Corrected an issue whereby processing CDP packets which contained malformed type-length-value (TLV) tuples could potentially cause a device reset.
14034 Resolved an issue whereby configuring an IP helper address on the 24th router interface failed with the following message, “Error: VlanId is not matching with any of router interface”.
14035 & 14774 802.1x supplicants now properly failover to specified backup RADIUS servers when the primary server is unavailable.
14109 Corrected an issue whereby changing the authentication precedence to an erroneous value via SNMP could disable 802.1X authentication.

Changes and Enhancements in 6.42.01.0046
14121 Resolved an issue whereby 802.1x client authentication packets were flooded out ports blocked by Spanning Tree. This resulted in supplicant authentication failures and high CPU utilization.
14136 Resolved a CLI display issue whereby the “show lldp port remote-info" and "show lldp port local-info" commands displayed incorrect device type for 1000BaseT ports.
14137 The snmpEngineTime (1.3.6.1.6.3.10.2.1.3) MIB value rolled over after 497 days of system uptime instead of the maximum allowed 24855 days. This has been fixed.
14170 Resolved an issue where the RADIUS Medium-Type Attribute failed to validate. This could potentially result in “maca_radius.c(378) 104065 %% macaRadiusAcceptProcess: invalid mediumType length 10” messages and a reset.
14258 The “clear snmp group “command is now persistent across reboots.
14260 Using the VLAN Elements Editor from the NetSight Policy Manager application to configure an access or trunk port caused the uplink to be removed from the egress list, this has been resolved. Previously this issue was reported on firmware 6.41.03.0018 and above.
14289 With this release the SNMP IF-MIB.ifHCInOctets (1.3.6.1.2.1.31.1.1.1.6) counters for LAGs have been changed from 32-bits to 64-bits.
14295 Resolved an issue which prevented accessing the device via SNMP when the management IP address was in the 172.16.0.0/16 network address range.
14342 Resolved an issue whereby 802.1x authenticated users could no longer authenticate after the port mode was changed from auto to forced authorized and back.
14408 Support for the 5M stacking cables has been added in this release.
14469 Resolved an issue whereby DHCP relay agent stopped forwarding client’s requests to the DHCP server.
14637 The SNMP group CLI commands now persist across device resets.
14649 The output of CLI command "show diffserv info" now displays the correct Maximum value of 120 for the Service Table Size.
14665 Resolved an issue whereby disabling MAC locking globally or on any port, would terminate all authenticated sessions (MAC authentication, 802.1X, PWA) on the MAC locked port.

Changes and Enhancements in 6.03.08.0012
14629 & 14690 Resolved as issue whereby applying policy to a port with existing policy would block traffic from egressing the port.

Changes and Enhancements in 6.03.06.0008
12697 The router interface state is only affected by the EAPOL status when in strict 802.1X mode. All other times it will be based only on the VLAN egress list.
12796 Resolved an issue whereby some MGBIC-LC03 LX SFP modules would display as type SX in the "show port status" command output.
13113 When restoring a saved configuration file, Spanning Tree settings are now loaded in correct order.
13153 Corrected an issue where loss of management could ensue when a Telnet session with an active TFTP transfer is terminated.
13392 Resolved an issue whereby static ARP entries were displayed in the configuration file after being administratively removed.
13422 The value of the MIB object snmpEnableAuthenTraps (1.3.6.1.2.1.11.30) is now persistent across device resets.

Changes and Enhancements in 6.03.06.0008
13674 Resolved an issue with IGMP snooping filters whereby the device could drop some SMB packets in transit, causing the file transfer to fail.
13867 Resolved an issue whereby applying a new policy role to a port caused the port's egress status to change from untagged to tagged.
13943 & 14096 Resolved a potential memory leak associated with IP multicast which could cause a reset with a message similar to "osapi.c(1381) and broad_cpu_intf.(3086)" or "CRASH - broad_cpu_intf and hapiBroadPruneTxPorts".
13980 The value of port utilization percentage is now calculated and displayed correctly in the "show rmon history" command output.
14003 Resolved an issue whereby Syslog messages were not generated for SSH login events.
14022 Corrected an issue whereby processing CDP packets which contained malformed type-length-value (TLV) tuples could potentially cause a device reset.
14034 Resolved an issue whereby configuring an IP helper address on the 24th router interface failed with the following message, "Error: VlanId is not matching with any of router interface".
14121 Resolved an issue whereby 802.1x client authentication packets were flooded out ports blocked by Spanning Tree. This resulted in supplicant authentication failures and high CPU utilization.
14295 Resolved an issue which prevented accessing the device via SNMP when the management IP address was in the 172.16.0.0/16 network address range.

Changes and Enhancements in 6.03.05.0004
12472 Resolved an issue where the switch could send duplicate ICMP response packets when the source/destination IP addresses of the ICMP request were on the same routing interface and ICMP redirect was enabled.
12606 The 'show multiauth session' command now properly displays the session timeout value. Previously the CLI returned a zero for this field when the Termination-Action RADIUS attribute was set to RADIUS-Request.
12767 The Spanning Tree path cost value for LAG ports is now properly calculated.
12870 The ICMP unreachable packets generated by the switch will now be transmitted in the order in which received.
13059 Resolved an issue which could cause loss of telnet and SSH management while the console continuously displayed 'ewsStringCopyIn: no net buffers available'. Traffic forwarding and SNMP management were unaffected.
13157 The 'clear port advertise' command now returns port settings to default values.
13180 MGBIC-LC01 SFPs are now detected in non PoE C3 and B3 switches. Previously the interface type of LC01 SFPs would not show in the 'show port status' command output.
13224 Resolved an SNMPv3 issue which under rare conditions could cause the CLI to overwrite the 'set snmp group' settings.
13238 Corrected an issue where the switch would not forward the IP helper client packets when only one DHCP relay agent was configured on the interface.
13261 Resolved an issue with the 'show port egress' command where the egress information for some ports were not displayed.
13340 The SNMP Target IP address mask is now properly displayed in the 'show config snmp' or 'show snmp targetaddr' command outputs.
13376 All super user accounts will now be re-enabled after the system lockout timer expires. Previously only the default admin super user account was re-enabled and all other super users would remain locked out after the maximum login attempts was reached.

Changes and Enhancements in 6.03.05.0004
13470 Corrected an issue where the NAS-Port-Type RADIUS attribute for an authorized console session would change from Async to Virtual after a Telnet user successfully logged in to the device.
13474 Corrected a potential reset which caused the following error message '../../../../andl/hapi/broadcom/esw/routing/broad_l3.c:4758 Invalid intfId for host: x.x.x.x, usp = 0.2.5'. Previously the reset could occur after a stack member was removed followed by a router interface state change on the manager.
13485 Resolved an issue where, in some rare cases, SSH users attempting to login to the switch could cause a reset if the RADIUS server returned incorrect attributes.
13540 Resolved an issue where using SCP to transfer files from a Telnet session could cause both the local console and telnet to hang. There was no issue transferring files with SCP from the console.
13620 The TACACS+ client session authorization settings will now be persistent across reboots.
13662 Resolved an issue with the TACACS+ session authorization where using non-default attributes for service level exec would not grant admin privileges to the user.
13860 Resolved an issue where the switch would not respond to SNMP management requests when the least significant digit of the NetSight server IP address was set to zero. Previously using the NetSight server address of x.x.x.0/255.255.252.0 would not work.
13892 Resolved an issue where enabling DHCP snooping on the switch could cause DHCP offer packets to be transmitted out the LAG member interfaces. This caused a packet loop leading to high CPU utilization.
14162 The WebView management application copyright date has been updated to 2010.

Changes and Enhancements in 6.03.04.0004
10874 Corrected an issue when under certain circumstances the SNTP client stopped processing requests.
11306 Resolved a CLI issue associated with save and restore of a config file which contained the "set DHCP exclude" command.
12357 Resolved an issue whereby multi-user-authentication failed when only one user was allowed to authenticate on a port. Previously policy was applied when the "set multiauth port numusers 2" command was issued.
12549 Corrected an issue whereby the "ip igmp enable" command was not included in the configuration without an active routing license key.
12702 Resolved an issue with the "set system login" command where the CLI accepted a password preceded with an "!" but errored out when restoring it from a saved config. Previously restoring the password caused the following message, "Error: Missing value for "password" and the user was unable to login.
12813 The switch now sends a small TFTP acknowledge packet at the completion of a successful download. Previously a 512 Byte ACK was transmitted which could potentially slow down the file transfer.
12848 Resolved an issue whereby link aggregation could potentially fail sometime after a LAG was formed. Previously the failure occurred when a network loop caused a participant switch to receive its own LACP PDUs.
12869 Resolved an issue whereby the switch could take up to 5 seconds to generate an ICMP host unreachable message when the remote host failed to reply.
12871 DHCP snooping now works on LAGs and their underlying physical ports when configured as trusted ports.
12893 Resolved an issue with sFlow whereby the actual packet sampling rate did not match the user configured value.
12899 Corrected an issue whereby LAGs failed to come up after upgrading from release 1.01 to 1.02.
12909 Corrected an issue with the "set length" command that could prevent the display of default routes in running config. Default routes could be displayed via the "show ip route" command.

Changes and Enhancements in 6.03.04.0004
12910 Corrected an issue whereby multiauth users which had successfully authenticated via dot1x and macauth lost network connectivity after their static egress was administratively removed.
12951 Resolved an LACP buffering issue which could prevent traffic flow across LAGs after some time.
12960 Resolved an issue with the “show vlan portinfo” command whereby the VLAN egress for dot1x clients would not appear in the output.
13111 Spanning Tree settings are now restored in proper order when loaded from a saved configuration file.
13150 Static ARP entries are now preserved across device resets or when interfaces change state.
13151 Resolved a display issue with the "show lldp port remote-info" command whereby the ”Operational Speed/Duplex/Type” field reported an incorrect value.
13176 The ifMIB module now supports the ifName object (1.3.6.1.2.1.31.1.1.1.1). Previously port link up/down traps did not include the interface name.

Changes and Enhancements in 6.03.03.0008
12635 Users can now change the TACACS+ session authorization attribute name by issuing the “set session authorization” command. Previously the default name “priv-lvl” could not be changed.
12884 Resolved a loss of management issue when using Cisco ACS version 3.3 to secure access switches using TACACS+. Previously CLI or console sessions could lock up once user name and password credentials were provided.
12897 Static route entries are now displayed in the “show running-config” command output.
12905 Resolved a RADIUS buffering issue whereby the switch stopped sending RADIUS request packets and reported the following error message “RADIUS: Msg Queue is full! Event: 19".
13062 Added support for the TAG field of the VLAN ID string in the “Tunnel-Private-Group-ID” RADIUS tunnel authentication attribute. Previously using the TAG field caused dot1x, MAC and PWA authentication to fail with the following error message: “maca_radius.c(365) 62 %% macaRadiusAcceptProcess: TunnelPrivateGroupId0 length is greater than 4!”.
13170 SSH client sessions are now consistently terminated after 3 failed attempts. Previously in some 6.03 releases when a user reached max login retries, all subsequent invalid logins were disconnected after first try.
13264 Corrected an issue which resulted in momentary loss of data shortly after users MAC authenticated. This issue did not affect dot1x clients and only occurred when a user’s MAC address appeared in multiple FID entries.

Changes and Enhancements in 6.03.02.0006
12437 Corrected an array indexing issue which could potentially cause memory corruption and a reset.
12793 Corrected an issue with the "show vlan static" command whereby the output would not display untagged egress ports.
12812 & 12941 Resolved an SSH issue where the client sent multiple access requests to the RADIUS server after the first request was already granted.
12823 Resolved a buffering issue which could cause loss of telnet and SSH management while the console continuously displayed “ewsStringCopyIn: no net buffers available”. Traffic forwarding and SNMP management were unaffected.
12833 Resolved an issue whereby occasionally members of the stack would report stacking port errors. These messages did not appear to adversely affect the network. IMPORTANT: This solution is not compatible with 5M cables; therefore, do not install this maintenance release if you have 5M cable installations.

Changes and Enhancements in 6.03.02.0006
12896 Corrected an issue where the host may stop responding to ARP requests causing loss of management (SNMP, telnet and SSH).

Changes and Enhancements in 6.03.01.0008
Added support for the following OIDs to the CTRON-CHASSIS-MIB ctChas object: • **ctChasFNB.0** denotes the presence or absence of the FNB. • **ctChasAlarmEna.0** allows an audible alarm to be either enabled or disabled. Setting this object to disable(1) will prevent an audible alarm from being heard and will also stop the sound from a current audible alarm. Setting this object to enable(2) will allow an audible alarm to be heard and will also enable the sound from a current audible alarm, if it has previously been disabled. • **chassisAlarmState.0** denotes the current condition of the power supply fault detection circuit. The object value will read chassisNoFaultCondition(1) when the chassis is operating with no power faults detected and will read chassisFaultCondition(2) when the chassis is in a power fault condition.
12665 Resolved an issue with the "show system" command where the thermal threshold percentage value would show NA (not available) on stack member switches that supported this functionality.
12661 Corrected an issue with the MAU-MIB etsysMultiAuthStationClearUsers object (1.3.6.1.4.1.5624.1.2.46.1.3.1.1.3) which could prevent users from reauthenticating after they were unauthenticated.
12646 Corrected an issue whereby executing the "clear snmp view all 1" command followed by a "show config" could result in a reset.
12640 Corrected a dot1x issue whereby policy was not applied on ports where authentication was not configured.
12574 Resolved an issue where all stack member switches were assigned identical self MAC addresses.
11683 &12561 The "show vlan" and "show port egress" command outputs now show the VLAN egress information assigned via dynamic policy.
12560 Resolved an issue with the NMS Inventory Manager Timed Reset function which could cause devices to reset some time after the scheduled reset time.
12517 Resolved an issue whereby the switch failed to forward DHCP client messages when DHCP snooping was disabled on the associated VLAN.
12513 The SNMP agent now uses the source IP address of the selected management interface (if specified) when generating traps.
12506 Corrected an issue with the “show support” command output when the screen length was set to greater than zero.
12499 Resolved a CLI issue associated with “show port egress" whereby the mirror source port failed to show in the command output.
12449 Resolved a potential memory leak associated with the “show config" CLI command.
12444 Corrected an issue whereby the sFlow SysUptime field of the sFlow packet was not properly initialized on bootup.
12445 Resolved and issue whereby the “set sflow interface” command would go into effect even if the specified interface was down.
12439 The switch now includes the NAS-identifier value in the RADIUS access-accept packet sent to the RADIUS server.
12438 Corrected an issue where the port inlinepower admin state was not persistent when it was preceded by a "set port inlinepower admin off” in the config file.
12430 Corrected a CLI issue where the “show config all” command could result in loss of management or high CPU utilization when screen length was greater than zero.

Changes and Enhancements in 6.03.01.0008
12427 Users are now able to access the web when PWA guest networking is enabled with no authentication method.
12302 PoE switches now support up to 375W of PoE power. This allows the switch to supply 15.4 watts of power for up to 24 ports simultaneously.
12289 Wake-on-LAN UDP packets destined to ports 0, 7 and 9 are now forwarded when configured via the "ip forwarding-protocol udp" command.
12241 Resolved an issue whereby the MAC addresses for the first two units of a stack were identical when management functionality was moved from switch 1 to switch 2.
12223 Corrected an issue where the MAC addresses of devices connected to the switch front panel failed to appear in the port MAC address table.
11784 Resolved an issue whereby moving a port to the VLAN specified by policy was delayed when DHCP snooping was enabled.
11613 SNTP packets are now forwarded across the switch using the IP address of the selectable management port (if configured).

Changes and Enhancements in 6.03.00.0022
All new features added in this release are documented under the What's New in 6.03 section above.
12345 Corrected an issue with the LLDP application that prevented the switch from correctly displaying LLDP neighbor information advertised by a Siemens OpenStage 40 SIP phone.
9714 Corrected an issue that prevented the "clear nodealias config <port>" from clearing non-default maxentries values.
9427 An RMON alarm now triggers correctly for a rising threshold when the startup parameter is configured for "either".
9637 An RMON alarm configured for both a rising threshold and falling threshold will not continuously be triggered for the falling threshold if the traffic rates do not exceed the falling threshold.
10411 Corrected an issue that prevented the configuration and enforcement of the system lockout feature after X number of SSH attempts failed.
9941 Corrected an issue causing an ACL to be applied to every virtual interface on a port if it was applied to a single VLAN. The issue is resolved via new support for VLAN-based ACLs.
12293 Resolved an issue where idle management sessions failed to disconnect after the maximum idle time was reached.
12254 Resolved an issue where expired SSH sessions failed to disconnect after 60 seconds.

KNOWN RESTRICTIONS AND LIMITATIONS:

Known Issues in 6.61.16.0002
There are no new known restrictions or limitations associated with this release.

Known Issues from Previous Releases
Extreme Summit and BlackDiamond platforms may use a single source MAC address for protocol and host generated packets. If redundant connections are made to these devices without the use of a link aggregation, the MAC address might be learned on a port in a blocking state. This may result in loss of connectivity to their host IP address.

Known Issues from Previous Releases
Direct firmware upgrades to 6.61 from 6.03 (and previous) images may result in the loss of some configuration. (notably SNTP) One workaround is to upgrade to 6.42 prior to loading 6.61. Alternatively the configuration may be saved to a file and reloaded after upgrade.
COS / TOS
2731 If the CoS state is disabled, but a CoS priority has been configured, the switch will continue to forward packets with the CoS priority. However, the ToS field will not be modified.
6660 Configuring the last two bits of the ToS field is not supported. For example, when a CoS Index is configured to set a ToS value of 255, it will result in only the value 0xFC being set in the matching packets.
Dynamic Egress
Egress assignments made to ports by using Dynamic Egress are only supported on VLANs which have been statically created.
GVRP
3532 GVRP frames are not forwarded when GVRP is disabled.
2031 The SecureStack will propagate GVRP packets containing any known VLANs. All VLANs learned via GVRP will appear in the GVRP MIBs, regardless of whether or not there are local users attached to those VLANs.
VLAN Tagging
3410 The “set port vlan” command requires that the VLAN(s) specified when executing the command must already be preconfigured statically on the device.
A VLAN cannot be disabled via CLI and/or WebView. SNMP must be used.
16569 If VLAN 4094 is provisioned in firmware 6.61, it must be removed prior to backreving to firmware 6.42 as VLAN 4094 is not supported in release 6.42. Failure to remove VLAN 4094 could potentially cause issues loading certain Layer 3 parameters.
Policy / Authentication
TACACS+ using single connect is configurable through the CLI but it is not supported in this release.
The B3 supports CoS-based Inbound Rate Limits for Policy Roles (profiles). Rule-based Inbound Rate Limits (IRLs) are not supported and will be ignored if configured.
Setting an extensive number of policy rules via the CLI can cause momentary loss of CLI and SNMP management.
Policies can only be assigned to ports on VLANs which have been statically created.
A role with CoS and/or PVID configured counts as an L2 rule and a mask. Multiple Roles with CoS and PVID configured counts only as one rule and one mask globally.
For policy roles that are set to “Deny Traffic” (e.g., Quarantine Role), ARP frames are dropped unless a policy rule explicitly permits forwarding of ARP frames.
Policy roles and rules cannot be applied to ports that are members of a link aggregation group (LAG).
3904 If a policy profile has cos-status enabled, only 99 rules can be supported per policy profile.
2175 ARP packets are not classified based on policy IP source/destination rules.
13421 Upgrading from firmware 6.03.02 to 6.03.03 from a TACACS+ account causes a console lockup. Workaround: Upgrade from a non TACACS+ user account.
VLAN Authorization
When a VLAN tunnel is applied, traffic is egressed untagged as expected. “Show vlanauthorization” will display the correct VLAN and MAC address; however “show vlan” and “show port egress” will not display tunnel ports.
MAC Locking
Static MAC locking a user on multiple ports is not supported.

Known Issues from Previous Releases
It is possible under extenuating circumstances that a violating MACLock user can dot1x authenticate on the port but all other traffic from that user will be dropped.
Statically MACLocked addresses in the Filtering Database show as “other” in the “show mac” response.
The MACLock table may show multiple entries for the same user depending upon the VLAN assignment.
RADIUS
By design, the switch does not allow the Primary and Secondary RADIUS servers to be using the same IP address.
MAC Authentication
10893 On rare occasions with authentication, there is a potential for the MAC address of a user who fails to authenticate to remain unlearned for a period of time.
In some rare cases, the command “set macauthentication portinitialize <port-string>” does not terminate mac-authenticated user sessions.
PWA
On switches that support multiauth, only one PWA authenticated user is supported per port
Spanning Tree
The “show spantree stats active” command may erroneously display some ports as active. If a port was once active and later goes down, the system will still show the port on the “active” list.
VLAN marking of mirrored traffic – Edge only
MAC addresses will be learned for packets tagged with the mirror VLAN ID. This will prevent the ability to snoop traffic across multiple hops.
Warning: Traffic mirrored to a VLAN may contain control traffic. This may be interpreted by the downstream neighbor as legal control frames. Users should disable any protocols on inter-switch connections that might be affected (i.e., Spanning Tree).
Routing
A user cannot overwrite the IP address of a configured interface if the new IP address is in the same subnet as the original. They must first delete the existing interface IP address and then add the new IP address.
The B3 will not add a host route to its routing table for a subnet it already knows about.
The B3 does not support the ability for a user to configure the host’s gateway to be a local routed interface IP. The host’s gateway must exist on a different device in the network, if one is configured.
The B3 only supports one default route. If a default route is configured on the router, it will take precedence over the default route configured for the host IP.
ACLs
Access Control Lists (ACLs) use the same hardware resources as Policy rules and should not be used simultaneously with Policy.
RIP
RIP stops calculating cost properly if cost ever equaled 16. If route cost is reduced below 16, the cost will not be propagated downstream properly.
Management
The switch can support up to two concurrent SSH client sessions.
An SNMPv3 configuration file created in an X.2 release will fail when loading into a switch running 6.03 and above. Workaround: After a switch has been upgraded, a previously created SNMPv3 configuration file MUST be re-generated (saved) using the new code in order for SNMPv3 to function correctly.

Known Issues from Previous Releases
9328 If the host IP address or the router IP interface used for management is in a zero subnet (i.e., 10.0.x.x/16), ARPs will resolve, and the host will be unable to ping devices within the subnet.
9367 ICMP packets containing the record route or timestamp options will not be forwarded by the device.
11539 It is highly recommended that DAI (dynamic ARP inspection) be configured on edge ports only, due to the potential for the DHCP snooping database to become out of sync during a system reset.
11567 When upgrading from 1.02.02 firmware or earlier to 6.03 firmware, the CPU LED blinks red on all units within the stack as the PoE driver is being updated. This only happens during the initial upgrade and will not appear in subsequent reboots.
11593 Setting the SNMP community context to default via the "set snmp community xxx context default" command could cause loss of SNMP management contact. In order to set a configured context back to the default (NULL) context, enter a hyphen as the value of the context parameter. For example, use the following command: "set snmp community abcde context –".
12329 User is unable to set port advertise speeds 10t, 10tfd, 100tx, and 100txfd on combo ports.
12737 When initiating a telnet session from the console of the device to another device, the telnet session will occasionally fail with the following error message: "telnet: Unable to connect to remote host: Connection timed out". Executing the command a second time will succeed.
SWITCH
Firmware 1.02.03 and above includes a new PoE driver which will require additional bootup time as the driver is being updated on PoE units within the stack. Once the initial boot of the code has completed and the PoE driver is updated, the delay should not be seen again.
WebView – Web-based Management
Configuration information for LAGs configured via WebView will not be reflected correctly when viewed via the CLI.
RMON
When packets are transmitted outbound they are counted under packet sizes 64-1518 in RMON stats but not total Packets or Octets.
Enabling RMON capture on an interface will cause packets to be duplicated on the interface while the functionality is enabled.
Only RMON offset values of 1-1518 are supported.
RMON automatically creates entries for stats using indexes associated with each port. If any of the automatically created indexes are cleared and then associated with a new entry with an index less than 450, the new entries will not be persistent. Upon resetting the device, RMON will automatically create entries for each port using the initial default indexes. To avoid this situation, always use an index of 450 or greater when creating new entries.
Port counters and RMON counter may display differing values.
Packets greater than 1518 will not be counted by the IfInErrors MIB.
Port counters and RMON counter may display differing values.

The switch now has support for RMON Capture Packet/Filter Sampling through both the CLI and MIBs, but with the following constraints:
• RMON Capture Packet/Filter Sampling and Port Mirroring cannot be enabled on the same interface concurrently.
• The user can capture a total of 100 packets on an interface, no more and no less.
  ○ The captured frames will be as close to sequential as the hardware will allow.
  ○ Only one interface can be configured for capturing at a time.
  ○ Once 100 frames have been captured by the hardware the application will stop without manual intervention.

Known Issues from Previous Releases

• As described in the MIB, the filter is only applied after the frame is captured, thus only a subset of the frames captured will be available for display.
• There is only one Buffer Control Entry supported.
• Due to the limitations of the hardware, the Buffer Control Entry table will have limits on a few of its elements:
  ○ MaxOctetsRequested can only be set to the value -1 which indicates the application will capture as many packets as possible given its restrictions.
  ○ CaptureSliceSize can only be set to 1518.
  ○ The Full Action element can only be set to —lockǁ since the device does not support wrapping the capture buffer.
• Due to hardware limitations, the only frame error counted is oversized frames.
• The application does not support Events, therefore the following elements of the Channel Entry Table are not supported: TurnOnEventIndex, TurnOffEventIndex, EventIndex, and EventStatus.
• There is only one Channel Entry available at a time.
  ○ There are only three Filter Entries available, and a user can associate all three Filter Entries with the Channel Entry.
Configured channel, filter, and buffer information will be saved across resets, but not frames within the capture buffer.

sFlow
12004 sFlow does not sample with frame rates < 1024fps.

For the most up-to-date information concerning known issues, go to the **Global Knowledgebase** section at http://support.extremenetworks.com/**.**

For the latest copy of this release note, go to http://support.extremenetworks.com/**.**

To report an issue not listed in this document or in the **Global Knowledgebase**, contact our Technical Support Staff.

IETF STANDARDS MIB SUPPORT:

RFC No.	Title
RFC 1213	MIBII
RFC 1493	Bridge MIB
RFC 2613	SMON MIB (portCopyConfig)
RFC 2819	RMON MIB
RFC 2668	MAU-MIB
RFC 2233	IfMIB
RFC 2863	IfMIB
RFC 2620	Radius Accounting MIB
RFC 2618	Radius Authentication MIB
RFC 3621	Power Ethernet MIB
IEEE 802.1X MIB	802.1-PAE-MIB
IEEE 802.3ad MIB	IEEE 8023-LAG-MIB
RFC 2674	802.1p/Q BridgeMIB
RFC 2737	Entity MIB (physical branch only)

RFC No.	Title
RFC 2933	IGMP MIB
RFC 2271	SNMP Framework MIB
RFC 3413	SNMP Applications MIB
RFC 3414	SNMP Usm MIB
RFC 3415	SNMP Vacm MIB
RFC 3584	SNMP Community MIB
RFC 1724	RIP Version 2 MIB
RFC 1981	Path MTU for IPv6
RFC 2465	IPv6 MIB
RFC 2466	ICMPv6 MIB
RFC 2460	IPv6 Protocol Specification
RFC 2461	Neighbor Discovery
RFC 2462	Stateless Autoconfiguration
RFC 2463	ICMPv6
RFC 4291	IP Version 6 Addressing Architecture
RFC 3587	IPv6 Global Unicast Address Format
RFC 4007	IPv6 Scoped Address Architecture

PRIVATE ENTERPRISE MIB SUPPORT:

Title
ctbroadcast mib
ctRatePolicing mib
ctQBridgeMIBExt mib
ctCDP mib
ctAliasMib
ctTxQArb mib
ctDownLoad mib
ctEntStateOperEnabled and ctEntStateOperDisabled
etsysRadiusAuthClientMIB
etsysRadiusAuthClientEncryptMIB
etsysPolicyProfileMIB
etsysPwaMIB
etsysSyslogClientMIB
etsysConfigurationManagementMIB
etsysMACLockingMIB
etsysSnmpPersistenceMIB
etsysMstpMIB
etsysMACAuthenticationMIB

Title
etsysletfBridgeMibExtMIB
etsysMultiAuthMIB
etsysSntpClientMIB
etsysIeee8023LagMibExtMIB
etsysVlanAuthorizationMIB
etsysCosMIB
etsysResourceUtilizationMIB
etsysMultiUser8021xMIB
etsysTacacsClientMIB
etsysSpanningTreeDiagnosticMIB

Private Enterprise MIBs are available in ASN.1 format from the ExtremeNetworks web site at: www.extremenetworks.com/support/policies/mibs/ Indexed MIB documentation is also available.

SNMP TRAP SUPPORT:

Traps	Description
Authentication Failure	User has failed network authentication
ColdStart (RFC 1213)	System has initialized due to power-up
CPU Utilization	CPU utilization exceeds configured threshold
ctEntStateOperEnabled	Unit has joined the stack
ctEntStateOperDisabled	Unit has left the stack
etsysPsePowerNotification	Power system failure
Fan failure	Fan state transitioned from “normal to failing” or from “failing to normal”
Link Up (RFC 1213)	User port transitioned to an up state
Link Down (RFC 1213)	User port transitioned to an up state
Link Flap	Link pattern has exceeded threshold parameters
LLDP	Remote system change detected
LLDP-MED	Topology change detected on the port (that is remote device has been attached or removed from the port)
newaddrtrap	New MAC address detected on non-CDP port
Maclock violation	Detected source MAC address not permitted
Overtemperature	Transitioned to thermal alarm state
PoE inlinepower	Port status change or power threshold exceeded
Policy Inbound Rate Limit	Rate limit violation
RMON FallingAlarm (RFC 1757)	A monitored MIB decreased to a trigger value
RMON RisingAlarm (RFC 1757)	A monitored MIB increased to a trigger value
RPS Power status	Redundant Power Supply status change
STP Disputed BPDU	Disputed BPDU events exceeded threshold
STP Loop Protect	Inconsistent BPDU receipt on ISL port
STP New Root (RFC 1493)	Root bridge role transition has occurred

Traps	Description
STP Spanguard	Incoming BPDU detected on edge port
STP Topology Change (RFC 1493)	Spanning Tree topology has changed

RADIUS ATTRIBUTES SUPPORT:

Attribute	RFC Source
Calling-Station-Id	RFC 2865, RFC 3580
Class	RFC 2865
EAP-Message	RFC 3579
Filter-ID	RFC 2865, RFC 3580
Framed-MTU	RFC 2865, RFC 3580
Message-Authenticator	RFC 3579
NAS-Identifier	RFC 2865, RFC 3580
NAS-IP-Address	RFC 2865, RFC 3580
NAS-Port	RFC 2865, RFC 3580
NAS-Port-Id	RFC 2865, RFC 3580
NAS-Port-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

RADIUS Accounting Attributes

Attribute	RFC Source
Acct-Session-Id	RFC 2866
Acct-Terminate-Cause	RFC 2866

GLOBAL SUPPORT:

By Phone: 603-952-5000
1-800-872-8440 (toll-free in U.S. and Canada)

For the Extreme Networks Support toll-free number in your country:
www.extremenetworks.com/support/contact/

By Email: support@extremenetworks.com

By Web: www.extremenetworks.com/support/

By Mail: Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134 (USA)

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

APPENDIX A: CHANGES AND ENHANCEMENT HISTORY FROM PREVIOUS RELEASES

Changes and Enhancements in 1.02.06.0004
11876 & 12073 Resolved an issue with LLDP which could potentially prevent users from authenticating successfully when attached to the switch via an IP phone.
11890 Corrected a CLI issue where the ‘show config all’ command erroneously displayed the STP Loop Protect status on ports as ‘enable’ for disabled ports.
11942 Resolved an issue whereby the bufferControlTurnOnTime RMON-MIB (1.3.6.1.2.1.16.8.1.1.11) returned an incorrect value causing the wrong date and time to be displayed.
11959 Resolved an issue associated with SSH end users whereby the switch would send a challenge request to the RADIUS server after the initial request was successfully granted.
11960 Corrected an issue associated with pasting CLI commands into the console via SSH or Telnet connections whereby pasted-in carriage return characters were ignored.
12078 Resolved an issue where the CLI displayed the Diffserv service port status as ‘up’ when the link status was ‘down’.
12121 Corrected an issue whereby configuring separate RADIUS authentication and RADIUS accounting servers caused the switch to send multiple accounting request packets per authenticating user. This could cause excessive CPU loads.
12132 Resolved an issue whereby a default policy rule could prevent admin policy from being applied.
12134 Corrected a potential issue with orphaned SSH sessions Which prevented the switch from properly cleaning up the connections.
12202 The output of the CLI command ‘show lldp port‘ will now display the port Id information received in the LLDPPDU from the remote device.
12209 Resolved an issue with the STP Loop Protect feature which could potentially slow down the Spanning Tree (RSTP) failover time.
12236 The ‘show SNTP’ command now displays correct values for the latest SNTP request and update times. Previously the ‘Last SNTP Request’ and ‘Last SNTP Status’ outputs were out of sync with the current time.
12244 Resolved an issue with the ‘show dot1x auth-diag’ command output whereby the ‘Backend Auth Fails’ field was missing for some ports.
10999 Resolved an issue that prevented a user and a VoIP phone from both MAC authenticating on the same port in PC+Phone deployments.

Changes and Enhancements in 1.02.05.0004
11540 Resolved a potential SNTP issue which could cause the switch to stop processing SNTP requests. Previously the state of a server which had become unavailable would show as "Not in service" after the server became available.
11588 Corrected an issue where monitoring RMON MIB statistics via an SNMP management station could potentially cause a device reset.
11649 Corrected an issue with “show policy rule admin-profile" command whereby showing policy classification rules related to a specific egress port generated the following error: Error: Missing value for "port-string".
11668 Resolved an issue where clients on a switch failed to obtain DHCP IP addresses when DHCP snooping was set on their VLAN interfaces but not globally enabled.
11681 Corrected an issue whereby applying a new policy on ports could potentially cause existing policies to be removed.
11830 802.1x authenticated users’ MAC addresses will now be learned on ports where multiauth mode is set to strict and firstarrival is 1. Previously unauthorized devices could prevent dot1x users from connecting to the network.

Changes and Enhancements in 1.02.05.0004
11845 Resolved an issue which prevented the MGBIC-LC01 from being hot inserted.
11849 Corrected an issue whereby enabling port mirroring across the stack could cause loss of network connectivity on mirrored ports.
11886 Resolved an issue whereby replacing the management switch in a stack could cause the Cisco DP/CDP packet transmission to stop on the new manager.
11949 Corrected an issue whereby setting an IP helper address on the switch could cause the DHCP server application to fail.
12047 Resolved a potential loss of port configuration which could occur when upgrading from firmware 1.01.01.0040 and above to 1.02.04.0005.

Changes and Enhancements in 1.02.04.0005
Implemented the ability for a user to set the port mdi / mdix settings via the CLI to allow support for a variety of media converters. This feature is not supported on RJ45 Combo ports that can be used in an either/or configuration with SFP MGBICs. The commands added are: **show port mdix** { **all** | **auto** | **forced-auto** | **mdi** | **mdix** } [*port-string*] **set port mdix** { **auto** | **forced-auto** | **mdi** | **mdix** } [*port-string*] By default, Enterasys Networks switch devices are configured to automatically detect the cable type connection, straight through (MDI) or cross-over (MDIX), required by the cable connected to the port.
10981 Corrected an issue whereby terminating user sessions from Policy Manager could potentially fail for multiauth users which were authenticated via dot1x then macauth, or vice versa.
11133 Corrected an issue whereby policy applied to a GVRP enabled switch could result in the loss of management or high CPU utilization.
11338 Corrected an issue whereby the daylight savings times function would fail if the start and end times spanned across a year.
11401 Corrected a potential indexing issue with the etsysMulti1xSupplicantAddressTable MIB (1.3.6.1.4.1.5624.1.2.53.1.2.5) which was added in firmware revision 1.02.03.0012.
11444 Corrected an issue which prevented users from configuring VLAN membership for ports belonging to dynamic VLANs.
11466 The IP helper function now uses the originating routers IP address when forwarding DHCP request packets. Previously the switch replaced the source IP address of the DHCP request with its own address.
11522 Resolved an issue whereby upgrading from firmware revision 1.0.x to 1.2.x could potentially cause the LACP configuration to be lost.
11536 Corrected an issue whereby enabling port mirroring across the stack could adversely affect traffic on mirrored ports.
11543 Resolved an issue whereby attaching a Redundant PoE Power Supply to the stack manager could potentially cause high CPU utilization or loss of management after a device reboot.
11566 Corrected an issue with igmpsnooping whereby if a user authenticated with dot1x and a dynamic policy was assigned, multicast traffic could cease to transmit to the authenticated port.
11584 Corrected an issue with the "show support" command which prevented the switch configuration from being displayed in its entirety.
11586 Corrected an issue with ciscoCdpMIB MIB where the cdpCacheEntry Table (1.3.6.1.4.1.9.9.23.1.2.1.1) could potentially fail to return a value.
11597 Corrected an issue with the "show config outfile" command which could prevent the backed up configuration file from being restored properly.
11675 Corrected a CLI display issue associated with the “set port txq” command. Previously the first 2 queue values would not be displayed when 100% of the traffic was assigned to the highest transmit queue.

Changes and Enhancements in 1.02.04.0005
11865 Corrected a potential connectivity issue whereby after a device reset, auto-MIDX was not enabled on ports with auto negotiation disabled.

Changes and Enhancements in 1.02.03.0012
Added a new feature that allows you to troubleshoot and locate faults in copper cable connections on a per port basis. A new CLI command, **show port cablestatus** <*port-string*>, allows you to diagnose cabling problems in realtime. The command returns the following: **Normal = normal** **Open = no cable attached to port** **Short = detection of an inter-pair short** **Fail = unknown error or crosstalk** **Detach = for ports on stack units no longer present, but were previously connected** **Not Supported = ports other than 1GE RJ45 ports** This command is only supported on RJ45 copper connections running at 1GE speeds.
9260 Added support for the ctAliasProtocolTable, ctAliasMacAddressTable, and ctAliasClearAll objects to the ctAliasMib MIB. Previously, multiple entries with the same MAC address on the same port could potentially cause the IP resolution for that MAC address to fail.
11204 Corrected an issue where removing an existing DHCP Relay Agent followed by adding a DHCP server on the switch could cause the server to fail.
11324 Resolved an issue where the UDP helper function would not forward packets destined to UDP port 4011.
11342 A change has been made which eliminates the second attempt to authenticate through a RADIUS server when the first attempt (using the specific client MAC address) is rejected and the mask to be used for the second attempt is set to all “F”s.
11377 Corrected an LLDP issue where the “show neighbor” command failed to display the neighbors' host IP addresses.
11385 Corrected an issue where high rates of multicast traffic caused pause frames to be generated on the upper ports (25-48) of B3G124-48/48P devices.
11401 & 11402 Added support for the etsysMulti1xSupplicantAddressTable (1.3.6.1.4.1.5624.1.2.53.1.2.5) from the Multi User 802.x MIB. This table gives a list of current dot1x users and indicates whether they are active (authenticated) and the user name associated with that user.
11420 The DHCP snooping function has been changed to only rate limit untrusted ports when a rate limit is configured. Previously, the rate limit was applied to all trusted and untrusted ports.
11599 Corrected an issue where upgrading a PoE capable switch or stack of switches to 1.02.03 could potentially cause “ge.1.1” link up to fail.

Changes and Enhancements in 1.02.02.0009
10597 & 11408 Resolved an issue in multiuserauth mode whereby an inactive user was dropped from the egress VLAN list and could no longer transmit packets out the egress VLAN.
10762 Resolved an issue where concurrent execution of the enterasys-resource-utilization-mib MIB could potentially cause a reset.
10827 Corrected an issue where the “show system” command failed to display maximum temperature threshold settings.
10889 Resolved an issue where a 2-port LAG would not failover to a single port LAG when a member port was removed.

Changes and Enhancements in 1.02.02.0009
10973 Corrected an issue where oversized SSH packets potentially caused a switch reboot.
10993 & 11071 Corrected an issue where the “show config” command would not display port speeds configured via CLI or WebView.
11070 Corrected an issue where VLAN egress settings via NetSight would not persist after a reboot.
11125 The fan number designators are now consistent between the CLI and Syslog messages.
11131 The RADIUS Filter-ID attribute is no longer case sensitive for management users.
11156 & 11322 Corrected an issue where the “show mac type self” command displayed an incorrect MAC address and could potentially lockup the CLI.
11168 Corrected an issue where manually configured port speed settings were not saved in the config file. System restoration using a newly saved config file properly restored configured port speeds.
11202 Corrected an issue with DHCP snooping across LAG ports which could prevent clients’ MAC addresses from being added to the bindings database.
11205 & 11206 Corrected an issue where the “show vlan portinfo vlan” command failed to display member LAGs and associated port details.
11215 Resolved an issue where enabling maclock agefirstarrival would fail to remove aged-out firstarrival maclock entries.
11221 Resolved an issue with DHCP snooping which could cause the server’s messages to be duplicated by the switch.
11234 Corrected an issue where user configured CDP hold time values would not to be applied. The default hold time value would be used instead.
11237 Corrected an issue with multiauth strict mode where the second user on a port would not appear in the forwarding database.
11240 Resolved an issue where “clear multiauth mode” did not restore default settings.
11260 Corrected an issue where B3s running RIP protocol in a mixed stack would attempt to apply the previously configured routing configuration when loading the 4.xx.xx image.
11267 Corrected an issue where the entPhysicalSerialNum MIB (1.3.6.1.2.1.47.1.1.1.1.11) could potentially return the wrong Serial Number.
11275 Corrected an issue where only the first IGMP group join message would be processed by the switch. All additional requests would potentially be ignored.
11372 Corrected an issue where fan tray operational failures would not generate Syslog messages.

Changes and Enhancements in 1.02.01.0004
Added multi-user authentication support for up to 3 concurrent policy users per port. Added support for the etsysMulti1xAccessEntityTable and etsysMulti1xSessionStatsTable MIB sets for monitoring multiple authenticated users per port via NetSight Policy Manager.
Added DHCP spoofing protection via DHCP snooping. Previously you could use Enterasys Policy to protect your DHCP services, but now DHCP protection is independent of ETS Policy. As a result you can reclaim those ETS Policy resources and use them to protect other network services.
Added protection from man-in-the-middle ARP spoofing attacks. This feature works in conjunction with the DHCP snooping database to ensure that ARP requests match the IP/MAC/Port binding relationship dynamically created during DHCP client/server exchanges.
Added support for the etsysResourcesScalarsGroup attribute from the etsysResourceUtilizationMIB to enable remote monitoring of the CPU load via SNMP management tools.

Changes and Enhancements in 1.02.01.0004
Added the ability for multiport LAGs to continue operating in multiport mode as long as there is at least one active port in the LAG. Previously administrators would need to create backup single-port LAGs to ensure that a multi-port LAG would not change its behavior if all but one port dropped out of the LAG. This redundant configuration effectively reduced the number of LAGs that could be configured in the switch by half. Alternatively, you would have had to configure egress tagging at the port level to match the LAG configuration ensuring that traffic would be marked appropriately when only a single port remained active.
Added support for forwarding broadcast IP traffic to a unicast IP address via the “ip forward-protocol” command.
10395 Added support for disabling ICMP redirects on routing interfaces to reduce CPU loads on certain configurations.
Added support for protecting the health of the switch based on predetermined safe operating temperature limits. The administrator can change the maximum thermal threshold where a trap and syslog message is generated warning them of high-temperature conditions before service is affected.
Modified the “set boot system” command to prompt the administrator before resetting the switch. If the administrator elects not to reset the switch, the new firmware is copied into the active partition but only takes effect after the switch is reset/rebooted.
Modified the newmac trap to include the MAC address of the client in the SNMP trap.
10274 & 10183 Corrected an issue where the first packet through the switch is dropped with policy applied, subsequent packet transmissions are successful.
10585 Resolved an issue where stacking switches using a 5 meters cable (C2CAB-5M) would cause errors on stack ports.
10995 Corrected an issue that prevented the “switch description” field from being permanently stored in the configuration.
10795 Addressed a potential SNMP vulnerability identified in US-CERT VU#878004.
9842 Resolved an issue with Cisco DP where the “show neighbor” command displayed an incorrect port ID

Changes and Enhancements in 1.01.06.0007
11052 Resolved an issue introduced in release 1.01.06.0006 that affected reassembly of IP fragments directed at a routed interface or the host address of the switch.

Changes and Enhancements in 1.01.06.0006
10256 Resolved an issue where enabling port mirroring on a link would cause STP to be disabled on the port.
10704 Corrected an issue whereby running macauth and dot1x simultaneously would cause port policies to be removed.
10809 Corrected a CLI issue where restoring a config file containing an extra space before the end of line generated errors.
10816 Corrected an issue where “clear port lacp port" did not restore default port LACP settings.
10848 Changed the MST configuration name default string from the bridge MAC address to a more generic name “default".
10874 Corrected an issue when under certain circumstances the SNTP client stopped processing requests.
10906 Corrected an issue that could prevent policy configurations from being loaded by the switch.
10972 Corrected an issue which could result in the loss of SNMP management.

Changes and Enhancements in 1.01.05.0004
10061 Added a CLI prompt message to "set port vlan" informing users that setting VLAN membership for dynamic VLANs is not supported.
10542 Corrected an issue where clients performing 802.1X authentication on ports configured for multiauth failed to obtain DHCP IP addresses after a device reset.
10201 Corrected an issue where "set switch movemanagement" caused the policy application to fail.
10440 Corrected an issue where the "[no] ip routing" command was not linked to the MIB-2 IpForwarding object.
10521 Resolved an issue which prevented DHCP clients from obtaining IP addresses from the DHCP server.
10700 Corrected an issue which prevented the "host ip" value to be properly restored from a saved configuration file.
10056 Enhanced 802.1x authentication whereby the switch continues to send periodic Unicast Request Identity frames after the first client authenticates. Previously the switch stopped sending EAP frames after the first successful authentication.
10356 Corrected an issue where enabling port mirroring would stop traffic flow across ports that were not members of the mirror group.
10712 / 10676 Corrected an issue where default policies were removed thus preventing 802.1x clients from authenticating.
10597 Resolved an issue in multiuserauth mode whereby an inactive user was dropped from the egress vlan list and could no longer transmit packets out the egress vlan.
10655 Resolved an issue where client authentication failed when the management ip address was not configured.

Changes and Enhancements in 1.01.04.0001
10140 Corrected an issue with the LLDP MIB implementation that could result in the loss of SNMP management or high CPU utilization.
10396 Corrected an issue whereby after an initial invalid RADIUS request fails, subsequent valid requests were rejected for the same user due to caching of the initial RADIUS state attribute.
10551 Corrected an issue with displaying the correct LACP partner key when doing a "show port lacp port <port string> status summary" command.
10443 Corrected an issue with the "clear radius server" command that could result in a reset.
10627/10697/10250 Corrected an issue whereby disabling dot1x on an authenticated port could affect SNMP management or cause a reset.
10314 Corrected an issue where ports could fail to 802.1x authenticate valid users if mac locking was enabled.
10324 Corrected an erroneous interface message timeout reset (NIM timeout event) caused during management changes of complex interface configurations.
10554 Corrected an issue causing an SSH login to appear to hang in configurations where the motd banner and length are set.
10501 Corrected an issue where "show mac type self command" would fail to show local mac addresses.
10498 Corrected a display issue with the "show config all spantree" command caused by a page break truncating the output.
10535 Added the ability to set the PVID on a port with a VLAN learned via GVRP. A new informational message "INFO: PVID has been set. VLAN membership cannot be set on dynamic VLAN" alerts the administrator that PVID is settable on a dynamic VLAN but VLAN membership is not configurable.
10227 Corrected issue with RADIUS server redundancy which could prevent users from authenticating via the secondary server.

Changes and Enhancements in 1.01.04.0001
10486 Corrected an issue where ACL entries restored using a configuration file could fail to be applied.

Changes and Enhancements in 1.01.03.0003
Corrected an issue in the Policy MIB where the etsysPortPolicyProfileSummaryTable (1.3.6.1.4.1.5624.1.2.6.3.3) failed to return a value for etsysPortPolicyProfileSummaryOperID.
Corrected an issue that prevented multiple 802.1x Policy authentications on a single port.
Corrected an issue where receiving constant pauses frames on a port could cause Spanning Tree instability on the switch.
Corrected a potential reset associated with one form of interface message timeout “NIM: Timeout event”.
Corrected an issue with GVRP that could cause a failure to properly configure egress on learned VLANs.
Corrected an issue where the port inlinepower admin state was not persistent.
Corrected an issue in the readability of output of the “show config vlan” command.
Corrected an issue where ASM is unable to apply actions to ports.
Corrected an issue concerning the “set ip protocol” command. If the static IP address of a switch is stored in a configuration file, then the IP is changed to be acquired using DHCP, the original IP can now be restored using the saved configuration file.
Corrected an issue with persistence of port advertised capability on combo ports.
Corrected an issue where high rates of multicast traffic caused pause frames to be generated on the upper ports (25-48) of 48 port B3G124-48/48P devices.
Corrected an issue with the RADIUS reauthentication timer. During an unrecognized overflow condition which occurred approximately once every 49 days, the switch would constantly attempt to authenticate all RADIUS supplicants. This would last for a period equal to the authentication time.
Corrected an issue in Policy that could prevent the application of a profile after a system reboot. Previously a hardware error would be given indicating a failure to set a profile on a port.

Changes and Enhancements in 1.01.02.0007
Corrected an issue where permanent licenses were incorrectly detected as having expired.
Corrected an issue with the “show mac port” command displaying output from multiple ports.
Corrected an issue where SSH IdleTimeOut was not initialized, causing a failure to timeout SSH sessions.
Corrected a potential memory corruption and reset associated with the MAC authentication process
Corrected a potential NIM timeout event reset associated with deleting interfaces with large numbers of VLANs (>1000).
Corrected an issue where Dynamic Egress failed if a rule to discard tagged packets was applied to the port.
Corrected a display issue where clearing default role on a port with Policy Manager, would prevent the display of user roles.
Corrected an issue in the MAU-MIB ability to set dot3MauType to dot3MauType1000BaseTFD.
Corrected an issue that could result in the inability to apply previously acceptable policies to ports after a system reboot.
Corrected an issue that prevented proper operation of IGMP Snooping on ports that had authenticated to a new VLAN.
Enabled the ability to syslog messages greater than 124 Characters in length. Previously some messages may have been truncated.

Changes and Enhancements in 1.01.01.0051
Corrected an issue in the Enterasys CoS MIB that could prevent new CoS MIB settings from being applied and enforced from Policy Manager. This issue was originally introduced in the 1.01.01.0047 firmware.

Changes and Enhancements in 1.01.01.0049
Corrected an issue with Bridge MIB that inverted the reading and setting of VLAN tagged egress. Untagged egress would read as tagged. Tagged VLAN egress would read as untagged. Setting tagged egress would result in untagged egress. Setting untagged egress would result in tagged egress. This issue was introduced in the previous release (1.01.01.0047)
Corrected an issue in the display of SNMP configuration that could cause a system reset when the “show configuration” command was issued. This issue was introduced in the previous release (1.01.01.0047)

Changes and Enhancements in 1.01.01.0047
Added Support for CoS MIB based flood control of broadcast, multicast and unknown unicast traffic.
Added SMON MIB support for management of Port Mirroring.
Added support for monitoring resource utilization via the etsysResourceUtilizationMIB.
Corrected a CLI issue that prevented insertion of text without erasing the remainder of the command line.
Corrected a reset issue with the “clear radius” command.
Corrected a reset issue with the “show config outfile command”.
Corrected an issue that prevented the clearing of the admin login using the “clear system login” command.
Corrected a display issue in the “show system utilization process” command.
Corrected an issue with counting RMON Statistics for 1024-1518 octet packets.
Corrected an issue with forwarding static multicast addresses after a reset.
Modified the Span Guard port lockout state to disable the port if the spanguardtimeout is set to zero. This will prevent any control traffic on this port from being processed when locked.
Moved the informational message “ewaNewConnection EmWeb socket accept() failed: S_errno_EWOULDBLOCK” to the informational level (7) for Syslog.
Corrected a potential loss of Spanning Tree configuration when upgrading from earlier images.
Corrected a CLI display issue with the “show inlinepower” command when the command is executed over an SSH session.
Added CLI support for the port string format of type ge.1-2.1.
Corrected an issue in migrating policy TCI rule configurations when upgrading system firmware from earlier images.
Corrected an issue that caused loss of SNMP configuration when restoring a configuration file.
Jumbo packets are now counted as errors when jumbo packets are disabled on the switch.
Modified the SNTP poll interval to be set as a power of 2 to conform to RFC1305.
Previous images supported only a single permit or deny any rule per ACL. The SecureStack B3 will now support one each for ICMP, UDP, TCP, and IP.
Improved the resiliency of the host process by ensuring control traffic (e.g. BPDUs) gets higher priority during heavy traffic loads.
Removed the requirement for a Policy license to support multiple RFC3580 VLAN authenticators per gigabit port.
Router will now accept a RIPv2 route with a 32 bit mask.
Corrected an issue were Policy rule counts could potentially be updated incorrectly when a rule was removed. This could have prevented new rules from being added.

Changes and Enhancements in 1.01.01.0040
Corrected a shared-memory timing issue that in rare circumstances could affect management access to the switches after a reset. The new code ensures that shared memory is accessed in an orderly fashion by multiple processes during startup.

Changes and Enhancements in 1.01.01.0039
Implemented the new Enterasys standard version numbering system on the SecureStack B3.
Added support for layer 3 functionality including: RIPv1/v2, ACLs, IRDP, IGMPv2/v3 querier, directed-broadcast, and traceroute.
Changed the default logging severity level to 6. The result of this will be that more informational messages may be seen in Syslog and CLI than in previous images. However, this does not affect the operation of the switch.
Added support for LACP short timers.
When a fiber port is disabled, both the transmit and receive links of the port will now be disabled.
Multi-word VLAN name assignments are supported and persistent when encapsulated in quotes.
Users can ping the host IP address from any port in a mixed stack as long as the port has the proper VLAN egress configuration.
Resolved an issue with policy where in certain configurations port policy assignments weren't being removed properly.
Support has been added for RFC-3580 VLAN authorization in conjunction with MAC Authentication services.
With a basic PWA configuration on the stack, users can now access the PWA login page by simply entering the PWA server IP address instead of being required to enter the entire URL.
Modifying the MACLock Firstarrival value will limit the number of user allowed network access on the port. Changes to this value will be enforced on the number of current users as well as new users.
Corrected the reporting of physical port and LAG port speeds using the ifSpeed MIB.
When executing the command "show config", the output will encrypt the passwords of SNMP users.
Resolved an issue where MAC Authenticated devices that were continuously sending data were required to re-authenticate every 10 minutes or so even though re-authentications has been disabled.
Multi-word SNMPv3 group names can now be configured and deleted as long as the group names are encapsulated in quotes.
The CLI output of the "show cdp", "show port egress", and "show mac port <port>" commands will now be managed properly by the terminal display value set using the "set length" command.
Removed an additional offset seen in the display output of the SNMP configuration when executing the CLI command "show config" or "show config snmp".
Modifying the lacptimeout value will no longer require globally disabling and re-enabling LACP to be enforced.
LAG ports which are spread across multiple units in a stack have been made more resilient in the event of a failure of one of the stack members.
Corrected an issue caused by an incorrect port index being used which presented itself as the Syslog message "Invalid hpc_index of 0".
Added support for the dot1dStpPortPathCost mib.
When configuring multiple RADIUS servers on the SecureStack, the RADIUS index will be used to determine the sequencing of which RADIUS server the RADIUS Access Request packets will be sent to when a client attempts to authenticate.
Users now have the ability to set objects via name for RMON Alarms, such as "set rmon alarm properties 1 object ifOperStatus.1".
A static LAG between multiple units of a SecureStack switch and a Cisco 2950 switch will now recover after a "set switch movemanagement" command is executed.
Static ARP entries are preserved across resets.
Corrected an IP assignment issue that occurred when more than one user authenticated via 802.1X from the same computer and was assigned to a different VLAN.
RMON Packet capture now displays bidirectional traffic.
When using policies with the untagged-vlan option, the VLAN egress will now be properly assigned when the policy is applied.

Changes and Enhancements in 1.01.01.0039
Corrected an issue with multiauth, where after an extended period time users trying to authenticate on the network would get trapped in a connecting state and were unable to gain network access.
The "show mac" and "show arp" commands will continue to reflect accurate information on all physical ports which have MAC Authentication enabled.
Corrected an issue in SNTP that prevented time synchronization to a broadcast SNTP server.
When polling the dot1dStpVersion oid, it will return the proper value for the Spanningtree version configured on the stack.
Resolved an issue where after rebooting a PC and re-authenticating, user's ports were not being assigned the appropriate policy.
Values for the MIB-2 counters will remain persistent regardless of link state.
The SecureStack will cease sending SNTP requests to SNTP servers which have been removed from the device configuration.
User configured forbidden egress settings will remain persistent in the device configuration and take precedence over dynamic VLAN assignments learned via GVRP.
Implemented dynamic rule allocation based on Policy type to manage policy resources.
The node alias create time information is now measured in Ticks as defined in the MIBs for ctAliasTimeFilter and ctAliasMacAddressTime.
Corrected an issue where the "show mac type self" command would not use the default of all ports when a port string was not entered.
When polling the dot1dTpFdbPort MIB, the results will be returned in ascending order.
Logging commands will remain persistent after executing the "set switch movemanagement" command.
The RADIUS Filter-ID case is no longer case sensitive.
The switch "clear arp all" command will only clear dynamic ARP entries.
Diffserv now supports the feature to class match based on VLAN Id.
Corrected an issue with calculating reauthentication periods when the internal real time clock rolls over. Approximately once every 50 days, for a time equal to the configured reauthentication period, all users with reauthentication enabled will continuously attempt to authenticate.
Corrected an issue in the IPNettoMedia MIB that prevented the ability to query the host ARP cache using SNMP.
Corrected an issue in the Bridge MIB implementation that could prevent querying learned MAC addresses using SNMP.
Corrected an issue in SNTP that prevented time synchronization to an SNTP server sending unicast traffic.
Corrected a CLI display issue with the alignment of output from the "show inlinepower" command.
Corrected the potential loss of a policy mask resource that could prevent some previously acceptable policy configurations from being applied. This issue was introduced with the forwarding of multicast addresses in the range of 01-80-C2-00-00-00 to 01-80-C2-00-00-FF. If you need to forward these multicast addresses you must now enable the "set mac unreserved-flood" command.
Corrected a potential reset condition that occurred when clearing the RMON history using the "clear rmon history to-defaults" command.
Corrected an issue that occurred when processing an invalid policy role received from RADIUS. The switch now applies the default port role, where previously the existing port role was unchanged.
Corrected a display issue where the operational status of a port would incorrectly be shown as "up".
Updated the Syslog event format to comply with the RFC 3164 standard.
Added a new feature enhancement to support LACP short timers.
Corrected an issue with RMON packet capture displaying only ingress packets.
Corrected a potential memory leak associated with SNMP calls with exception conditions.
Corrected an issue in the "set policy profile" command that could prevent users from cutting and pasting configurations.
Corrected an issue in setting SNTP server precedence. We now allow up to 10 entries.
Corrected a display issue with the CLI help for the "show mac type ?" command.
Corrected an issue where access lists that are applied to ports that only contain a LAG do not get displayed in the configuration.
Corrected an issue where the MIB object ifOperStatus of the host port would always return "down".
Corrected an issue in the DHCP server CLI that could prevent long strings from being entered.

Changes and Enhancements in 1.01.01.0039
Updated the SNTP poll interval value to be configured as a power of 2, with a valid range between six and ten as described in RFC-1305 (i.e., a poll interval set to “6” would be equal to 2^6 or 64 seconds). If upgrading from configuration which has a SNTP poll-interval set outside of the valid range of between 6 and 10, the default of 6 (2^6 = 64 seconds) will be set.
The SecureStack device will no longer send SNTP requests to SNTP servers which have been deleted from the device configuration.
Corrected processing of packets with network directed broadcast addresses to enable support for the SNTP Broadcast mode.
Resolved a Policy issue where PCs were not being correctly reassigned to the default policy if they were rebooted.
Rectified an issue where policies using the untagged-vlan option were not writing the correct VLAN egress into the device hardware.
The aging process for MAC Authentication has been modified. If a MAC address is learned on multiple VLANs, but only remains active on one VLAN (such as having been reassigned to a new VLAN after MAC Authenticating), the device will now age out the correct MAC address entry by keying on the MAC address/VLAN id pair.
GVRP will no longer have an effect on static VLAN settings manually configured by the administrator.
Noticeably improved the routing performance of clients which are using MAC Authentication.

GLOBAL SUPPORT:

By Phone: +1 877-801-7082 (toll-free in U.S. and Canada)

For the toll-free support number in your country:
www.extremenetworks.com/support/

By Email: support@extremenetworks.com

By Web: www.extremenetworks.com/support/

By Mail: Extreme Networks, Inc.
145 Rio Robles
San Jose, CA 95134

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