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

Customer Release Notes

B-Series B5
Firmware Version 6.81.07.0004
March 2016

INTRODUCTION:

This document provides specific information for version 6.81.07.0004 of firmware for the following B5 products:
Note: this version of firmware is **not compatible** with the Enterasys **B2 or B3** platforms.

B5G124-24	B5G124-24P2	B5G124-48	B5G124-48P2
B5K125-24	B5K125-24P2	B5K125-48	B5K125-48P2

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:
www.extremenetworks.com/support/contact/

FIRMWARE SPECIFICATION:

Status	Version No.	Type	Release Date
Current Version	6.81.07.0004	Maintenance Release	March 2016
Previous Version	6.81.06.0002	Maintenance Release	November 2015
Previous Version	6.81.05.0003	Maintenance Release	July 2015
Previous Version	6.81.04.0001	Maintenance Release	April 2015
Withdrawn	6.81.03.0007	Maintenance Release	March 2015
Previous Version	6.81.02.0007	Maintenance Release	Sept 2014
Previous Version	6.81.01.0027	Feature Release	April 2014
Previous Version	6.71.04.0004	Maintenance Release	January 2014
Previous Version	6.71.03.0025	Maintenance Release	October 2013
Previous Version	6.71.02.0008	Maintenance Release	July 2013
Previous Version	6.71.02.0007	Feature Release	June 2013
Previous Version	6.71.01.0067	Feature Release	May 2013
Previous Version	6.61.08.0013	Maintenance Release	March 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

Status	Version No.	Type	Release Date
Previous Version	6.51.02.0018	Feature Release	October 2011
Previous Version	6.42.03.0004	Maintenance Release	January 2011
Previous Version	6.42.02.0006	Maintenance Release	December 2010
Previous Version	6.42.01.0046	Maintenance Release	November 2010
Previous Version	6.41.06.0002	Maintenance Release	August 2010
Previous Version	6.41.05.0001	Maintenance Release	July 2010
Previous Version	6.41.04.0003	Maintenance Release	June 2010
Previous Version	6.41.03.0018	B5 Only Feature Release	June 2010

HARDWARE COMPATIBILITY:

This version of firmware is **not compatible** with **B2 or B3** platforms. This version of firmware is **only supported** on the **B5** switch family.

BOOTPROM COMPATIBILITY:

This version of firmware is compatible with all boot code versions of the B5.

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-LC04	100Base-FX, IEEE 802.3 MM, 1310 nm Long Wave Length, 2 KM, LC SFP
MGBIC-LC05	100Base-FX, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 KM, LC SFP
MGBIC-BX10-D	1000Base-BX10-D 1 Gb, Single Fiber SM, Bidirectional, 1490nm Tx / 1310nm Rx, 10 km, Simplex LC SFP (must be paired with MGBIC-BX10-U)

MGBICs	Description
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)

The following 10 Gb transceivers are supported in the B5K models only:

10 Gb Transceivers	Description
10GB-ER-SFPP	10 Gb, 10GBASE-ER, IEEE 802.3 SM, 1550 nm Long Wave Length, 40 km, LC SFP+
10GB-LR-SFPP	10 Gb, 10GBASE-LR, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 km, LC SFP+
10GB-LRM-SFPP	10 Gb, 10GBASE-LRM, IEEE 802.3 MM, 1310 nm Long Wave Length, 220 m, LC SFP+
10GB-SR-SFPP	10 Gb, 10GBASE-SR, IEEE 802.3 MM, 850 nm Short Wave Length, 33/82 m, LC SFP+
10GB-C10-SFPP	10 Gb, pluggable copper cable assembly with integrated SFP+ transceivers, 10 meters
10GB-C03-SFPP	10 Gb, pluggable copper cable assembly with integrated SFP+ transceivers, 3 meters
10GB-C01-SFPP	10 Gb, pluggable copper cable assembly with integrated SFP+ transceivers, 1 meter
10GB-LW-SFPP	10 Gb, Laserwire® SFP+ adapter for use with Laserwire cable assembly
10GB-F10-SFPP	10Gb SFPP to SFPP AOC 10 M
10GB-F20-SFPP	10Gb SFPP to SFPP AOC 20 M
10GB-BX10-D	10Gb, Single Fiber SM, Bidirectional, 1330nm Tx / 1270nm Rx,10 Km SFP+
10GB-BX10-U	10Gb, Single Fiber SM, Bidirectional, 1270nm Tx / 1330nm Rx, 10 Km SFP+
10GB-BX40-D	10Gb, Single Fiber SM, Bidirectional, 1330nm Tx / 1270nm Rx, 40 Km SFP+
10GB-BX40-U	10Gb, Single Fiber SM, Bidirectional, 1270nm Tx / 1330nm Rx, 40 Km SFP+
10GB-USR-SFPP	10 Gb, Ultra Short Reach Multi-mode, 850 nm, 100m on OM3 SFP+
10GB-ZR-SFPP	10 Gb, 10GBASE-ZR, SM, 1550 nm, 80 Km SFP+

*The Laserwire® mark is a registered trademark and is the property of Finisar Corporation.

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 6.81

IPv6 UDP/TCP port rules - Policy UDP/TCP source and destination port rules will now apply to both IPv4 and IPv6 traffic. These rule types require no additional policy resources.
IPv6 Destination Address rules – Policy support for IPv6 destination address rule.

IPv6 Router Advertisements drop rules – Policy support for ICMPv6 type = 134 drop rules.
Increased Policy Roles – System role (Profile) limit increased from 15 to 21.
Denial Of Service Control – Application to support hardware based drop rules for common forms of network attacks. These checks can be run simultaneously with the Policy application.
Default Route Redistribution – Added optional redistribution of default route to both RIP.
RADIUS Accounting - Extended Accounting to include management-access users.
MAC Authentication auth-mode - MAC authentication can be configured to use the RADIUS server configured username credential where the password is the same as the username.
MIB object chEnvAmbientStatus of the CTRON-ENVIRONMENT-MIB – Allow remote SNMP monitoring of thermal state of the master unit.
Enterasys Networks' Multiple Authentication MIB Notification Group – Added support for etsysMultiAuthSuccess, etsysMultiAuthFailed, etsysMultiAuthTerminated, etsysMultiAuthMaxNumUsersReached notifications.
Diagnostic Message MIB - The Enterasys Diagnostic MIB allows network administrators to monitor the current.log file through snmp.
RADIUS Accounting Client MIB - Enterasys RADIUS Accounting Client MIB allows network administrators to configure radius accounting.
Login Accounts – Increased the number of supported local login accounts from 16 to 32.

Existing Product Features	
Hybrid Policy Mode	VLAN-to-Policy Mapping via hybrid mode
LLDP-MED Network-Policy TLV	sFlow support
TACACS+ management support	Host Protect (permanently enabled)
Standard and Extended ACLs	AES-128 support with SNMPv3
Secure Copy / Secure FTP (SCP/SFTP)	Selectable source management interfaces
Power Supply & Fan Monitoring via SNMP	IP Forward-Protocol command
Copy & Paste of configuration files between switches	ARP Spoof Protection
Multi-user authentication per port (up to 4 policy users per port)	High-Temperature Alerts
Multiport LAG to single port LAG automatic failover	Show support command
DHCP Spoof Protection	Configurable Login Banner
Control mdi/mdix port settings via CLI to prevent network loops	24 Gbps Full Duplex (48 Gbps bidirectional) closed-loop stacking
TDR-based cable status check detects cable breaks and disconnections	32K MAC Address Table
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 4)

Existing Product Features	
802.1w – Rapid Spanning Tree	User + IP Phone Authentication
RFC-3580 dynamic VLAN assignment 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
MSTP Multisource Detection	Spanning Tree Diagnostic MIB
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
Multicast Listener Discovery (MLD) Snooping	L2 IGMP/MLD Querier
Syslog	New MAC Trap
Text-based Configuration Upload/Download	Dynamic Egress
CLI Management	SSHv2 Support
Telnet Support	WebView
IPv4/IPv6 Dual Host Management Support (SNMP,Telnet,SFTP,SCP,SSH,RADIUS)	SSL Interface to WebView
Discard VLAN Tagged Frames	RMON (4 groups)
Jumbo Frame (up to 9K)	RMON View in the CLI With Persistent Sets
Priority Classification L3-L4	RMON Packet Capture/Filtering Sampling
VLAN-to-Policy Mapping on a per Port Basis*	SNMPv1, SNMPv2c, SNMPv3
Node/Alias Table	Simple Network Time Protocol (SNTP)
ToS Rewrite	CPU/Memory utilization monitoring via SNMP
SMON MIB support for Port Mirroring	Alias Port Naming
Basic IPv4 Routing (static, RIP v1/v2, IRDP)	Ability to Set Time and Date via the MIB
Multiple IP Helpers per Interface (up to 6)	32K MAC Address Table
CoS MIB based Flood Control (broadcast, multicast, and unknown unicast)	IEEE 802.3at High Power
Policy Included in all B5 Switches	Improved Policy Capabilities (4 users per port and 250 rules per profile)
No Backwards Stacking	100Base-FX Support on All SFP Ports
10 Gb Support	Display 802.3 pause counters
Tx Queue Monitoring	Service Access Control Lists
IPsec for RADIUS transactions	Command Logging
Access Control Lists	SNTP Server-Client Authentication
Increased Password Security	Console Disconnect

Existing Product Features	
Login Banner	VLAN 4094
VLAN Classification	Mixed Strict and WRR Port Transmit Queue settings
Password Reset Button Enhancements	Security Log
OpenSSL FIPS Object Cryptographic Module	Secure directory
Time Based Reset	Flexible Link Aggregation Groups
Convergence End Points (CEP) Phone Detection	Automated Deployment

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:

- 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.

- Complete stacks running code prior to 6.51 can be successfully upgraded to 6.51 (or later) by just upgrading the Master Switch.

- 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 B5 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 www.extremenetworks.com/support/contact/ for the latest firmware updates to the B-Series B5 and follow the TFTP download instructions that are included in your *B5 CLI Reference* and the *Fixed Switch Configuration Guide*.

Soft copies of the *B5 CLI Reference* and *Fixed Switch Configuration Guide* are available at no cost on the Extreme Networks web site, www.extremenetworks.com/support/contact/.

The B5 family of stackable switches is managed by a single IP address for a stack of up to 8 switches.

To download the new software to a stack of B5 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 for B5 Only

Feature	Capacity
Policy roles (profiles) per system	21
Number of users per port	Tunnel Mode = 4, Policy Mode = 4, Hybrid Mode = 4
Number of unique rules per system	1536
L3/L4 rules	1024 (768 ipv6dest enabled)
EtherType rules	256
MAC rules	256
IPv6 Destination Address	256 (ipv6dest enabled)
Number of rules per single role	250
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
IPv6 dest	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

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
Multicast Groups	512
IGMP Static Routes	100

sFlow Capacities

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

ACL Capacities

Feature	Capacity
Access Rules (inbound only)	200
Access Rules – Per ACL IPv4 IPv6 MAC	40 per list – 120 per interface 1536/512 ipv6mode 512 512
Access Rules – Per system IPv6 IPv6, in no ipv6mode MAC/IPV4 MAC/IPV4, in no ipv6mode MAC/IPv6 MAC/IPv6 , in no ipv6mode	100 total per system 256 0 256 768 256 0
Access Rules – Per port IPv6 MAC/IPV4 MAC/IPv6	 60, 20 per ACL list 60, 20 per ACL list 60, 20 per ACL list

FIRMWARE CHANGES AND ENHANCEMENTS:

Changes and Enhancements in 6.81.07.0004
19650 Corrected a reset issue that can occur when an IP helper address is configured for the same subnet as the interface it is added to.
19644 Corrected an issue in Port mac locking that could result in a ““nim_events.c(213)” reset event.
19320 Corrected an issue where the SNTP server table is restored in reverse order from entry configuration.
19614 Added support for UDP port 7777 to “ip forward-protocol”. Note: Other ports not specified the configuration guide are still not supported by this functionality.
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):”
19649 Corrected an issue in the display of radius server configuration that could erroneously be detected as a configuration change.
19568 The previous resolution to this issue was not complete if Cisco CDP is being used.

Changes and Enhancements in 6.81.06.0002
19608 Corrected a potential reset condition when attempting to save a prompt (“set prompt”), of 50 or more characters.
19511 Corrected a potential loss of management and eventual reset condition seen when monitoring the etsysResourceUtilizationMIB.
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.
19579 Corrected an issue where the “set length" command was not persistent.
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.
19588 Corrected a reset issue in the LLDP application, which produced the log entry, “reset caused by buff.c(546)”
19599 Corrected a condition that prevented switching user’s VLAN from RFC3580 assigned to Policy assigned.
19552 Some remote PD devices require PoE Negotiation over LLDP to enable. C5 POE capable switches will now respond to PD power request in the Power via MDI IEEE 802.3 Extensions TLV. This TLV must first be enabled “set lldp port tx-tlv poe”. The inlinepower management mode must also be ‘realtime”.

Changes and Enhancements in 6.81.05.0003
19553 Corrected a potential reset condition when processing jumbo 802.1x and 802.1s control frames.
19568 Extreme Summit and BlackDiamond platforms may use a single source MAC address for protocol and host generated packets. Previously, If redundant connections were 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 would resulting in loss of connectivity to their host IP address.
19267 Corrected an issue that could prevent SFPs from linking on bootup if auto-negotiation is disabled.

Changes and Enhancements in 6.81.05.0003
19534 Corrected an SNMP issue with in the ctChasPowerTable where power supply redundancy may be incorrectly returned.
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.
19440 Updated MIB to support new 10G ifMauTypes found in RFC3636.

Changes and Enhancements in 6.81.04.0001
19532 Corrected an issue where configuration changes are not saved on member units. This may result in loss of configuration on change of master unit.

Changes and Enhancements in 6.81.03.0007
Added Support for the Extreme Stacking MIB. Note: Not all objects translate to B5-Series functionality (see know issues).
19319 The TLS_FALLBACK_SCS mechanism was added to SSL. When run with a supporting browser, it will prevent a third party from exploiting the SSL protocol fallback mechanism (CVE-2014-3566). Note: SSL is supported only for the purpose of web based management and is disabled by default.
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.
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.
19437 Corrected a reset issue with support of the LLDP POE tx-tlv which resulted in the message “NIM B5 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”
18789 Corrected an issue that could prevent support of 10GB-SR-SFPP on platforms that support 10G SFPPs.
19287 Corrected a reset issue associated with accessing the ctChasFanModuleState MIB object.
19288 Corrected an issue that prevented do1x authentication of Cisco Voice Gateways.
19377 Corrected an issue that prevented the disabling of an admin login account from being persistent.
19311 Corrected an issue that could prevent host transmission of a gratuitous ARP on master unit failover.
18907 Corrected an issue with support of the NetSight Inventory Manager "Configuration Template”.
19305 Addressed a delay in transmitting LLDP Network Policy on ports that are authenticating. It had been observed that Polycom IP phones using LLDP may timeout on booting.
19330 Corrected reset issue that resulted in the message “broad_cpu_intf.(2992): Error code 0x00000FFF”
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)”.
19366 Corrected an issue where the output of “show lldp port remote-info” was missing remote-info POE Device-Type information.
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.

Changes and Enhancements in 6.81.02.0007
Modified Spanning Tree loop protect behavior to disable a protected port when in a state where multiple BPDU sources have been detected.
18787 Corrected a potential reset condition in the “dot1s_timer_task” task, which produced the log entry, “Last switch reset was caused by sal.c(1184): Error code 0x00000000”.
19196 Addressed an issue which allowed corrupted DHCP packets, to be looped back on dhcpsnooping trusted ports.
19163 Corrected a potential reset condition in the “ipMapForwardingTask” task, which produced the log entry, “sal.c(1184): Error code 0x00000000”.
The B5 no longer logs the informational message "License file not present" when no license file is found on boot.
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”.
19249 Modified the logging behavior of SNTP to prevent excessive changed system time messages, “sntp_client.c(2109) 62 %% SNTP has changed system time”.
18499 Corrected an issue that prevented identification of Avago MGBIC-LC04s.
18919 Corrected a potential exception condition with the resulting log message “Last switch reset caused by Fault(0x00000300)”.
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.
18907 Corrected an issue that prevented clearing the SNMP community name public using NetSight.
19033 Corrected an issue in TACACS+ command accounting, where the receipt of an unknown TACAC reply packet caused the CLI to become unresponsive.
18931 Syslog messages will now be generated on SNMP user authentication failure.
18864 Corrected an issue with timed resets, where the current configuration would be saved automatically even if the SNMP Persistmode was set to manual.
18861 Added support for the ctAliasEntryClearAll object of the Ctron Alias MIB. Note: This change now requires Netsight Management Software 5.1/6.1 or higher to read the Alias table.
18490 Corrected an issue where Loop Protect could erroneously lock a link aggregation.
19257 Corrected an issue with Policy CoS rate limiter implementation that could cause loss of Spanning Tree BPDUs.
19158 Corrected an issue that resulted in erroneous LLDP traps. lldpStatsRemTablesInserts + Wrong Type (should be gauge 32 or Unassigned32) xxx lldpStatsRemTablesDelets + Wrong Type (should be gauge 32 or Unassigned32)xxx lldpStatsRemTablesDrops + Wrong Type (should be gauge 32 or Unassigned32)xxx lldpStatsRemTableAgeOuts + Wrong Type (should be gauge 32 or Unassigned32)xxx

Changes and Enhancements in 6.81.01.0026
19793 Ported Common Vulnerabilities and Exposures (CVE) patches to SSH to address: CVE-2006-4925, CVE-2008-1657, and CVE-2012-0814. Note: Vulnerability scan tool that report vulnerabilities based on SSH version may still report these as issues.

Changes and Enhancements in 6.71.04.0004
18948 Corrected an issue that prevented support of 10GB-ZR-SFPP transceivers.
18891 The output of the CLI command "show spantree stats active", will now display the role of lag member physical ports as "disabled". Previously their role was displayed as "designated".
18691 Corrected an issue in the implementation of the Enterasys Resource Utilization MIB, where setting etsysResource1minThreshold to zero, did not prevent etsysResourceLoad1minThresholdExceeded notifications.
18747 Corrected an issue with support for MGBIC-LC04 transceivers which could cause failure to link on boot up.
18761 Corrected an issue where etsysMACLockingMACViolation traps could erroneously be generated
18789 Corrected an issue where an errant log message "Unsupported pluggable module detected", is generated for an 10GB-SR-SFPP transceiver.

Changes and Enhancements in 6.71.03.0025
18771 Corrected an issue where an 802.1x supplicant client's packet are leaked to the network during the authentication process.
16073 Adjusted the priority of packets destined to IPv4 primary and loopback interface addresses, to increase the ability to maintain management, when there is large volumes for traffic trapped to the host CPU.
17978 Allow local login authentication, when TACACS+ management authentication is configured and the TACACS+ server is offline.
18421 Corrected an issue where 802.1x supplicant EAP packets where flooded to other ports.
16911 Corrected an issue where the "show logging default" command, displays the incorrect severity values.
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"
18468 Modified the IP helper application to allow forwarding of packets with a TTL=1. This previously prevented one IP Phone vendor's bootp requests from being forwarded.
18569 Corrected an issue with the interaction of MAC Locking and 802.1x, which could prevent client network access.
18383 Addressed a 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.

Changes and Enhancements in 6.71.03.0025
18421 Corrected an issue where the Policy application allowed 802.1x supplicant EAP packets to be leaked to other ports.

Changes and Enhancements in 6.71.02.0008
18589 Corrected an issue where a switch exposed to VRRP traffic, may respond to an ARP request for its own host IP address, with the MAC address of the VRRP Virtual IP address. This issue was first introduced in release 6.71.01.0067 and may result in network connectivity problems.

Changes and Enhancements in 6.71.02.0007
Support Automated Deployment – This feature allows a newly installed device with no configuration (default configuration), to obtain the latest firmware revision and/or configuration automatically from the network.

Changes and Enhancements in 6.71.01.0067
17239 Corrected issue where the etsysMultiAuthSessionAuthAttemptTime MIB object was not updated each time a session attempted re-authentication.
17419 Corrected an issue where changing a port mirror destination port, to a port on a different unit, could cause the mirror to fail.

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.
17175 Corrected an issue where “clear port advertise <port-string> pause” would disable a 10Gb (tg) port.
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.

Changes and Enhancements in 6.61.08.0013
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.
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 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.
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.
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)”.
17256 Addressed a reset associated with issuing the “clear snmp community” command when the switch security mode was set to c2.
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 while device ports were coming 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.
15894 Addressed a routing issue which prevented IPv6 clients from pinging their default gateway when the associated route prefix exceeded 64 bits.
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.
16182 The user defined port speed and autonegotiation settings are now persistent for SFP combo ports across resets. Previously custom settings could revert back to defaults after a reboot.
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.
16521 Addressed an issue with Syslog message format by removing extra spaces between timestamp and host’s IP address.

Changes and Enhancements in 6.61.06.0009
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.
16958 Addressed an issue with the TCP MIB in which a continuous GetNext on the tcpListenerProcess OID would loop.

Changes and Enhancements in 6.61.03.0004
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.
14077 & 16236 Addressed an issue which resulted in high CPU utilization when the switch received Kiss-o'-death packets from an SNTP server.
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.
15007 Corrected a port MAC layer communication issue that resulted in the logging of a "bcm_port_update failed: Operation failed" message.
15297 Addressed an issue associated with the switch port state machine which could potentially cause device ports to lockup.
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.
15752 Addressed an issue introduced in firmware 6.42.07, in which the switch failed to detect Pre-IEEE Standard POE phones on ports 12 and higher.
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.
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.
15974 Resolved a buffer allocation issue which could cause the switch to stop generating console and syslog messages.
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.
16039 Addressed an issue whereby sFlow datagrams were transmitted with invalid packet type when selectable management was configured.
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.

Changes and Enhancements in 6.61.02.0007
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".
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.
16135 Addressed a buffer management issue which limited the number of LLDP-MED endpoint connections to the switch. Previously only 6 connections were allowed.
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.
16156 & 16760 Addressed an issue where a stack could fail to reform after the management unit was powered off.
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.
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".
16447 Addressed an issue where the user defined MDI/MDIX port setting was reversed after moving the management unit.
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 6.51.02.0018
6672 The "clear spantree adminpathcost" CLI command now works when using wildcards for the port-string option field.
13100 Resolved an issue whereby executing the "show config outfile" command followed by "show support" could cause a device reset.
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.
14038 A Syslog message is now generated when the manager switch is removed from the stack. Previously only a CLI message was reported.

Changes and Enhancements in 6.51.02.0018
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.
14582 Corrected a formatting issue associated with the "show dhcpsnooping port" command output display.
14639 The "movemanagement" command is now supported over SSH sessions.
14716/15019/15350/15357 Addressed a DHCP snooping issue whereby DHCP packets originated from LAG ports to the CPU egressed back to the source causing a data loop and high CPU utilization.
14776 Corrected an issue whereby read-write and read-only SSH users were unable to log back onto the switch once locked out.
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.
14817 Resolved an issue whereby SNMPv3 inform requests were not sent when the device was in router mode.
14835 & 15361 Addressed an issue with Policy based CoS assignment that mapped traffic internally to the incorrect transmit queue. COS queue 6 and 7 are reserved and are not configurable via the CLI.
14903 Corrected an issue whereby the egress ports on GVRP-generated VLANs were removed after LACP was disabled on the associated LAG port.
14910 Addressed an issue where the “set port advertise” command was removed from the config following an upgrade to firmware 6.42.
14954 & 15182 Corrected an issue whereby MAC addresses that were learned on switched interfaces were not properly added to the ARP table.
14989 Addressed a CLI issue which could potentially cause a reset when the output of the “show config” command exceeded 9K lines.
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.
15013 Addressed a potential TCP vulnerability identified in US-CERT VU#723308.
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 even when the path to the network DHCP server was known.
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.
15452 Corrected an issue which could potentially prevent MAC address notification traps from being generated and cause a CLI lockup.
15114 Resolved an issue in the CPLD status handler task which could result in high CPU utilization when an RPS was detected.

Changes and Enhancements in 6.51.02.0018
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.
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.
15196 Users are no longer required to enable IPv6 administrative mode to configure an IPv6 gateway address for the host interface.
15203 Corrected an issue where Multiple Spanning Tree ID (SID) to filtering database ID (FID) mappings were not persistent across a reset if CoS was enabled. This error may have resulted in loss of network connectivity.
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 config correctly.
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.
15308 Resolved an issue associated with RSTP when automatic edge port detection was disabled and adminedge was set to false on an active port. This issue could cause the alternate port to stop forwarding traffic after failing over and becoming the root port.
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.
15346 & 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.").
15347 Addressed a POE power management issue that resulted in ports not supplying POE power even when power was available.
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.
15384 Corrected an issue which resulted in erroneous syslog messages similar to “radius_txrx.c(395) 1006 % RADIUS: Failed to send the request “when users logged in with proper credentials.
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.
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 6.51.02.0018
15841 Addressed an issue where the user defined MDI/MDIX mode was reversed when issuing the "Set port mdix" command.
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 6.42.03.0004
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.
14592 Resolved as issue whereby the 1000BASE-SX ports remained operationally active after being disabled via the CLI.
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 the 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.
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
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.

Changes and Enhancements in 6.42.01.0046
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.
13850 The “set cdp state” command failed with the following error “Invalid range specified”, when issued for a range of 10-Gigabit ports. This has been resolved.
13851 The “set length” command is now persistent after a reset.
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.
13941 The daylight savings time function (Summer Time) now works properly when SNTP is enabled.
13943/14091/14096/14186/14199/14223 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" or "Fault(0x00001100) SRR0(0x00074ce8) SRR1(0x4002b030) MSR(0x00001030) DMISS(0x9990693a) IMISS(0x00000000)".
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.
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.

Changes and Enhancements in 6.42.01.0046
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.
14463 The fan controller speed will now switch to high when temperature rises above the high temperature trip point threshold value.
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.
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 6.41.06.0002
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.
14265 Resolved a slow memory leak associated with the licensing task.
14295 Resolved an issue with firmware 6.41.03.0018 and above which prevented SNMP access when the management IP address was in the 172.16.0.0/16 network address range.

Changes and Enhancements in 6.41.05.0001
This is a release to manufacturing only firmware for the B5 platform.

Changes and Enhancements in 6.41.04.0003
14105 & 14117 MGBIC-LC04 and MGBIC-LC05 are now supported in standalone as well as stacked switches.
14129 Resolved an issue where disabling f pre-6.51low control while the system was under load could cause ports to stop forwarding.
14166 Resolved an issue where the client authentication packets were being forwarded out the device ports after being processed.

KNOWN RESTRICTIONS AND LIMITATIONS:

Known Issues in 6.81.07.0004
There are no new known restrictions or limitations associated with this release.

Known Issues From Previous Releases
WARNING: Configuration files containing a login banner may suspend operation of images prior to 6.51. 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-6.51 images.
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.
Switching
COS / TOS
13257 When the B5 is configured for "User + Phone" authentication, the phone's VLAN-tag to role mapping will be counted as a user against the number of multiauth users allowed per-port.
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 switch 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
6.51 images will not stack with earlier versions of code, due to the use of VLAN 4094. When adding a new unit to an existing stack running 6.51 or higher, the unit will need to be running 6.51 or higher. When adding a new unit to an existing stack running a pre-6.51 image, the new unit will need to be downgraded to a pre-6.51 image.
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.
POE
15780 When attached to other switches capable of being power sourcing equipment (PSE). The switch may continuously cycle POE detection status, resulting in pethPsePortDetectionStatus traps. This may be avoided by disabling inlinepower on the inter-switch links.
Policy / Authentication
Policy IPv6 Router Advertisements drop rules (ICMPv6 type = 134) require special handling. When this rule type is applied to a user, it will be applied to all users on the same port. It will also result in all ICMPv6 traffic being soft forwared on the given port.
Setting the security profile to c2 changes certain system defaults, including encryption algorithms used for storing passwords, shared secrets, and routing keys. As a result, configuration files for devices operating in different security profiles are not fully compatible and may result in some loss of configuration if loaded.
13770 When running multiple authentication mechanisms dot1x and macauth, do1x should have higher precedence. If the order is reversed, dot1x authenticated traffic is diverted to the host until macauth is performed.

Known Issues From Previous Releases
13998 When setting the multiauth mode from multi to strict, some previously authenticated users may be unable to re-authenticate. The work around is to disable PWA and MAC Authentication prior to switching modes.
TACACS+ using single connect is configurable through the CLI but it is not supported in this release.
The B5 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.
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 249 rules can be supported per policy profile.
2175 ARP packets are not classified based on policy IP source/destination rules.
MAC Locking
Static MAC locking a user on multiple ports is not supported.
A violating MAC lock user can authenticate on the port using dot1x, but all other traffic from that user will be dropped.
Statically MAC locked 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 use the same IP address.
MAC Authentication
10893 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
13849 When PWA enhanced mode is enabled and a user authenticates with a lower precedence method, that user’s port 80 traffic will continue to be intercepted, until PWA authenticates the user. The work around to this is to insure PWA has a lesser precedence.
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 (for example, Spanning Tree).
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.

Known Issues From Previous Releases
Routing
The B5 is not capable of routing unicast IPv4 addresses that resolve to multicast MAC address. This is used in some clustering applications.
You cannot overwrite the IP address of a configured interface if the new IP address is in the same subnet as the original. You must first delete the existing interface IP address and then add the new IP address.
The B5 will not add a host route to its routing table for a subnet it already knows about.
The B5 does not support configuring 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 B5 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 cannot be used simultaneously with Policy.
IPv6
Enabling IPv6 and MAC ACLs with the "access-list ipv6mode" will reduce the total number of standard ACL rules currently supported. It will also prevent the use of Policy.
14036 When using IPv6 management, the movement of the master as the result of a "set switch movemanagement" commands or a reset, can result in the loss of the host address. This can result in the loss of remote management. This can only be recovered by reloading the configuration.
Servers for PWA cannot be configured with an IPv6 address.
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
Extreme Stacking MIB: 1) extremeStackMemberStackPriority as defined by the MIB has a valid range 1-15. The B5 will default to 16. 2) extremeStackMemberCurConfig is not supported. 3) extremeStackingPortIfIndex ranges from 1-16. Odd numbered indexes are stack UP ports and even number indexes are stack DOWN ports. Each stack unit has two indexes which are assigned sequentially based on unit number (i.e. extremeStackingPortIfIndex 1 = unit 1 UP, 2 = unit 1 DOWN, 3 = unit 2 UP, 4 = unit 2 DOWN …). 4) extremeStackingPortRemoteMac is not supported
The switch can support up to two concurrent SSH client sessions.
9328 If the host IP address or the router IP interface used for management is in a zero subnet (for example, 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.
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 You cannot set port advertise speeds of 10t, 10tfd, 100tx, and 100txfd on combo ports.

Known Issues From Previous Releases
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.
13709 Auto-negotiation is required for MGBIC-LC01 link.
13972 Link Traps will only be sent to a maximum of three SNMPv3 notification targets.
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 through 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 counters may display differing values.
Packets greater than 1518 will not be counted by the IfInErrors MIB.
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. o The captured frames will be as close to sequential as the hardware will allow. o Only one interface can be configured for capturing at a time. o Once 100 frames have been captured by the hardware the application will stop without manual intervention. • 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: o MaxOctetsRequested can only be set to the value -1 which indicates the application will capture as many packets as possible given its restrictions. o CaptureSliceSize can only be set to 1518. o 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. o 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.

Known Issues From Previous Releases
sFlow
14061 sFlow can create varying degrees of CPU utilization depending on the number of samplers, sampling rate, pollers, and sampling interval. High CPU utilization can be mitigated by reducing samplers and pollers, or increasing sampling rate and interval. Since traffic is switched in hardware, CPU utilization should not affect switch performance. However, it may slow management response.
12004 sFlow does not sample with frame rates < 1024fps.
SFPP
The follow SFPPs (while functional), will identify their transceiver types incorrectly: 10GB-ZR-SFPP ZR is reported as an ER 10GB-USR-SFPP USR is reported as an SR. 10GB-BX10 BX10 is reported as an LR 10GB-BX40 BX40 is reported as an ER

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

For the latest copy of this release note, go to www.extremenetworks.com/support/contact/.

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 5519	MGMD-STD-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 4113	UDP MIB

RFC No.	Title
RFC 4022	TCP 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

EXTREME NETWORKS 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
etsysletfBridgeMibExtMIB
etsysMultiAuthMIB
etsysSntpClientMIB
etsysIeee8023LagMibExtMIB
etsysVlanAuthorizationMIB
etsysCosMIB
etsysResourceUtilizationMIB
etsysMultiUser8021xMIB
etsysTacacsClientMIB
etsysSpanningTreeDiagnosticMIB
extremeStackable

Enterasys Networks Private Enterprise MIBs are available in ASN.1 format from the Enterasys Networks 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

Traps	Description
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
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@enterasys.com

By Web: **www.extremenetworks.com/support/contact/**

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.