6480 Via Del Oro
San Jose, CA 95119
+1 888-257-3000

Customer Release Notes

I-Series

Firmware Version 6.61.18.0001
July 2016

INTRODUCTION:

This document provides specific information for version 6.61.18.0001 of firmware for the following I-Series products:

I3H252-12TX	I3H252-4FXM	I3H252-8FXM	I3H252-02
I3H252-4FX-MEM	I3H252-6TX-MEM	I3H252-8TX-2FX	I3H-4FXM-MEM
I3H252-24TX	I3H252-16FXM	I3H252-8FXM-12TX	I3H-4FX-MM
I3H-6TX-MEM	I3H-8TX-2FX	I3H-MEM	I3H-8FX-MM

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	6.61.18.0001	Maintenance Release	July 2017
Previous 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
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	6.42.01.0046	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	1.02.03.0010	Maintenance Release	January 2009
Previous Version	1.02.02.0009	Maintenance Release	November 2008
Previous Version	1.02.00.0043	Feature Release	October 2008
Previous Version	1.00.03.0002	Maintenance Release	July 2008
Previous Version	1.00.02.0001	Maintenance Release	May 2008
Previous Version	1.00.01.0058	Maintenance Release	May 2008
Previous Version	1.00.00.0054	Initial Release	March 2008

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
I-MGBIC-GLX	I-Series Only, -40°C to +60°C, 1 Gb, 1000BASE-LX, MM - 550 m, SM - 10 km, 1310 nm Long Wave Length, LC SFP.
I-MGBIC-GSX	I-Series Only, -40°C to +60°C, 1 Gb, 1000BASE-SX, IEEE 802.3 MM, 850 nm Short Wave Length, 220/550 m, LC SFP.
I-MGBIC-GTX	I-Series Only, -40°C to +60°C, 1 Gb, 1000BASE-T, IEEE 802.3 Cat5, Copper Twisted Pair, 100 m, RJ 45 SFP.
I-MGBIC-GZX	I-Series Only, -40°C to +60°C, 1 Gb, 1000BASE-LX/LH, IEEE 802.3 SM, 1550 nm Long Wave Length, 80 km, LC SFP.
I-MGBIC-LC03	I-Series Only, -40°C to +60°C, 1 Gb, 1000BASE-LX, MM, 1310 nm, 2 km with 62.5 MMF, 1 km with 50 MMF, 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-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-BX40-U	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-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)

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.
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).
Increased Password Security – Supports new password options including: complexity, history, 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.
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.
VLAN 4094 – VLAN 4094 is no longer reserved.

Existing Product Features	
802.1D	Auto Negotiation
802.1Q – VLAN Tagging	Primary and Secondary Relays for activating external alarms
802.1p – Traffic Management / Mapping to 6 queues	8K MAC Address Table
802.3x Flow Control	Selectable MAC hashing algorithms
802.3ad – Dynamic and Static Creation for Link Aggregation	MGBIC support: I-MGBIC-GLX and I-MGBIC-GSX – industrial MGBICs to maintain -40 to +60 degrees C operation
802.1s – Multiple Spanning Tree Protocol (up to 4 instances)	8 Priority Queues Per port
802.1w – Rapid Spanning Tree	Web Redirect – PWA+ and URL redirection
Spanning Tree Backup Root	Session-Timeout and Termination-Action RADIUS Attributes Support
Legacy path cost	Ability to set port advertise ability via CLI
Spanning Tree Pass Thru	Multi-Method Authentication
Span Guard	Alias Port Naming
Link Flap Detection	DHCP Server
Per Port Broadcast Suppression	Web Authentication (PWA)
Port Mirroring (Single instance)	Queuing Control Strict & Weighted Round Robin
Node/Alias Table	802.1X Authentication
Private Port (Private VLAN)	Non Strict 802.1X default RFC 3580 With Auth Failure
Cabletron Discovery Protocol (CDP)	RADIUS Client
Cisco Discovery Protocol v1/2	Turn off RADIUS Authentication (RADIUS Realm)
GVRP	Ability to set time and date via the MIB
IGMP v1/v2/v3 and IGMP Snooping	MAC Authentication / MAC Authentication Masking
Setting static multicast MAC address	MAC Authentication retained after age out
Syslog	RADIUS Accounting for MAC Authentication
Text-based Configuration Upload/Download	EAP pass-through
CLI Management	Dynamic and Static MAC Locking
Telnet Support	New Mac trap
IPv4/IPv6 Dual Host Management Support (SNMP, Telnet, SFTP, SCP, SSH, RADIUS)	Dynamic Egress
Discard VLAN Tagged Frames	SSHv2 Support
Policy – Single User	WebView
Priority Classification L2-L4	SSL Interface to WebView
VLAN Classification	RMON (4 groups)

ToS Rewrite	RMON View in the CLI With Persistent Sets
Dynamic VLAN Assignment (RFC 3580)	RMON Packet Capture/Filtering Sampling
Configurable Login Banner	SNMPv1, SNMPv2c, SNMPv3
COS Inbound Rate limiting	Simple Network Time Protocol (SNTP)
AES-128 support with SNMPv3	VLAN-to-Policy Mapping
Dynamic ARP inspection	Non-Strict 802.1X VLAN authentication
Flood Control	Protected Port
CPU/Memory utilization monitoring via MIB	Secure Copy / Secure FTP
DHCP Snooping	Serviceability enhancements
Display 802.3 pause counters	SMON MIB support for Port Mirroring
Dynamic VLAN assignment based on PWA	Spanning Tree Loop Protect
Host Protect	TACACS+
Hybrid Policy Mode	Tx Queue Monitoring
LLDP-MED Network-Policy TLV	VLAN marking of mirrored traffic
Multiple RFC3580 Users	

INSTALLATION AND CONFIGURATION NOTES:

Warning:

- 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.
- Direct firmware upgrades to 6.61 from 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.

Note:
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** <*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.

Note:
If VLAN 4094 is provisioned in firmware 6.61, it must be removed prior to back-revving 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

The I3 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 I-Series and follow the TFTP download instructions that are included in your *I-Series CLI Reference* guide and the *Fixed Switch Configuration Guide*.

Soft copies of the *I-Series CLI Reference* guide and the *Fixed Switch Configuration Guide* are available at no cost on the Extreme Networks documentation site, http://documentation.extremenetworks.com.

POLICY CAPACITIES

Maximum supported roles per system	15
Maximum number of rules per role	100
Maximum number of unique rules per system	128 unique L2 rules and 128 unique L3/L4 rules (rules may be shared across roles)

FIRMWARE CHANGES AND ENHANCEMENTS:

Changes and Enhancements in 6.61.18.0001
19704 Corrected an issue with saving the configuration after a NAC enforce
19718 Corrected an issue in CiscoDP where an IP phone does not get authenticated.
19707 Add chkdsk(check Disk) output to show support for debug
19685 Corrected an issue in Cisco Discover Protocol support where VMware ESXi devices are not shown as neighbors.
19693 Modified the routing command “show interface” to have rtr.0.x in output instead of repeating VLAN xxx and modified linkup/linkdown syslog to have ifName instead of unit/slot/port.
19689 Corrected a reset issue in the tEmWeb Task that resulted in the message “tEmWeb(0xa1da038) Fault(0x00000300) SRR0(0x013C0354) SRR1(0x0000B032)”.

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.

Changes and Enhancements in 6.61.15.0003
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.
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.
19534 Corrected an SNMP issue within the ctChasPowerTable where power supply redundancy may be incorrectly returned.
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”
19318 Corrected an issue where the “set length” command was not persistent.
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.
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.
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.

Changes and Enhancements in 6.61.13.0006
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.
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 CVEs.
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.

Changes and Enhancements in 6.61.12.0005
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 authentication failure.

Changes and Enhancements in 6.61.11.0006
18749 Corrected an issue in Policy where attempting to configure an unsupported rule type caused continuous rebooting.
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
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 daylight 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.

Changes and Enhancements in 6.61.09.0012
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” state, with multiauth mode set to strict, and maclocking firstarrival set to 1.
18231 Resolved an issue with RFC-3580 VLAN Authorization where the VLAN returned by RADIUS failed to be applied to the user if MultiAuth mode was set to "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 issue that 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
17440 Corrected an issue that prevented the use of memory cards.
16442 Corrected an issue with DHCP relay agent that could have 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 6.03.xx
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 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.

Changes and Enhancements in 6.61.08.0013
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 an issue with calculating policy profile use counts. Previously 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 showed an 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 cause memory exhaustion and result 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

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 approx. 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)”.
17215 Addressed a platform related issue which prevented the switch to generate syslog entry and SNMP trap messages for temperature changes.
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.

Changes and Enhancements in 6.61.07.0010
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.
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.
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.
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.

Changes and Enhancements in 6.61.06.0009
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 SNMPTask 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 pressed. This has been addressed.

Changes and Enhancements in 6.61.05.0009
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.
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
13946 Addressed an issue which prevented GVRP from automatically propagating VLANs assigned to ports via VLAN authentication.
15007 Corrected a port MAC layer communication issue that resulted in the logging of a "bcm_port_update failed: Operation failed" message.
15974 Resolved a buffer allocation issue which could cause the switch to stop generating console and syslog messages.

Changes and Enhancements in 6.61.02.0007
16041 Addressed an issue associated with transmit queue monitoring whereby an oversubscribed front-panel port could potentially cause spanning tree topology change and re-convergence when flow control was enabled.
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.
16815 Resolved a multiauth issue which prevented a user to authenticate via multiple authentication methods using the same VLAN assignment.

Changes and Enhancements in 6.42.11.0006
14077 & 16236 Addressed an issue which resulted in high CPU utilization when the switch received kiss-of-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.
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.

Changes and Enhancements in 6.42.10.0016
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.
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“.

Changes and Enhancements in 6.42.10.0016
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.

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.
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 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.

Changes and Enhancements in 6.42.09.0005
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.

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.
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.

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.

Changes and Enhancements in 6.42.07.0010
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.
14776 Corrected an issue whereby read-write and read-only SSH users were unable to log back onto the switch once locked out.
14903 Corrected an issue whereby the egress ports on GVRP-generated VLANs were removed after LACP was disabled on the associated LAG port.
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.

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.

Changes and Enhancements in 6.42.03.0004
13979 Resolved a Multiauth issue whereby the switch continued to send MAC authentication requests after the supplicant successfully authenticated via 802.1X, this 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.
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.
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.
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
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.
11667 The CLI now prevents users from exceeding the maximum allowed policy profiles. Previously the command succeeded with the following error message “Policy: Hardware error setting profile policy id on Port x”.
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.
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.
12767 The Spanning Tree path cost value for LAG ports is now properly calculated.
12796 Resolved an issue whereby some MGBIC-LC03 LX SFP modules would display as type SX in the "show port status" command output.

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.

Changes and Enhancements in 6.42.01.0046
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".
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.
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.
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.
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!”.
13113 When restoring a saved configuration file, Spanning Tree settings are now loaded in correct order.
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.
13153 Corrected an issue where loss of management could ensue when a Telnet session with an active TFTP transfer is terminated.
13157 The “clear port advertise” command now returns port settings to default values.
13170 SSH client sessions are now consistently terminated after 3 failed attempts.
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.
13224 Resolved an SNMPv3 issue which under rare conditions could cause the CLI to overwrite the ‘set snmp group’ settings.
13261 Resolved an issue with the 'show port egress' command where the egress information for some ports were not displayed.
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.
13298 The NMS Policy Manager now correctly displays the status for LAG ports.
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.
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.
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.
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.

Changes and Enhancements in 6.42.01.0046
13636 The etsysMultiAuthSessionPolicyIndex MIB object (1.3.6.1.4.1.5624.1.2.46.1.4.1.1.7) now returns the correct Policy Profile Index value for the session.
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 persistence after a reset.
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.
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.
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.
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.
14162 The WebView management application copyright date has been updated to 2010.
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.
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.
14629 & 14690 Resolved as issue whereby applying policy to a port with existing policy would block traffic from egressing the port.
14637 The SNMP group CLI commands now persist across device resets.

Changes and Enhancements in 6.42.01.0046
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 01.01.18.0008
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*] Due to hardware limitations, the forced-auto mode is not supported. 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.

Changes and Enhancements in 01.01.18.0006
12907 Corrected a CLI issue whereby executing the “set port negotiation disable” command returned the following error message: “Invalid Slot in [port-string].”

Changes and Enhancements in 01.01.18.0005
With this release the firmware revision numbers will consist of three numeric revision identifiers and a numeric build number (xx.yy.zz.nnnn).
Added support for the following model numbers: I3H252-24TX, I3H252-16FXM, I3H252-8FXM-12TX.
9823 The Bridge MIB object dot1dTpFdbTable (1.3.6.1.2.1.17.4.3) now correctly reports the bridge table contents.

11598 Resolved an issue with the "configure" command whereby previously saved SNMP configurations were not restored correctly.
The processing of packets with network directed broadcast addresses has been corrected to enable support for the SNTP Broadcast mode.
VLAN name assignments are now properly restored when loading a configuration file onto the device.

Changes and Enhancements in 1.01.14
Added support for the following model numbers: I3H252-4FX-MEM, I3H252-6TX-MEM, I3H252-8TX-2FX, I3H-4FXM-MEM, I3H-6TX-MEM, I3H-8TX-2FX, and I3H-MEM.

Changes and Enhancements in 1.00.37
Initial customer release.

KNOWN RESTRICTIONS AND LIMITATIONS:

Known Issues in 6.61.18.0001
There are no new known restrictions or limitations associated with this release.

Known Restrictions in 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.
Access Control Lists (ACLs) use the same hardware resources as Policy rules and should not be used simultaneously with Policy.
Direct firmware upgrades to 6.61 from 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.
15841 The user defined MDI/MDIX mode is reversed when issuing the "Set port mdix" command.
The I-Series supports ethertype policy rules, but does not support DA MAC or SA MAC rules.
The command “clear cos settings <class of service entry number> priority” should only clear the priority value for the class of service entry number specified, but the command will also end up removing the ToS-value and irl-reference for the class of service entry specified as well.
Servers PWA cannot be configured with an IPv6 address.
Link Flap Detection cannot be configured on a port that is a member of a link aggregation group.
RFC-3580 VLAN authentication is only supported with 802.1x. It will not function with MAC or PWA authentication.
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.
If policy profile has cos-status enabled, only 99 rules can be supported per policy profile.

When using MAC authentication with authentication optional, there is a potential for the MAC address of users who fail to authenticate to remain unlearned for a period of time.

GVRP frames not forwarded when GVRP is disabled.

Packets less than 64 bytes or greater than 1518 will not be counted by IfInErrors MIB.

All the VLANs learned via GVRP will appear in the GVRP MIBs regardless of there being local users attached to those VLANs or not.

The PWA duration times may increase to values over 60 minutes when executing the “show pwa session” command.

Enabling RMON capture on an interface will cause packets to be duplicated on the interface while the functionality is enabled.

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. 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:
  - 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.

Only RMON offset values of 1-1518 are supported.

The “set port priority” command will not change the 802.1p priority tag on tagged traffic with a default priority tag. The command only has an effect on how untagged traffic will be prioritized as it passes internally through the I-Series switch.

The “set port vlan” command requires that the VLAN(s) specified when executing the command must already be preconfigured statically on the device.

The I-Series switch supports RMON Capture Packet/Filter Sampling through both the CLI and MIBs, but with the following MIB constraints:

- 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 “lock” since the device does not support wrapping the capture buffer.
- The application does not support Events, therefore the following elements of the Channel Entry Table are not supported: TurnOnEventIndex, TurnOffEventIndex, EventIndex, and EventStatus.

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, 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.

If port mirroring is enabled on devices which have spanning tree disabled and spanning tree bpdu-forwarding enabled, the destination mirror port will initially display one additional BPDU packet for each member of the port mirror.

When issuing the command "set macauthentication portreauthentication <port>", the sessions currently existing on the port specified will be reset in addition to having the MACs re-authenticate.

The I-Series supports per port broadcast suppression, and is hardset to be globally enabled. If you would like to disable broadcast suppression, you can get the same result by setting the threshold limit for each port to the maximum number of packets which can be received per second:

Fast Ethernet: 148810

Gigabit: 1488100

The default broadcast suppression threshold for all ports has been set to 14881.

The I-Series device only knows about VLANs which have been created statically or via GVRP. Applications such as policy can only assign ports to VLANs which have been statically created; the device cannot do it with dynamically-created VLANs.

If the singleportlag variable is set to disable and link failures reduce the number of ports which compose a dynamic LAG to one, the member ports will revert back to normal port status.

If MSTP has maps that are associated with GVRP-generated VLANs and GVRP communication is lost, the MSTP maps will be removed from the configuration. It is recommended that users only create MSTP maps on statically-created VLANs.

Only statically created VLANs are supported with Dynamic Egress.

Static MAC locking list MAC address entries in the "show mac" output as "other”, and will not remove them on link down.

A Radius authenticated users session will not timeout on the expiration of the idle timeout.

The command “set macauthentication portinitialize <port-string>” does not remove any currently active sessions.

If a fid is mapped to a sid through WebView, the action is executed. However, if there are any fids currently mapped to the sid they will be removed. Only the most recent mapping will be preserved.

The I-Series will propagate GVRP packets containing any known VLANs. If the user creates a VLAN without adding ports to the egress list, it will begin propagating GVRP packets with that VLAN.
Policy roles and rules cannot be applied to ports that are members of a link aggregation group.
IGMP snooping cannot be controlled via WebView.
The “set mirror vlan” command is not supported in the I-Series.
Web Authentication does not support accounting.
WebView does not timeout after being idle. It is recommended that the user logout when they have finished using WebView.

For the most up-to-date information concerning known issues, see the **GTAC Knowledge** section at https://extremeportal.force.com/. For the latest copy of this release note, go to http://documentation.extremenetworks.com.

To report an issue not listed in this document or in GTAC Knowledge, contact Technical Support.

IETF STANDARDS MIB SUPPORT:

RFC No.	Title
RFC 1213	MIBII
RFC 1493	Bridge MIB
RFC 2819	RMON MIB
RFC 2668	MAU-MIB
RFC 2233	ifMIB
RFC 2863	ifMIB
RFC 2620	RADIUS Accounting MIB
RFC 2618	RADIUS Authentication 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 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 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
RFC 1213	ColdStart Link Up Link Down Authentication Failure
RFC 1493	New Root Topology Change
RFC 1757	RisingAlarm FallingAlarm

PRIVATE ENTERPRISE MIB SUPPORT:

Title
ctenviron-mib
ctbroadcast mib
ctRatePolicing mib
ctQBridgeMIBExt mib
ctCDP mib
ctAliasMib
ctTxQArb mib
ctDownLoad mib
etsysRadiusAuthClientMIB
etsysRadiusAuthClientEncryptMIB
etsysPolicyProfileMIB
etsysPwaMIB
etsysSyslogClientMIB
etsysConfigurationManagementMIB
etsysMACLockingMIB
etsysSnmpPersistenceMIB
etsysMstpMIB
etsysMACAuthenticationMIB
etsysletfBridgeMibExtMIB
etsysMultiAuthMIB
etsysSntpClientMIB
etsysIeee8023LagMibExtMIB
etsysVlanAuthorizationMIB
etsysCosMIB

etsysSpanningTreeDiagnosticMIB

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

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: +1 800-998-2408 (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.
6480 Via Del Oro
San Jose, CA 95119

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