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

Customer Release Notes

A-Series A4

Firmware Version 6.61.18.0001
December 2017

INTRODUCTION

This document provides specific information for version 6.61.18.0001 of firmware for the A-Series A4 products:

A4H124-24FX	A4H254-8F8T	A4H124-24	A4H124-24P
A4H124-48	A4H124-48P		

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	December 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	3.03.02.0002	Maintenance Release	September 2011
Previous Version	3.03.01.0011	Feature Release	June 2011
Previous Version	3.02.02.0002	Maintenance Release	February 2011

BOOTPROM COMPATIBILITY

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

NETWORK MANAGEMENT SOFTWARE SUPPORT

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

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

PLUGGABLE PORTS SUPPORTED:

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

PRODUCT FEATURES

New Product Features in 6.61	
Enterasys Policy Single user or User + IP Phone	Basic IPv4 Routing (static, RIP v1/v2)
LLDP-MED Network-Policy TLV	Security Log
VLAN 4094 – VLAN 4094 is no longer reserved for stacking.	Console Disconnect – Support added for Console disconnect through the use of VT100 terminal emulation.
Serviceability enhancements – System dump files `show support` command Remote debug commands (over telnet)	Mixed Strict and WRR Port Transmit Queue settings
TACACS+ management	Service Access Control Lists (SACL)
IPv4/IPv6 Dual Host Management Support (SNMP,Telnet,SFTP,SCP,SSH,RADIUS)	Enterasys Spanning Tree Diagnostic MIB
Cable Status	Flexible Link Aggregation Groups
Secure Copy / Secure FTP (SCP/SFTP)	AES-128 support for SNMPv3
CoS MIB based Flood Control (broadcast, multicast, and unknown unicast)	Display 802.3 pause counters
Increased Password Security – • Complexity • History, Aging • FIPS 1402 approved encryption algorithm	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.
Secure directory	Tx Queue Monitoring
DHCP Spoof Protection	OpenSSL FIPS Object Cryptographic Module
ARP Spoof Protection	IPsec for RADIUS transactions
Command Logging	SNTP Server-Client Authentication
RFC-3580 dynamic VLAN assignment based on PWA	Web Authentication (PWA)
Web Redirect – PWA+ and URL redirection	MAC Locking clearonlinkchange
MSTP Multisource Detection	MAC Locking Threshold Notification
Time Based Reset	Login Banner

Existing Product Features	
1 Gbps Full Duplex Stacking (2 Gbps bi-directional) Stacking Interconnect	MGBIC support: MGBIC-LC01, MGBIC-LC03, MGBIC-LC07, MGBIC-LC09, MGBIC-02, MGBIC-08, MGBIC-MT01
8 Priority Queues Per port	MAC Address Table – 16K/A4
Weighted Round Robin Queuing	RFC 3580 VLAN authorization using MAC authentication
802.3x Flow Control	Jumbo Frame (up to 9K)

Existing Product Features	
Per Port Broadcast Suppression	Auto-negotiation
Inbound Rate Limiting	Ability to configure mdi/mdix port settings via CLI
802.3ad – Dynamic and Static Link Aggregation	802.1p Mapping to 6 queues
802.1s – Multiple Spanning Tree Protocol (up to 4 instances)	Queuing Control Strict & WRR
802.1w – Rapid Spanning Tree	Ability to set port advertise ability via CLI
Spanning Tree Backup Root	Port Mirroring (up to 8 ports anywhere in the stack)
Legacy Path Cost	DHCP Server
Link Flap Detection	Layer 2 ACLs
Spanning Tree SpanGuard	802.1X Authentication
Spanning Tree Loop Protect	Non Strict 802.1X default RFC 3580 with Auth Failure
802.1p – Traffic Management	Dynamic and Static MAC Locking
802.1Q – VLAN tagging and identification	Cabletron Discovery Protocol (CDP)
802.1D	RADIUS Client
Packets can be dropped, shaped, marked (with an IP DSCP or IP precedence value), or sent unchanged to the switching process.	Session-Timeout and Termination-Action RADIUS Attributes Support
CDP Support	Turn off RADIUS Authentication (RADIUS Realm)
CiscoDP with MIB Support	MAC Authentication / MAC Auth Masking
Cisco Phone Discovery	MAC Authentication retained after ageout
GVRP	RADIUS Accounting for MAC Authentication
IGMP v1/v2/v3 and IGMP Snooping (up to 256 multicast groups)	EAP Pass Thru
Syslog	New MAC Trap
SSHv2 Support	CLI Management
Private (Protected) Port (Private VLAN)	Telnet Support
Dynamic VLAN Assignment (RFC 3580)	WebView
Dynamic Egress	SSL Interface to WebView
Discard VLAN Tagged Frames	RMON (4 groups)
Node/Alias Table	RMON View in the CLI
SNMPv1, SNMPv2c, SNMPv3	RMON Packet Capture/Filtering Sampling
Text-based Configuration Upload/Download	RMON View in CLI with Persistent Sets
Alias Port Naming	Simple Network Time Protocol
Configurable Login Banner	

INSTALLATION AND CONFIGURATION NOTES

Warning:

- Direct firmware upgrades to 6.61.05 (and above) from 3.02 (and earlier) images may leave the switch in an unrecoverable state. It is **required** to upgrade to 3.03 prior to loading 6.61.05.
- Version 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 three 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.
- An SNMPv3 configuration file created in a release 3.03 will fail when loading into a switch running 6.61. Workaround: after a switch has been upgraded to 6.61, a previously created SNMPv3 configuration file MUST be re-generated (saved) using 6.61 code in order for SNMPv3 to function correctly.

Note:

- Stacks running images prior to 6.61.02 may be upgraded to 6.61 (or later); however, a stack running 6.61 (or later) will not detect a switch added to the stack if it is running any code prior to 6.61.02. Any switch added to a 6.61 (or later) stack must be individually upgraded to 6.61.02 (at a minimum), prior to attempting to add the switch to the stack.
- 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 6.61.02 to a previous firmware version.
- Significant differences in feature set exist between 6.61 and previous images. This includes the replacement of the Diffserv application with Enterasys Policy. As a result some configuration may be lost on upgrade to 6.61.02 (or later), from previous images.

The A-Series switch 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 the product pages at https://extremeportal.force.com/ for the latest firmware updates to the A-Series A4 and follow the TFTP download instructions that are included in your *A4 CLI Reference* and the *Fixed Switch Configuration Guide*.

Soft copies of the *A4 CLI Reference* and the *Fixed Switch Configuration Guide* are available at no cost to the user on the Extreme Networks documentation site, http://documentation.extremenetworks.com.

The A-Series family of stackable switches is managed by a single IP address for a stack of up to eight switches. To download the new firmware to a stack of A4 switches, simply follow the instructions to upgrade a switch with new firmware and then the system will automatically download the new firmware to all the members in the stack controlled by that stack manager.

POLICY CAPACITIES

Maximum Policy roles (profiles) per system	15
Maximum number of users per port	2 (PC + Phone)
Maximum number of unique rules per system	100
Maximum number of unique masks per system	17
Maximum number of unique masks per profile	9

* 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 (PC + Phone).

*** When in multi-user mode ("PC + Phone"), the combined user and phone profiles may not exceed nine unique masks.

**** .An IRL is considered a unique rule and uses a unique mask.

ROUTER CAPACITIES

Feature	Capacity
ARP Dynamic	2024
ARP Static	512
Route Table	64
Static Routes	64
RIP Routes	2500
IP Interfaces	24
Secondary IP addresses per Interface	31
IP Helper Address	6 Per Interface
Access Rules (inbound only)	100
Access Rules – Per ACL	20 per ACL, 20 per interface
IGMP Groups	256

FIRMWARE CHANGES AND ENHANCEMENTS

Changes and Enhancements in 6.61.18.0001
19704 Corrected an issue with saving the configuration after a NAC enforce.
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".

Changes and Enhancements in 6.61.16.0002
19652 Corrected an issue with processing LLDP packets that could result in a reset with the message “ Last switch reset was caused by buff.c(546):”
19643 Corrected a reset condition resulting in the message “dot1s_task(0xac24038) + broad_l3_mcast.(2766):Error 0xFFFFFFFC”.
19320 Corrected an issue where the SNTP server table is restored in reverse order from entry Configuration.

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

Changes and Enhancements in 6.61.14.0006
19241 Corrected an issue where erroneous POE traps "etsysPseChassisPowerNonRedundant" and "etsysPseChassisPowerRedundant" were transmitted.
19318 Corrected an issue where the `set length` command was not persistent.
19366 Corrected an issue where the output of "show lldp port remote-info" was missing remote-info POE Device-Type information.
19372 Added support for the ability to separately configure RADIUS and RADIUS accounting parameters.
19282 Corrected an issue that could cause the CLI to lock.
19437 Corrected a reset issue concerning the LLDP POE tx-tlv option which resulted in the message "NIM A4 reset 0x0000BADD caused by nim_t :Task ID:0x0a6dcd20".
19434 Corrected a reset issue which resulted in the message "Nim_T reset due to TASK 0x0a758ec0".
19383 Corrected a potential method of corrupting the startup configuration file. This may previously have resulted in the continuous rebooting of the system on power up.

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

Changes and Enhancements in 6.61.13.0006
16086 Attempt to recover from a L2 table DMA error that previously resulted in a reset with a log entry of: “soc_l2x_thread DMA failed too many times”. On an L2 Table DMA failure we will now walk the table to find the corrupted entry and remove it. The expected warning message is: “warning soc_l2x_thread: Bad L2 table entry found. Recovering”.
19163 Corrected a potential reset condition in the “ipMapForwardingTask” task, which produced the log entry, “sal.c(1184): Error code 0x00000000”.

Changes and Enhancements in 6.61.12.0005
19033 Corrected an issue in TACACS command accounting, where the receipt of an unknown TACAC reply packet caused the CLI to become unresponsive.
19076 Modified the SNTP protocol to insure that the UDP source port will not be equal to the UDP destination port.
18793 Patched updates to SSH to address the following Common Vulnerabilities and Exposures (CVEs): CVE-2006-4925, CVE-2012-0814, and CVE-2008-1657. Note: Scan tools that report potential vulnerabilities based on SSH version may still report these.
18455 Addressed an issue in the SSH application that could result in a reset with the error message, “Fault (0x00000E00) Task EDB BXS”.
18490 Corrected an issue in Spanning Tree Loop Protection on aggregated ports, which could cause the port to inadvertently become locked.
18711 Addressed an issue in the IGMP application that could result in a reset with the error message, “nim_events.c(216) 593 %% NIM: Timeout event(UP) on unit(1) slot(0) port(46)(intIfNum(46)) for components(IGMP_SNOOPING)”
18861 Added support for the ctAliasEntryClearAll object of the Ctron Alias MIB.
18864 Corrected an issue with timed resets, where the current configuration would be saved automatically even if the SNMP persistmode was set to manual.
18891 Corrected an issue in the output of “Show spantree stats active”, which displayed the incorrect role for the physical ports that are currently a member of an aggregation.
18928 Corrected an issue that prevented more than 1024 ARP cache entries from being displayed in the CLI when paginating.
18931 Syslog messages will now be generated on SNMP user authtication failure.

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

Changes and Enhancements in 6.61.10.0008
18584 Addressed an issue in MAC Locking application that could result in a reset with the error message, “nim_events.c(213): Error code 0x0000BADD”

Changes and Enhancements in 6.61.10.0008
18554 Corrected a port VLAN mapping error on A4 platforms having more than 24 ports. This issue prevented routing on the upper 24 ports.
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.
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.
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.
18009 Corrected an issue where IGMP query packets where not processed by IGMP unless IGMP Snooping was also configured.
17263 Corrected the format of lldpStatsRemTablesInserts in the LLDP MIB.
17116 Corrected the inability to append to a configuration file that has flow control disabled.
17957 Addressed an issue where a port could stop learning MAC addresses if the policy maptable response set to both (i.e. Hybrid authentication mode).
18012 Added support for the etsysRadiusAcctClientMIB
18103 Corrected an issue where removing an IP helped address from one interface prevented its use globally.
18194 Corrected the inability to access the network from a port in "force-auth", with multiauth mode set to strict, and maclocking firstarrival set to 1.
18231 Corrected an issue where the VLAN returned by RADIUS as a result of an RFC 3580 VLAN Authorization, fails to be applied to the user, when the MultiAuth mode is strict.
18275 Packets with an invalid destination mac address (All zero's) are now dropped.
18281 Corrected an issue where **`sys-des`** option was not persistent in LLDP commands.
18369 Corrected an issue where Dynamic ARP Inspection (DAI) was not functioning on VLAN authenticated ports.

Changes and Enhancements in 6.61.09.0012
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
16442 Corrected an issue with DHCP relay agent that could prevent completion of the DHCP process.
16911 Corrected incorrect values displayed in the output of the `show logging default` command.
17038 Corrected an issue with failing to timeout TACACS+ transactions. Loss of contact with the TACACS server could have resulted in loss of switch management.
17046 Addressed potential loss of configuration when upgrading image from 6.3
17081 Adapted disputed BPDU algorithm to support Cisco 2950 MSTP/RSTP behavior, which previously prevented spanning tree convergence.
17497 The timing of a reset configured by the `reset at` command now takes into account the offset configured through the `set summertime enable` command.
18021 Corrected an issue with enabling VLAN authenticated, Wake-On-LAN devices.
17949 Corrected a display issue with the `show mac port` command being case sensitive.
17884 The output of the `show port status` command displayed the an MGBIC-08 as 1000-lx. It is now displayed as 1000-lx/lh.
17875 Addressed a VLAN egress issue where a port’s statically applied egress could be cleared by removal of policy applied egress.
17797 Addressed a display issue with output of “show spantree nonforwardingreason” so it accurately reports the non-forwarding reason.
17717 Corrected an issue where “show config outfile” would display corrupted file names, when TACACS was used to authenticate the command.
17673 Corrected issue with calculating profile use counts. Previous the output of “show policy profile all”, could incorrectly display an applied profile as not as being in use.
17498 Corrected an issue with the processing of large LLDP PDUs that previously resulted in a system reset.
17485 Corrected an issue in TACACS+ authentication that could hang SSH and Telnet sessions.
17482 Added SNMP support for ifdescr (1.3.6.1.2.1.2.2.1.2) for SFP ports. Previously Netsight shows installed MGBIC-BX## as not installed.
17479 Resolved an issue with link up/down messages not displaying on the local console.
17478 Corrected an issue with memory utilization associated with saving configuration files. This issue could result in memory exhaustion resulting in a reset.
17286 Corrected an issue with VLAN Authorization (RFC 3580), where RADIUS VLANID tunnel attributes greater than 999 were not accepted.

Changes and Enhancements in 6.61.08.0013
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 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 during port bring-up following a stack reset.
14359 Corrected an issue whereby the `show rmon stats` command output displayed incorrect value for oversized packet counters.
14938 Corrected an issue whereby under certain circumstances the SNTP client could stop processing requests.

Changes and Enhancements in 6.61.06.0009
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.
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.
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 Addressd 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)".

Changes and Enhancements in 6.61.06.0009
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
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.
16956 Removed a spurious error message generated on deleting a loopback interface. "DAPI: Command DAPI_CMD_INTF_AUTONEG_LOCAL_ADVERTIS not supported for usp"
16958 Addressed an issue with the TCP MIB in which a continuous GetNext on the tcpListenerProcess OID would loop.
16966 Addressed an issue with rule ordering in Multi-User Authentication (User + IP phone) that resulted in a policy error, "Policy: Hardware error setting profile 7 on Port 1"
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.
17008 Addressed potential CLI hang condition when entering rules via CLI.

Changes and Enhancements in 6.61.02.0007
Added the capability to detect unidirectional stacking communication failures. This mode of failure may have resulted in units being in a permanently detached state. On detection, the failing unit will automatically reset and rejoin the stack.
13946 Addressed an issue which prevented GVRP from automatically propagating VLANs assigned to ports via vlan authentication.
15007 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.
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.
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".

Changes and Enhancements in 6.61.02.0007
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.
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.

KNOWN RESTRICTIONS AND LIMITATIONS

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

Known Issues From Previous Releases
The A4H124-48 cannot correctly read and report status of external power supplies.
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.
An SNMPv3 configuration file created in a release 03.03 will fail when loading into a switch running 6.61. **Workaround:** after a switch has been upgraded to 6.61, a previously created SNMPv3 configuration file MUST be re-generated (saved) using 6.61 code in order for SNMPv3 to function correctly.
WARNING: 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.
16569 If VLAN 4094 is provisioned in firmware 6.61, it must be removed prior to backreving firmware as VLAN 4094 is not supported in prior releases.

STANDARDS MIB SUPPORT:

RFC No.	Title
RFC 793	TCP MIB
RFC 791	IP MIB
RFC 1213	MIBII
RFC 1493	Bridge MIB
RFC-1724	RIP version 2 MIB
RFC 2819	RMON MIB
RFC 2271	SNMP Framework MIB
RFC 2668	MAU-MIB

RFC No.	Title
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 2933	IGMP MIB
RFC 3289	DiffServ MIB
RFC 3413	SNMP Applications MIB
RFC 3414	SNMP USM MIB
RFC 3415	SNMP VACM MIB
RFC 3584	SNMP Community MIB
RFC 4022	TCP MIB
RFC 4113	UDP MIB
RFC 2460	IPv6 Protocol Specification
RFC 2461	Neighbor Discovery
RFC 2462	Stateless Autoconfiguration
RFC 2463	ICMPv6
RFC 4291	IP Version 6 Addressing Architecture
RFC 3587	IPv6 Global Unicast Address Format
RFC 4007	IPv6 Scoped Address Architecture

PRIVATE ENTERPRISE MIB SUPPORT:

Title
ctbroadcast MIB
ctRatePolicing MIB
ctQBridgeMIBExt MIB
ctCDP MIB
ctAliasMib
ctTxQArb MIB
ctDownLoad MIB
etsysRADIUSAuthClientMIB
etsysRADIUSAuthClientEncryptMIB
etsysSyslogClientMIB
etsysConfigurationManagementMIB
etsysMACLockingMIB

Title
etsysSnmpPersistenceMIB
etsysMstpMIB
etsysMACAuthenticationMIB
etsysIetfBridgeMibExtMIB
etsysSntpClientMIB
EtsysIeee8023LagMibExtMIB
etsysVlanAuthorizationMIB
etsysMultiAuthMIB
etsysSpanningTreeDiagnosticMIB

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

SNMP TRAP SUPPORT

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

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

Attribute	RFC Source
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.