

Customer Release Notes

A-Series A4

Firmware Version 6.81.10.0001

February 2018

INTRODUCTION

This document provides specific information for version 6.81.10.0001 of firmware for 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:
www.extremenetworks.com/support/

FIRMWARE SPECIFICATION

| Status | Version No. | Type | Release Date |
|------------------|--------------|---------------------|---------------|
| Current Version | 6.81.10.0001 | Maintenance Release | February 2018 |
| Previous Version | 6.81.09.0001 | Maintenance Release | July 2017 |
| Previous Version | 6.81.08.0005 | Maintenance Release | June 2016 |
| Previous Version | 6.81.07.0004 | Maintenance Release | March 2016 |
| Previous Version | 6.81.06.0002 | Maintenance Release | November 2015 |
| Previous Version | 6.81.05.0003 | Maintenance Release | July 2015 |
| Previous Version | 6.81.04.0001 | Maintenance Release | April 2015 |
| Withdrawn | 6.81.03.0007 | Maintenance Release | March 2015 |
| Previous Version | 6.81.02.0007 | Maintenance Release | Sept 2014 |
| Previous Version | 6.81.01.0027 | Feature Release | April 2014 |
| Previous Version | 6.71.04.0004 | Maintenance Release | January 2014 |
| Previous Version | 6.71.03.0025 | Maintenance Release | October 2013 |
| Previous Version | 6.71.02.0008 | Maintenance Release | July 2013 |
| Previous Version | 6.71.02.0007 | Feature Release | June 2013 |
| Previous Version | 6.71.01.0067 | Feature Release | May 2013 |
| Previous Version | 6.61.08.0013 | Maintenance Release | March 2013 |
| Previous Version | 6.61.07.0010 | Maintenance Release | October 2012 |
| Previous Version | 6.61.06.0009 | Maintenance Release | August 2012 |
| Previous Version | 6.61.05.0009 | Maintenance Release | July 2012 |
| Previous Version | 6.61.03.0004 | Maintenance Release | April 2012 |

| Status | Version No. | Type | Release Date |
|------------------|--------------|---------------------|----------------|
| 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

WHAT'S NEW IN 6.61:

| |
|--|
| RADIUS Accounting – Extended Accounting to include management-access users. |
| Diagnostic Message MIB – The Enterasys Diagnostic MIB allows network administrators to monitor the current.log file through snmp. |
| RADIUS Accounting Client MIB – The Enterasys RADIUS Accounting Client MIB allows network administrators to configure RADIUS accounting |
| MAC Authentication auth-mode – MAC authentication can be configured to use the RADIUS server configured username credential where the password is the same as the username. |
| MIB object chEnvAmbientStatus of the CTRON-ENVIRONMENT-MIB – Allow remote SNMP monitoring of thermal state of the master unit. |
| Enterasys Networks' Multiple Authentication MIB Notification Group – Added support for etsysMultiAuthSuccess, etsysMultiAuthFailed, etsysMultiAuthTerminated, etsysMultiAuthMaxNumUsersReached notifications. |
| Login Accounts – Increased the number of supported local login accounts from 16 to 32. |

| 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) |
| 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 | MSTP Multisource Detection |
| 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 |

| Existing Product Features | |
|---|--|
| 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 | Dynamic and Static MAC Locking |
| 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 | New MAC Trap |
| LLDP-MED Network-Policy TLV | Secure directory |
| Basic IPv4 Routing (static, RIP v1/v2) | Enterasys Policy Single user or User + IP Phone |
| Console Disconnect | Security Log |
| Service Access Control Lists (SACL) | Tx Queue Monitoring |
| TACACS+ management | Secure Copy / Secure FTP (SCP/SFTP) |
| Mixed Strict and WRR Port Transmit Queue settings | IPv4/IPv6 Dual Host Management Support (SNMP, Telnet, SFTP, SCP, SSH, RADIUS) |
| Enterasys Spanning Tree Diagnostic MIB | TDR-based cable status check detects cable breaks and disconnections |
| ARP Spoof Protection | IPsec for RADIUS transactions |
| Flexible Link Aggregation Groups | Web Authentication (PWA) / Web Redirect PWA+ |
| SNTP Server-Client Authentication | Time Based Reset |
| CoS MIB based Flood Control (broadcast, multicast, and unknown unicast) | DHCP Spoof Protection |
| Automated Deployment | Convergence End Points (CEP) Phone Detection |
| Multicast Listener Discovery (MLD) Snooping | L2 Multicast Querier for IGMP and MLD |

INSTALLATION AND CONFIGURATION NOTES

Warning:

- Direct firmware upgrades to 6.61.05 from 3.02 (and previous) images may leave the switch in an unrecoverable state. It is **required** to upgrade to 3.03 prior to loading 6.61.05.
- 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 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.

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, we recommend 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 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 www.extremenetworks.com/support/ for the latest firmware updates to the A-Series A4 and follow the TFTP download instructions that are included in your Configuration Guide or CLI Reference.

Soft copies of the A4 Configuration Guide and the A4 CLI Reference are available at no cost on the Extreme Networks documentation site, <http://documentation.extremenetworks.com>.

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 | 9 |
| 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 9 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 6.81.10.0001

19751 Corrected a reset condition caused by a memory leak in Extreme Stacking MIB.

19752 Corrected the use of an incorrect MAC address in syslog messages.

19755 Corrected reset condition associated with the mishandling of telnet buffers.

Changes and Enhancements in 6.81.09.0001

19704 Corrected an potential reset while saving the configuration after a NAC enforce

Changes and Enhancements in 6.81.08.0005

19702 Corrected an issue in CEP LLDP-MED detection where Class Type 1 devices were incorrectly assigned to a policy.

19694 Removed a check (first introduced in 6.81.02) that terminated Telnet/SSH sessions if the window size was small.

19511 Corrected an issue where polling of the etsysResourceUtilizationMIB could cause a loss of management and/or a reset.

19671 Corrected a potential user VLAN assignment error when an authenticated VLAN assignment is removed.

19633 Corrected an issue with multicast forwarding to stack members on a change of stacking port link state.

19685 Corrected an issue in Cisco Discover Protocol support where VMware ESXi devices are not shown as neighbors.

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 6.81.07.0004 |
|--|
| 19650 Corrected a reset issue that can occur when an IP helper address is configured for the same subnet as the interface it is added to. |
| 19644 Corrected an issue in Port mac locking that could result in a “nim_events.c(213)” reset event. |
| 19320 Corrected an issue where the SNTP server table is restored in reverse order from entry configuration. |
| 19614 Added support for UDP port 7777 to “ip forward-protocol”. Note: Other ports not specified the configuration guide are still not supported by this functionality. |
| 19652 Corrected an issue with processing LLDP packets that could result in a reset with the message: <code>Last switch reset was caused by buff.c(546)</code> : |
| 19649 Corrected an issue in the display of radius server configuration that could erroneously be detected as a configuration change. |

| Changes and Enhancements in 6.81.06.0002 |
|---|
| 19608 Corrected a potential reset condition when attempting to save a prompt (<code>set prompt</code>), of 50 or more characters. |
| 19511 Corrected a potential loss of management and eventual reset condition seen when monitoring the <code>etsysResourceUtilizationMIB</code> . |
| 19586 Corrected an issue where the <code>snmpEngineTime</code> (1.3.6.1.6.3.10.2.1.3) MIB value rolled over after 497 days of system uptime instead of the maximum allowed 24855 days. |
| 19579 Corrected an issue where the <code>set length</code> command was not persistent. |
| 19528 Corrected an issue in the TFTP application that may have resulted in corrupted file transfers. |
| 19450 Corrected an issue in the output of the <code>show vlan portinfo vlan</code> 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: <code>edb_bxs.c(1314) 286 %% Last switch reset caused by Fault(0x00000E00) SRR0(0x01554000)</code> |
| 19583 Corrected a memory loss issue in SNMP trap processing that could result in a reset. |
| 19588 Corrected a reset issue in the LLDP application, which produced the log entry: <code>reset caused by buff.c(546)</code> |
| 19599 Corrected a condition that prevented switching user's VLAN from RFC3580 assigned to Policy assigned. |

| Changes and Enhancements in 6.81.05.0003 |
|--|
| 19553 Corrected a potential reset condition when processing jumbo 802.1x and 802.1s control frames. |
| 19267 Corrected an issue that could prevent SFPs from linking on bootup if auto-negotiation is disabled. |
| 19534 Corrected an SNMP issue with in the <code>ctChasPowerTable</code> where power supply redundancy may be incorrectly returned. |
| 19484 Corrected a logic error with handling of an apostrophe as the second character of a system login. This error previously resulted in the incorrect storage of the password. |

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

Changes and Enhancements in 6.81.03.0007

Added Support for the Extreme Stacking MIB.

Note: Not all objects translate to A4-Series functionality (see Known Issues).

19319 The TLS_FALLBACK_SCS mechanism was added to SSL. When run with a supporting browser, it will prevent a third party from exploiting the SSL protocol fallback mechanism (CVE-2014-3566).

Note: SSL is supported only for the purpose of web-based management and is disabled by default.

19383 Corrected a potential method of corrupting the startup configuration file. This may previously have resulted in the continuous rebooting of the system on power up.

19276 Corrected an issue where ports could erroneously be removed from link aggregations. This could result in users MAC addresses being learned on incorrect ports.

19437 Corrected a reset issue with support of the LLDP POE tx-tlv which resulted in the message:

NIM 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

19287 Corrected a reset issue associated with accessing the ctChasFanModuleState MIB object.

19288 Corrected an issue that prevented do1x authentication of Cisco Voice Gateways.

19377 Corrected an issue that prevented the disabling of an admin login account from being persistent.

19311 Corrected an issue that could prevent host transmission of a gratuitous ARP on master unit failover.

18907 Corrected an issue with support of the NetSight Inventory Manager "Configuration Template".

19305 Addressed a delay in transmitting LLDP Network Policy on ports that are authenticating. It had been observed that Polycom IP phones using LLDP may timeout on booting.

19330 Corrected reset issue that resulted in the message: broad_cpu_intf.(2992): Error code 0x00000FFF

19332 Corrected a reset issue in the SNMP Task that resulted in the message:

edb_bxs.c(1314) 73 %% Last switch reset caused by Fault(0x00000300)
SRR0(0x01104270) ESR(0x00800000) MSR(0x00000200) DEAR(0x0000000C)
IMISS(0x01104270)

19366 Corrected an issue where the output of show lldp port remote-info was missing remote-info POE Device-Type information.

19241 Corrected an issue where erroneous POE traps "etsysPseChassisPowerNonRedundant" and "etsysPseChassisPowerRedundant" were transmitted.

19318 Corrected an issue where the "set length" command was not persistent.

Changes and Enhancements in 6.81.02.0007

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

18787 Corrected a potential reset condition in the "dot1s_timer_task" task, which produced the log entry:

Last switch reset was caused by sal.c(1184): Error code 0x00000000

19196 Addressed an issue which allowed corrupted DHCP packets, to be looped back on dhcp snooping trusted ports.

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 6.81.02.0007

Prevent logging the informational message `License file not present` when no license file is found on boot.

16086 Attempt to recover from a L2 table DMA error that previously resulted in a reset with a log entry of: "soc_l2x_thread DMA failed too many times". On an L2 Table DMA failure we will now walk the table to find the corrupted entry and remove it. The expected warning message is:
warning soc_l2x_thread: Bad L2 table entry found. Recovering

19249 Modified the logging behavior of SNTP to prevent excessive changed system time messages:
sntp_client.c(2109) 62 %% SNTP has changed system time

18919 Corrected a potential exception condition with the resulting log message:
Last switch reset caused by Fault(0x00000300)

18870 Corrected a potential reset condition in the "snoopTask" task, which produced the log entry, "sal.c(1197): Error code 0x00000000".

18880 Corrected an issue where Initiating a Secure Copy (SCP) file transfer could result in loss of management.

18907 Corrected an issue that prevented clearing the SNMP community name public using NetSight.

19033 Corrected an issue in TACACS+ command accounting, where the receipt of an unknown TACAC reply packet caused the CLI to become unresponsive.

18931 Syslog messages will now be generated on SNMP user authentication failure.

18864 Corrected an issue with timed resets, where the current configuration would be saved automatically even if the SNMP Persistmode was set to manual.

18861 Added support for the ctAliasEntryClearAll object of the Ctron Alias MIB.

Note: This change now requires NetSight Management Software 5.1/6.1 or higher to read the Alias table.

18490 Corrected an issue where Loop Protect could erroneously lock a link aggregation.

19257 Corrected an issue with Policy CoS rate limiter implementation that could cause loss of Spanning Tree BPDUs.

19158 Corrected an issue that resulted in erroneous LLDP traps.

lldpStatsRemTablesInserts + Wrong Type (should be gauge 32 or Unassigned32) xxx

lldpStatsRemTablesDelets + Wrong Type (should be gauge 32 or Unassigned32)xxx

lldpStatsRemTablesDrops + Wrong Type (should be gauge 32 or Unassigned32)xxx

lldpStatsRemTableAgeOuts + Wrong Type (should be gauge 32 or Unassigned32)xxx

Changes and Enhancements in 6.81.01.0027

19793 Ported Common Vulnerabilities and Exposures (CVE) patches to SSH to address: CVE-2006-4925, CVE-2008-1657, and CVE-2012-0814.

Note: Vulnerability scan tool that report vulnerabilities based on SSH version may still report these as issues.

Changes and Enhancements in 6.71.04.0004

18891 The output of the CLI command `show spantree stats active` will now display the role of lag member physical ports as "disabled". Previously their role was displayed as "designated".

18691 Corrected an issue in the implementation of the Enterasys Resource Utilization MIB, where setting `etsysResource1minThreshold` to zero, did not prevent `etsysResourceLoad1minThresholdExceeded` notifications.

Changes and Enhancements in 6.71.04.0004

18761 Corrected an issue where etsysMACLockingMACViolation traps could erroneously be generated

Changes and Enhancements in 6.71.03.0025

18771 Corrected an issue where an 802.1x supplicant client's packet are leaked to the network during the authentication process.

17978 Allow local login authentication, when TACACS+ management authentication is configured and the TACACS+ server is offline.

18421 Corrected an issue where 802.1x supplicant EAP packets where flooded to other ports.

16911 Corrected an issue where the `show logging default` command, displays the incorrect severity values.

18584 Addressed an issue in MAC Locking application that could result in a reset with the error message: `nim_events.c(213): Error code 0x0000BADD`

18554 Corrected a port VLAN mapping error on 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.

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.

Changes and Enhancements in 6.71.02.0008

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

Changes and Enhancements in 6.71.02.0007

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

Changes and Enhancements in 6.71.01.0067

17239 Corrected issue where the `etsysMultiAuthSessionAuthAttemptTime` MIB object was not updated each time a session attempted re-authentication.

17419 Corrected an issue where changing a port mirror destination port, to a port on a different unit, could cause the mirror to fail.

| Changes and Enhancements in 6.61.08.0013 |
|---|
| 16442 Corrected an issue with DHCP relay agent that could prevent completion of the DHCP process. |
| 16911 Corrected incorrect values displayed in the output of the <code>show logging default</code> 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 <code>set summertime enable</code> command. |
| 18021 Corrected an issue with enabling VLAN authenticated, Wake-On-LAN devices. |
| 17949 Corrected a display issue with the <code>show mac port</code> command being case sensitive. |
| 17884 The output of the <code>show port status</code> command displayed the an MGBIC-08 as 1000-lx. It is now displayed as 1000-lx/lh. |
| 17137 The output of the <code>show port status</code> command displayed an MGBIC-LC03 as 1000-sx. It is now displayed as 1000-lx/lhmm. |
| 17875 Addressed a VLAN egress issue where a port's statically applied egress could be cleared by removal of policy applied egress. |
| 17797 Addressed a display issue with output of <code>show spantree nonforwardingreason</code> so it accurately reports the non-forwarding reason. |
| 17717 Corrected an issue where <code>show config outfile</code> 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 <code>show policy profile all</code> 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. |
| 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 startup:

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.

| Changes and Enhancements in 6.61.06.0009 |
|--|
| 14359 Corrected an issue whereby the <code>show rmon stats</code> command output displayed incorrect value for oversized packet counters. |
| 14938 Corrected an issue whereby under certain circumstances the SNMP client could stop processing requests. |
| 15192 Resolved an issue whereby the <code>ifTableLastChange</code> MIB object (1.3.6.1.4.1.9.9.27) returned incorrect data. |
| 15283 Addressed an issue whereby the <code>entPhysicalsFRU</code> MIB object (1.3.6.1.2.1.47.1.1.1.16) 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 <code>mdi</code> and <code>mdix</code> strings to be interchanged in <code>show port mdix all</code> and <code>show config port</code> 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 <code>chHotTemp</code> object (. 1.3.6.1.4.1.52.11004) in the <code>xtraps</code> 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 <code>set policy rule < profile-index > ipdestsocket</code> 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. |

Changes and Enhancements in 6.61.06.0009

17048 Resolved a code exception in SNMP with reset

```
BOOT[141143864]: edb_bxs.c(1226) 108 %% Last switch reset caused by
Fault(0x00001100) SRR0(0x01162ae8) SRR1(0x4000b030) MSR(0x00001030)
DMISS(0xc914d6d0) IMISS(0x00000000)
```

17083 Addressed an issue whereby logging to the switch via WebView could cause a reset with a message similar to:

```
edb_bxs_api.c(786) 202 %% Last switch reset caused by Fault(0x00000300)
SRR0(0x01113A40) SRR1(0x0000B030) DMISS(0x13350104) IMISS(0x00000000)
DAR(0x00000000) DSISR(0x0A000000)
```

17120 Removed informational debug messages from the CLI output that are similar to:

```
SIM[88867688]: broad_hpc_drv.c(2686) 19017 % bcm_port_update: u=0 p=20 link=1 rv=-
15
```

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.

Changes and Enhancements in 6.61.02.0007

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".

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 6.81.10.0001**

There are no new known restrictions or limitations associated with this release.

Known Issues From Previous Releases

Extreme Summit and BlackDiamond platforms may use a single source MAC address for protocol and host generated packets. If redundant connections are made to these devices without the use of a link aggregation, loss of connectivity to their host IP address may result. True for all releases.

Extreme Stacking MIB:

1. `extremeStackMemberStackPriority` as defined by the MIB has a valid range 1-15. The A4 will default to 16.
2. `extremeStackMemberCurConfig` is not supported.
3. `extremeStackingPortIfIndex` ranges from 1-16. Odd numbered indexes are stack UP ports and even number indexes are stack DOWN ports. Each stack unit has two indexes which are assigned sequentially based on unit number (i.e., `extremeStackingPortIfIndex 1` = unit 1 UP, `2` = unit 1 DOWN, `3` = unit 2 UP, `4` = unit 2 DOWN ...).
4. `extremeStackingPortRemoteMac` is not supported

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 back-revving firmware as VLAN 4094 is not supported in prior releases.

Convergence End Points (CEP) Phone Detection is limited to single user authentication. It is not compatible with "User plus Phone".

STANDARD 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 | Ethernet-Like MIB |
| RFC 2233 | ifMIB |
| RFC 2863 | ifMIB |
| RFC 2620 | RADIUS Accounting MIB |
| RFC 2618 | RADIUS Authentication MIB |
| RFC 3621 | Power Ethernet MIB |
| IEEE 802.1X MIB | 802.1-PAE-MIB |
| IEEE 802.3ad MIB | IEEE 8023-LAG-MIB |
| RFC 2674 | 802.1p/Q BridgeMIB |
| RFC 2737 | Entity MIB (physical branch only) |
| RFC 5519 | MGMD-STD-MIB |
| RFC 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 |

EXTREME NETWORKS PRIVATE ENTERPRISE MIB SUPPORT

| Title |
|--------------------|
| ctbroadcast MIB |
| ctRatePolicing MIB |

| Title |
|---------------------------------|
| ctQBridgeMIBExt MIB |
| ctCDP MIB |
| ctAliasMib |
| ctTxQArb MIB |
| ctDownLoad MIB |
| etsysRADIUSAuthClientMIB |
| etsysRADIUSAuthClientEncryptMIB |
| etsysSyslogClientMIB |
| etsysConfigurationManagementMIB |
| etsysMACLockingMIB |
| etsysSnmpPersistenceMIB |
| etsysMstpMIB |
| etsysMACAuthenticationMIB |
| etsysletfBridgeMibExtMIB |
| etsysSntpClientMIB |
| Etsysleeee8023LagMibExtMIB |
| etsysVlanAuthorizationMIB |
| etsysMultiAuthMIB |
| etsysSpanningTreeDiagnosticMIB |
| extremeStackable |

Extreme Networks 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.

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 AUTHENTICATION AND AUTHORIZATION ATTRIBUTES

| Attribute | RFC Source |
|--------------------|--------------------|
| Calling-Station-Id | RFC 2865, RFC 3580 |
| Class | RFC 2865 |

| Attribute | RFC Source |
|-----------------------|------------------------------|
| 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.