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

Customer Release Notes

D-series

Firmware Version 6.03.17.0001
February 2018

INTRODUCTION

This document provides specific information for version 6.03.17.0001 of firmware for the following D2 products:

D2G124-12	D2G124-12P

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	6.03.17.0001	Maintenance Release	February 2018
Previous Version	6.03.16.0001	Maintenance Release	October 2016
Previous Version	6.03.15.0002	Maintenance Release	December 2015
Previous Version	6.03.14.0004	Maintenance Release	February 2015
Previous Version	6.03.13.0001	Maintenance Release	October 2013
Previous Version	6.03.12.0006	Maintenance Release	May 2013
Previous Version	6.03.11.0004	Maintenance Release	April 2012
Previous Version	6.03.10.0003	Maintenance Release	June 2011
Previous Version	6.03.09.0005	Maintenance Release	January 2011
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	Feature Release	September 2009
Previous Version	1.00.04.0001	Maintenance Release	March 2009
Previous Version	1.00.03.0002	Maintenance Release	September 2008
Previous Version	1.00.02.0002	Maintenance Release	August 2008
Previous Version	1.00.01.0005	Maintenance Release	July 2008
Previous Version	1.00.00.0029	Initial Release	May 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	6.1
NMS Console	6.1
NMS Inventory Manager	6.1
NMS Policy Manager	6.1
NMS NAC Manager	6.1

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

PLUGGABLE PORTS SUPPORTED

MGBICs	Description
MGBIC-LC01	1000Base-SX, IEEE 802.3 MM, 850 nm Short Wave Length, 220/550M, LC SFP
MGBIC-LC03	1000Base-SX-LX/LH, MM, 1310 nm Long Wave Length, 2 KM, LC SFP
MGBIC-LC07	Extended 1000Base-LX, IEEE 802.3 SM, 1550 nm Long Wave Length, 110KM, LC SFP.
MGBIC-LC09	1000Base-LX, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 KM, LC SFP
MGBIC-MT01	1000Base-SX, IEEE 802.3 MM, 850 nm Short Wave Length, 220/550 M, MTRJ SFP
MGBIC-02	1000Base-T, IEEE 802.3 Cat5, Copper Twisted Pair, 100 M, RJ45 SFP
MGBIC-08	1000Base-LX/LH, IEEE 802.3 SM, 1550 nm Long Wave Length, 80 KM, LC SFP
MGBIC-LC04	100Base-FX, IEEE 802.3 MM, 1310 nm Long Wave Length, 2 KM, LC SFP
MGBIC-LC05	100Base-FX, IEEE 802.3 SM, 1310 nm Long Wave Length, 10 KM, LC SFP
MGBIC-BX10-D	1000Base-BX10-D, 1 Gb, Single Fiber SM, Bidirectional, 1490nm Tx / 1310nm Rx, 10 km, Simplex LC SFP (must be paired with MGBIC-BX10-U)
MGBIC-BX10-U	1000Base-BX10-U, 1 Gb, Single Fiber SM, Bidirectional 1310nm Tx / 1490nm Rx, 10 km, Simplex LC SFP (must be paired with MGBIC-BX10-D)
MGBIC-BX40-U	1 Gb, 1000Base-BX40-U Single Fiber SM, Bidirectional, 1310nm Tx / 1490nm Rx, 40 Km, Simplex LC SFP (must be paired with MGBIC-BX40-D)
MGBIC-BX40-D	1 Gb, 1000Base-BX40-D Single Fiber SM, Bidirectional, 1490nm Tx / 1310nm Rx, 40 Km, Simplex LC SFP (must be paired with MGBIC-BX40-U)
MGBIC-BX120-D	1 Gb, 1000Base-BX120-D Single Fiber SM, Bidirectional, 1590nm Tx / 1490nm Rx, 120 Km, Simplex LC SFP (must be paired with MGBIC-BX120-U)
MGBIC-BX120-U	1 Gb, 1000Base-BX120-U Single Fiber SM, Bidirectional, 1490nm Tx / 1590nm Rx, 120 Km, Simplex LC SFP (must be paired with MGBIC-BX120-D)

NOTE

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

PRODUCT FEATURES

What's New in 6.03

Hybrid Policy Mode provides greater deployment flexibility by enabling simultaneous support of Enterasys Policy and RFC3580 tunneling on the system. For example, in hybrid mode VLANs can be assigned via the tunnel RADIUS attributes while the user role can be assigned via the filter RADIUS attributes. This separation gives the administrator additional flexibility to segment their networks into more VLANs than the number of roles that a given switch supports.
PWA & RFC3580 enables VLAN authorization and segmentation for PWA sessions.
LLDP-MED Network-Policy TLV reduces deployment costs of VoIP deployments by enabling standards-based provisioning of VoIP phones. The switches can be configured to assign VLAN, QoS, rate-limiting, and other operational parameters for LLDP-MED enabled VoIP phones. When combined with Enterasys Policy at the edge it is a powerful, low cost solution for deploying convergent networks.
TACACS+ is a protocol that enables authentication, command-level authorization, and auditing of administrative sessions. TACACS+ enables IT organizations to meet compliance and auditing requirements for system management.
Host Protect improves resiliency of the switching infrastructure by leveraging hardware-based rate limiters to protect the host CPU from being overburdened by control traffic. For example, using this functionality the switch CPU will be unaffected by network loops that occur in downstream hubs and unintelligent switches. Use it in combination with STP Loop Protect, SpanGuard, and disabling Auto MDI/MDI-X per port for the highest level of protection against inadvertent or malicious switching loops! Host protect is permanently enabled and not managed via the CLI.
Secure Copy / Secure FTP (SCP/SFTP) provides the means to securely transfer configuration and log files from the switches under management. The new applications address can be leveraged to meet compliance and auditing guidelines.
AES-128 support with SNMPv3 extends the highest level of confidentiality protection for SNMP management traffic.
Power Supply & Fan Monitoring via SNMP enables visibility to potential hardware issues that could affect network availability. The early view enables administrators to proactively address hardware issues and ensure business continuity!
Copy & Paste of configuration files between switches enable quick troubleshooting, deployment or problem resolution.
Removal of 18 Mask Limitation for policy implementations. Previously up to 10 masks per port were supported with a total switch limitation of 18 unique masks. The 18 unique mask switch limitation has been eliminated.
Show support CLI command to display switch information for troubleshooting
High-Temperature Alerts allows the network administrator to change the maximum temperature threshold where a trap and syslog message is generated warning them of high-temperature conditions before service is affected.

Multiport LAG to single port LAG automatic failover – allows multiport LAGs to continue operating in multiport mode as long as there is at least one active port in the LAG. Previously administrators would need to create backup single-port LAGs to ensure that a multi-port LAG would not change its behavior if all but one port dropped out of the LAG. This redundant configuration effectively reduced the number of LAGs that could be configured in the switch by half. Alternatively, you would have had to configure egress tagging at the port level to match the LAG configuration ensuring that traffic would be marked appropriately when only a single port remained active.
DHCP Spoof Protection - Previously Enterasys Policy had to be used to protect DHCP services, but now DHCP protection is independent of ETS Policy. Thus, ETS Policy resources can now be reclaimed and used to protect other network services.
ARP Spoof Protection from man-in-the-middle attacks. This feature works in conjunction with the DHCP snooping database to ensure that ARP requests match the IP/MAC/Port binding relationship dynamically created during DHCP client/server exchanges.
CPU/Memory utilization monitoring via SNMP to enable remote monitoring of these resources
Implemented the ability to set the port mdi / mdix settings via the CLI to allow support for a variety of media converters. This feature is not supported on RJ45 Combo ports that can be used in an either/or configuration with SFP MGBICs. The commands added are: show port mdix { all | auto | forced-auto | mdi | mdix } [port-string] set port mdix { auto | forced-auto | mdi | mdix } [port-string] By default, Enterasys Networks switch devices are configured to automatically detect the cable type connection, straight through (MDI) or cross-over (MDIX), required by the cable connected to the port.
Cable Troubleshooting - Added a new feature that allows you to troubleshoot and locate faults in copper cable connections on a per port basis. A new CLI command, “show port cablestatus <port-string>,” allows you to diagnose cabling problems in realtime. The command returns the following: Normal = normal Open = no cable attached to port Short = detection of an inter-pair short Fail = unknown error or crosstalk Detach = for ports on stack units no longer present, but were previously connected Not Supported = ports other than 1GE RJ45 ports The “Detach” designation is applicable to stacking products only. This command is only supported on RJ45 copper connections running at 1GE speeds.
Added support for the etsysResourceScalarsGroup attribute from the etsysResourceUtilizationMIB to enable remote monitoring of the CPU load via SNMP management tools.
Prompt before reboot - Modified the “set boot system” command to prompt the administrator before resetting the switch. If the administrator elects not to reset the switch, the new firmware is copied into the active partition but only takes effect after the switch is reset/rebooted.
Modified the newmac trap to include the MAC address of the client in the SNMP trap.
Added SMON MIB support for management of Port Mirroring.
Added support for monitoring resource utilization via the etsysResourceUtilizationMIB.

Existing Product Features	
802.1D	16K MAC Address Table
802.1Q -VLAN Tagging	Selectable MAC Hashing Algorithms
802.1p -Traffic Management / Mapping to 6 Queues	Auto-Negotiation
802.3x Flow Control	8 Priority Queues per Port

Existing Product Features	
802.1x IP Phone Authentication	MGBIC Support: MGBIC-LC01, MGBIC-LC03, MGBIC-LC09, MGBIC-02, MGBIC-08, MGBIC-MT01, MGBIC-LC04, MGBIC-LC05, MGBIC-LC07
802.3ad – Dynamic and Static Creation for Link Aggregation (6 LAGs, 8 ports per LAG)	Session-Timeout and Termination-Action RADIUS Attributes Support
802.1s – Multiple Spanning Tree Protocol (up to 4 instances)	Ability to Set Port Advertised Ability via CLI
802.1w – Rapid Spanning Tree	Multi-method Authentication
RFC-3580 VLAN authentication using MAC Authentication, Dot1x	User + IP Phone Authentication
Spanning Tree Backup Root	Dynamic VLAN Assignment (3 RFC3580 users/port)
Spanning Tree Loop Protect	L2 Policy Rules
LLDP/LLDP-MED with TLVs	COS based Inbound Rate Limiter per Policy User
Legacy Path Cost	DHCP Server
Spanning Tree Pass Through	Web Authentication (PWA)
SpanGuard	Web Redirect – PWA+ and URL redirection
Link Flap Detection	802.1X Authentication
Per Port Broadcast Suppression	Non-Strict 802.1X Default RFC 3580 With Auth Failure
Port Mirroring	RADIUS Client
Private Port (Private VLAN)	Turn Off RADIUS Authentication (RADIUS Realm)
Cabletron Discovery Protocol (CDP)	Queuing Control Strict and Weighted Round Robin
Cisco Discovery Protocol (CDP) v1/2	MAC Authentication / MAC Authentication Masking
Cisco IP Phone Discovery	MAC Authentication Retained After Age Out
GVRP	RADIUS Accounting for MAC Authentication
IGMP v1/v2/v3 and IGMP Snooping	EAP Pass Through
Syslog	Dynamic and Static MAC Locking
Text-based Configuration Upload/Download	New Mac Trap (like the Matrix-E1)
CLI Management	Dynamic Egress
Telnet Support	SSHv2 Support
IPv4/IPv6 Dual Host Management Support	WebView
Discard VLAN Tagged Frames	SSL Interface to WebView
Policy	RMON (4 groups)
Priority Classification L3-L4	RMON View in the CLI With Persistent Sets
VLAN-to-Policy Mapping on a per Port Basis	RMON Packet Capture/Filtering Sampling
Node/Alias Table	SNMPv1, SNMPv2c, SNMPv3
ToS Rewrite	Simple Network Time Protocol (SNTP)
SMON MIB support for port mirroring	Alias Port Naming
DiffServ	Ability to Set Time and Date via the MIB
Clear config/clear config all will retain host IP	Jumbo Frame (up to 9K)
VLAN Classification	Configurable Login Banner

Existing Product Features	
TACACS+	Secure Copy & Secure FTP
Copy & Paste of configuration files	Hybrid Policy Mode
Host Protect	AES-128 support with SNMPv3
Power Supply & Fan Monitoring via SNMP	Show support CLI command
High-Temperature Alerts	Multiport LAG to single port LAG automatic failover
DHCP Spoof Protection	ARP Spoof Protection
CPU/Memory utilization monitoring via SNMP	TDR - Cable Troubleshooting
CoS MIB based Flood Control (broadcast, multicast, and unknown unicast)	User selectable code points for Voice over IP via DiffServ
Packets can be dropped, shaped, marked (with an IP DSCP or IP precedence value) or sent unchanged to the switching process	

INSTALLATION AND CONFIGURATION NOTES

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 configs/<filename> command. Please note that you will need a copy of your previous configuration if you need to back-rev from 6.03.xx.xxxx to the previous firmware version.

The D2 most likely will not be shipped to you pre-configured with the latest version of software. It is strongly recommended that you upgrade to the latest firmware version BEFORE deploying any new switches. Please refer to www.extremenetworks.com/support/ for the latest firmware updates to the D-Series and follow the TFTP download instructions that are included in your Configuration Guide.

TFTP download instructions are also available on the Extreme Networks support website at: www.extremenetworks.com/support/.

Policy Capacities

Policy roles (profiles) accepted from NetSight	255
Max Number of simultaneously enforced roles	13 (12 port roles + one Phone role)
Single role (Policy) limitation	100 rules and 10 masks
Number of users per port	Tunnel Mode = 3, Policy Mode = 1 or PC+Phone
Number of unique rules per system	1200 (12 ports of 100 rules)
Number of rules per single role or port	100
Number of unique masks per system	120 (12 ports with 10 masks each)
Number of masks per single role or port	10

FIRMWARE CHANGES AND ENHANCEMENTS:

Changes and Enhancements in 6.03.17.0001
19757 Corrected a syslog message format issue with MAC addresses containing zeros.

Changes and Enhancements in 6.03.16.0001
19680 Corrected an issue in the processing of received LLDP packets that could result in loss connectivity with the transmitting device.

Changes and Enhancements in 6.03.15.0002
19500 TFTP now accepts file names of up to a maximum length of 31 characters.
19476 Corrected an issue where the RADIUS VLAN attribute was not applied, when the maptable response was set to set to “both”, and the RADIUS response contained both a VLAN and a filter ID (Policy ID).
19380 Corrected an issue were a login account lockout would become permanent if the switch was reset during the lockout period.
16741 Corrected an issue where a “Kiss of Death packets” would cause the SNTP application to place active servers in an out of Service state.

Changes and Enhancements in 6.03.14.0004
19199 Added support for Secure Copy (SCP) and SFTP copy of firmware images. **Note**: This capability is only available through the CLI “copy” command.
18880 Corrected an issue where initiating a Secure Copy (SCP) file transfer could result in loss of management.
18764 Corrected an issue in LLDP-MED that could prevent device participation.
18990 Corrected an issue where Spanguard locking can be triggered by LLDP.
18934 Corrected an issue in Policy Hybrid mode where the VLAN returned in the RADIUS tunnel attribute was not correctly applied to the authenticating port.
19212 Addressed an issue which allowed corrupted DHCP packets, to be looped back on dhcpsnooping trusted ports.
19125 Removed third party trap 1.3.6.1.4.1.6132.1.1.1.50(1).
19255 Ported Common Vulnerabilities and Exposures (CVE) patches to SSH to address: CVE-2006-4925. **Note**: Vulnerability scan tools that report vulnerabilities based on SSH version may still report this issue.

Changes and Enhancements in 6.03.13.0001
18273 Corrected an issue that prevented an IPv6 host response to an ICMPv6 echo request.
18565 Corrected an issue with DHCP Snooping where DHCP NACK packets were flooded.
18582 Corrected an issue where local management configured for RADIUS authentication would not failover to local authentication, if the RADIUS server was unreachable.

Changes and Enhancements in 6.03.12.0006
18453 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.
16742 Corrected error message “PoE timeout while in reset and recovery mode”.
17286 Corrected an issue with VLAN Authorization (RFC 3580), where RADIUS VLANID tunnel attributes greater than 999 were not accepted.

Changes and Enhancements in 6.03.12.0006
17817 Corrected an issue where disabling a copper port causes an SFP port to drop link.
17909 Addressed an issue which prevented DHCP to function properly on trusted ports when DHCP snooping was enabled.
17978 Corrected an issue which prevented local management login when configured for TACACS+ authentication and the TACACS+ server cannot be reached.

Changes and Enhancements in 6.03.11.0004
13946 Addressed an issue which prevented GVRP from automatically propagating VLANs assigned to ports via VLAN authentication.
14575 Addressed an issue associated with EAP pass-through mode which could potentially cause a reset or loss of management. This issue was seen when multiple PoE IP phones on a stack lost connection to the voice controller and simultaneously failed over to the backup server.
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.
14938 & 16741 Corrected an issue whereby under certain circumstances the SNTP client could stop processing requests.
15013 Addressed a potential TCP vulnerability identified in US-CERT VU#723308.
15189 With this release UDP ports 7700 and 7800 are no longer used during the TFTP image download operation.
15841 Addressed an issue where the user defined MDI/MDIX mode was reversed when issuing the "Set port mdix" command.
15859 Corrected an issue with the premature closure of the RADIUS UDP socket. This issue could have prevented user authentication when the server response was routed through the unit and was not received from the RADIUS server within 1 second.
16042 Addressed an issue with hybrid policy authentication where the authenticated user was not moved to the VLAN specified by tunnel attributes.
16262 Addressed an issue introduced in firmware 6.03.10 whereby the link state between two D2 switches remained up after one side was administratively shut down.
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.
16300 Corrected an issue which prevented locking a MAC address to a new port once it was locked to a range of ports via the “set macklock” command.
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 6.03.10.0003
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.
14857 Resolved an issue with SNTP which caused the “show support” command output to display incorrect time of reset for the unit.
15081 802.1x supplicants now properly failover to specified backup RADIUS servers when the primary server is unavailable.
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 6.03.10.0003
15384 Corrected an issue which resulted in erroneous syslog messages similar to “radius_txrx.c(395) 1006 % RADIUS: Failed to send the request” when users logged in with proper credentials.

Changes and Enhancements in 6.03.09.0005
13278 Resolved an SSH issue introduced in firmware 6.03.02 whereby users were unable to login to the switch using the Ponderosa SSH Client application.
13979 Resolved a Multiauth issue whereby the switch continued to send MAC authentication requests after the supplicant successfully authenticated via 802.1X, which could potentially cause a reset.
14196 & 14334 The “show port advertise” command now correctly displays advertised capabilities for ports 9 through 12 when link is down.
14447 Monitoring SSH connections 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 port VLAN egress list.
14739 The LLDP auto-negotiation TLV definition now advertises correct port capability.

Changes and Enhancements in 6.03.08.0012
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.
14629 & 14690 Resolved an issue introduced in release 6.03.06 whereby applying policy to a port with existing policy would block traffic from egressing the port.

Changes and Enhancements in 6.03.06.0008
12796 Resolved an issue whereby some MGBIC-LC03 LX SFP modules would display as type SX in the "show port status" command output.
13113 When restoring a saved configuration file, Spanning Tree settings are now loaded in correct order.
13153 Corrected an issue where loss of management could ensue when a Telnet session with an active TFTP transfer is terminated.
13392 Resolved an issue whereby static ARP entries were displayed in the configuration file after being administratively removed.
13422 The value of the MIB object snmpEnableAuthenTraps (1.3.6.1.2.1.11.30) is now persistent across device resets.
13674 Resolved an issue with IGMP snooping filters whereby the device could drop some SMB packets in transit, causing the file transfer to fail.
13867 Resolved an issue whereby applying a new policy role to a port caused the port’s egress status to change from untagged to tagged.
13943 & 14096 Resolved a potential memory leak associated with IP multicast which could cause a reset with a message similar to "osapi.c(1381) and broad_cpu_intf.(3086)" or "CRASH - broad_cpu_intf and hapiBroadPruneTxPorts".
13980 The value of port utilization percentage is now calculated and displayed correctly in the “show rmon history” command output.
14003 Resolved an issue whereby Syslog messages were not generated for SSH login events.
14022 Corrected an issue whereby processing CDP packets which contained malformed type-length-value (TLV) tuples could potentially cause a device reset.
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.

Changes and Enhancements in 6.03.06.0008
14295 Resolved an issue which prevented accessing the device via SNMP when the management IP address was in the 172.16.0.0/16 network address range.

Changes and Enhancements in 6.03.05.0004
12472 Resolved an issue where the switch could send duplicate ICMP response packets when the source/destination IP addresses of the ICMP request were on the same routing interface and ICMP redirect was enabled.
12606 The ‘show multiauth session’ command now properly displays the session timeout value. Previously the CLI returned a zero for this field when the Termination-Action RADIUS attribute was set to RADIUS-Request.
12767 The Spanning Tree path cost value for LAG ports is now properly calculated.
12870 The ICMP unreachable packets generated by the switch will now be transmitted in the order in which received.
12900 The 'show system' command now correctly displays the system power supply status and module information.
13059 Resolved an issue which could cause loss of telnet and SSH management while the console continuously displayed ’ewsStringCopyIn: no net buffers available'. Traffic forwarding and SNMP management were unaffected.
13157 The 'clear port advertise' command now returns port settings to default values.
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.
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.
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 into 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.
13540 Resolved an issue where using SCP to transfer files from a Telnet session could cause both the local console and Telnet to hang. There was no issue transferring files with SCP from the console.
13620 The TACACS+ client session authorization settings will now be persistent across reboots.
13662 Resolved an issue with the TACACS+ session authorization where using non-default attributes for service level exec would not grant admin privileges to the user.
13860 Resolved an issue where the switch would not respond to SNMP management requests when the least significant digit of the NetSight server IP address was set to zero. Previously using the NetSight server address of x.x.x.0/255.255.252.0 would not work.
13951 Resolved a CLI display issue where the ‘show port’ command output incorrectly reported the 1000BASE-LX SFP module type as 1000BASE-SX. This was only a display issue and did not affect link operations.
14162 The WebView management application copyright date has been updated to 2010.

Changes and Enhancements in 6.03.04.0004
10874 Corrected an issue when under certain circumstances the SNTP client stopped processing requests.

Changes and Enhancements in 6.03.04.0004
11306 Resolved a CLI issue associated with save and restore of a config file which contained the “set DHCP exclude” command.
12357 Resolved an issue where multi-user-authentication failed when only one user was allowed to authenticate on a port. Previously policy was applied when the “set multiauth port numusers 2” command was issued.
12702 Resolved an issue with the “set system login” command where the CLI accepted a password preceded with an "!" but errored out when restoring it from a saved config. Previously restoring the password caused the following message, “Error: Missing value for "password" and the user was unable to login.
12813 The switch now sends a small TFTP acknowledge packet at the completion of a successful download. Previously a 512 Byte ACK was transmitted which could potentially slow down the file transfer.
12836 Resolved an issue where CDP and Cisco DP packets reported incorrect platform information.
12848 Resolved an issue where 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.
12867 Corrected an issue with the “show inlinepower” command where occasionally the CLI reported zero's for “Power (W)” and “Usage (%)”. In some cases, attached POE devices experienced loss of power and reset.
12871 DHCP snooping now works on LAGs and their underlying physical ports when configured as trusted ports.
12909 Corrected an issue with the “set length” command that could prevent the display of default routes in running config. Default routes could be displayed via the "show ip route" command.
12910 Corrected an issue where multiauth users which had successfully authenticated via dot1x and macauth lost network connectivity after their static egress was administratively removed.
12951 Resolved an LACP buffering issue which could prevent traffic flow across LAGs after some time.
12960 Resolved an issue with the “show vlan portinfo” command where the VLAN egress for dot1x clients would not appear in the output.
13111 Spanning Tree settings are now restored in proper order when loaded from a saved configuration file.
13150 Static arp entries are now preserved across device resets or when interfaces change state.
13151 Resolved a display issue with the "show lldp port remote-info" command where the “Operational Speed/Duplex/Type” field reported an incorrect value.
13176 The ifMIB module now supports the ifName object (1.3.6.1.2.1.31.1.1.1.1). Previously port link up/down traps did not include the interface name.

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

Changes and Enhancements in 6.03.03.0008
13264 Corrected an issue which resulted in momentary loss of data shortly after users MAC authenticated. This issue did not affect dot1x clients and only occurred when a user's MAC address appeared in multiple FID entries.

Changes and Enhancements in 6.03.02.0006
12793 Corrected an issue with the "show vlan static" command where the output would not display untagged egress ports.
12812 & 12941 Resolved an SSH issue where the client sent multiple access requests to the RADIUS server after the first request was already granted.
12823 Resolved a buffering issue which could cause loss of telnet and SSH management while the console continuously displayed "ewsStringCopyIn: no net buffers available". Traffic forwarding and SNMP management were unaffected.
12896 Corrected an issue where the host may stop responding to ARP requests causing loss of management (SNMP, telnet and SSH).

Changes and Enhancements in 6.03.01.0008
All new features added in this release are documented under the What's New in 6.03 section above.
Added support for the following OIDs to the CTRON-CHASSIS-MIB ctChas object: • **ctChasFNB.0** denotes the presence or absence of the FNB. • **ctChasAlarmEna.0** allows an audible alarm to be either enabled or disabled. Setting this object to disable(1) will prevent an audible alarm from being heard and will also stop the sound from a current audible alarm. Setting this object to enable(2) will allow an audible alarm to be heard and will also enable the sound from a current audible alarm, if it has previously been disabled. • **chassisAlarmState.0** denotes the current condition of the power supply fault detection circuit. The object value will read chassisNoFaultCondition(1) when the chassis is operating with no power faults detected and will read chassisFaultCondition(2) when the chassis is in a power fault condition.
12345 Corrected an issue with the LLDP application that prevented the switch from correctly displaying LLDP neighbor information advertised by a Siemens OpenStage 40 SIP phone.
9714 Corrected an issue that prevented the "clear nodealias config <port>" from clearing non-default maxentries values.
9427 An RMON alarm now triggers correctly for a rising threshold when the startup parameter is configured for "either".
9637 An RMON alarm configured for both a rising threshold and falling threshold will not continuously be triggered for the falling threshold if the traffic rates do not exceed the falling threshold.
10411 Corrected an issue that prevented the configuration and enforcement of the system lockout feature after X number of SSH attempts failed.
12293 Resolved an issue where idle management sessions failed to disconnect after the maximum idle time was reached.
12254 Resolved an issue where expired SSH sessions failed to disconnect after 60 seconds.
11817 Corrected an issue whereby clients running Windows XP SP3 and using MD5 authentication, failed to dot1x authenticate upon bootup. Subsequent authentication attempts were successful.
11876 & 12073 Resolved an issue with LLDP which could potentially prevent users from authenticating successfully when attached to the switch via an IP phone.
11890 Corrected a CLI issue where the "show config all" command erroneously displayed the STP Loop Protect status on ports as "enable" for disabled ports.
11942 Resolved an issue whereby the bufferControlTurnOnTime RMON-MIB (1.3.6.1.2.1.16.8.1.1.11) returned

Changes and Enhancements in 6.03.01.0008
an incorrect value causing the wrong date and time to be displayed.
11959 Resolved an issue associated with SSH end users whereby the switch would send a challenge request to the RADIUS server after the initial request was successfully granted.
11960 Corrected an issue associated with pasting CLI commands into the console via SSH or Telnet connections whereby pasted-in carriage return characters were ignored.
12078 Resolved an issue where the CLI displayed the Diffserv service port status as “up” when the link status was “down”.
12121 Corrected an issue whereby configuring separate RADIUS authentication and RADIUS accounting servers caused the switch to send multiple accounting request packets per authenticating user. This could cause excessive CPU loads.
12132 Resolved an issue whereby a default policy rule could prevent admin policy from being applied.
12134 Corrected a potential issue with orphaned SSH sessions that prevented the switch from properly cleaning up the connections.
12202 The output of the CLI command “show lldp port” will now display the port Id information received in the LLDPPDU from the remote device.
12209 Resolved an issue with the STP Loop Protect feature which could potentially slow down the Spanning Tree (RSTP) failover time.
12236 The “show SNTP” command now displays correct values for the latest SNTP request and update times. Previously the “Last SNTP Request” and “Last SNTP Status” outputs were out of sync with the current time.
12244 Resolved an issue with the “show dot1x auth-diag” command output whereby the “Backend Auth Fails” field was missing for some ports.
11540 Resolved a potential SNTP issue which could cause the switch to stop processing SNTP requests. Previously the state of a server which had become unavailable would show as "Not in service" after the server became available.
11588 Corrected an issue where monitoring RMON MIB statistics via an SNMP management station could potentially cause a device reset.
11649 Corrected an issue with “show policy rule admin-profile" command whereby showing policy classification rules related to a specific egress port generated the following error: Error: Missing value for "port-string".
11668 Resolved an issue where clients on a switch failed to obtain DHCP IP addresses when DHCP snooping was set on their VLAN interfaces but not globally enabled.
11681 Corrected an issue whereby applying a new policy on ports could potentially cause existing policies to be removed.
11845 Resolved an issue which prevented the MGBIC-LC01 from being hot inserted.
10981 Corrected an issue whereby terminating user sessions from Policy Manager could potentially fail for multiauth users which were authenticated via dot1x then macauth, or vice versa.
11133 Corrected an issue whereby policy applied to a GVRP enabled switch could result in the loss of management or high CPU utilization.
11338 Corrected an issue whereby the daylight savings times function would fail if the start and end times spanned across a year.
11444 Corrected an issue which prevented users from configuring VLAN membership for ports belonging to dynamic VLANs.
11566 Corrected an issue with igmpsnooping whereby if a user authenticated with dot1x and a dynamic policy was assigned, multicast traffic could cease to transmit to the authenticated port.

Changes and Enhancements in 6.03.01.0008
11584 Corrected an issue with the "show support" command which prevented the switch configuration from being displayed in its entirety.
11586 Corrected an issue with ciscoCdpMIB MIB where the cdpCacheEntry Table (1.3.6.1.4.1.9.9.23.1.2.1.1) could potentially fail to return a value.
11597 Corrected an issue with the "show config outfile" command which could prevent the backed up configuration file from being restored properly.
11865 Corrected a potential connectivity issue whereby after a device reset, auto-MIDX was not enabled on ports with auto negotiation disabled.
9260 Added support for the ctAliasProtocolTable, ctAliasMacAddressTable, and ctAliasClearAll objects to the ctAliasMib MIB. Previously, multiple entries with the same MAC address on the same port could potentially cause the IP resolution for that MAC address to fail.
11204 Corrected an issue where removing an existing DHCP Relay Agent followed by adding a DHCP server on the switch could cause the server to fail.
11324 Resolved an issue where the UDP helper function would not forward packets destined to UDP port 4011.
11342 A change has been made which eliminates the second attempt to authenticate through a RADIUS server when the first attempt (using the specific client MAC address) is rejected and the mask to be used for the second attempt is set to all “F”s.
11377 Corrected an LLDP issue where the “show neighbor” command failed to display the neighbors' host IP addresses.
11420 The DHCP snooping function has been changed to only rate limit untrusted ports when a rate limit is configured. Previously, the rate limit was applied to all trusted and untrusted ports.
10762 Resolved an issue where concurrent execution of the Enterasys-resource-utilization-mib MIB could potentially cause a reset.
10827 Corrected an issue where the “show system” command failed to display maximum temperature threshold settings.
10889 Resolved an issue where a 2-port LAG would not failover to a single port LAG when a member port was removed.
10973 Corrected an issue where oversized SSH packets potentially caused a switch reboot.
10993 & 11071 Corrected an issue where the “show config” command would not display port speeds configured via CLI or WebView.
11070 Corrected an issue where VLAN egress settings via NetSight would not persist after a reboot.
11131 The RADIUS Filter-ID attribute is no longer case sensitive for management users.
11156 & 11322 Corrected an issue where the “show mac type self” command displayed an incorrect MAC address and could potentially lockup the CLI.
11168 Corrected an issue where manually configured port speed settings were not saved in the config file. System restoration using a newly saved config file properly restored configured port speeds.
11202 Corrected an issue with DHCP snooping across LAG ports which could prevent clients MAC addresses from being added to the bindings database.
11205 & 11206 Corrected an issue where the “show vlan portinfo vlan” command failed to display member LAGs and associated port details.
11215 Resolved an issue where enabling maclock agefirstarrival would fail to remove aged-out firstarrival maclock entries.

Changes and Enhancements in 6.03.01.0008
11221 Resolved an issue with DHCP snooping which could cause the server's messages to be duplicated by the switch.
11234 Corrected an issue where user configured CDP hold time values would not to be applied. The default hold time value would be used instead.
11267 Corrected an issue where the entPhysicalSerialNum MIB (1.3.6.1.2.1.47.1.1.1.1.11) could potentially return the wrong Serial Number.
11275 Corrected an issue where only the first IGMP group join message would be processed by the switch. All additional requests would potentially be ignored.
11372 Corrected an issue where fan operational failures would not generate Syslog messages.
10274 & 10183 Corrected an issue where the first packet through the switch is dropped with policy applied, subsequent packet transmissions are successful.
10995 Corrected an issue that prevented the "switch description" field from being permanently stored in the configuration.
9842 Resolved an issue with Ciscodp where the "show neighbor" command displayed an incorrect port ID
10256 Resolved an issue where enabling port mirroring on a link would cause STP to be disabled on the port.
10704 Corrected an issue whereby running macauth and dot1x simultaneously would cause port policies to be removed.
10809 Corrected a CLI issue where restoring a config file containing an extra space before the end of line generated errors.
10816 Corrected an issue where "clear port lacp port" did not restore default port LACP settings.
10848 Changed the MST configuration name default string from the bridge MAC address to a more generic name "default".
10874 Corrected an issue when under certain circumstances the SNTP client stopped processing requests.
10906 Corrected an issue that could prevent policy configurations from being loaded by the switch.
10972 Corrected an issue which could result in the loss of SNMP management.
10061 Added a CLI prompt message to "set port vlan" informing users that setting VLAN membership for dynamic VLANs is not supported.
10521 Resolved an issue which prevented DHCP clients from obtaining IP addresses from the DHCP server.
10700 Corrected an issue which prevented the "host ip" value to be properly restored from a saved configuration file.
10056 Enhanced 802.1x authentication whereby the switch continues to send periodic Unicast Request Identity frames after the first client authenticates. Previously the switch stopped sending EAP frames after the first successful authentication.
10356 Corrected an issue where enabling port mirroring would stop traffic flow across ports that were not members of the mirror group.
10712 / 10676 Corrected an issue where default policies were removed thus preventing 802.1x clients from authenticating.
10655 Resolved an issue where client authentication failed when the management ip address was not configured.
10140 Corrected an issue with the LLDP MIB implementation that could result in the loss of SNMP management or high CPU utilization.
10396 Corrected an issue whereby after an initial invalid RADIUS request fails, subsequent valid requests were rejected for the same user due to caching of the initial RADIUS state attribute.

Changes and Enhancements in 6.03.01.0008
10551 Corrected an issue with displaying the correct LACP partner key when doing a “show port lacp port <port string> status summary” command.
10443 Corrected an issue with the “clear radius server” command that could result in a reset.
10627/10697/10250 Corrected an issue whereby disabling dot1x on an authenticated port could affect SNMP management or cause a reset.
10314 Corrected an issue where ports could fail to 802.1x authenticate valid users if mac locking was enabled.
10324 Corrected an erroneous interface message timeout reset (NIM timeout event) caused during management changes of complex interface configurations.
10554 Corrected an issue causing an SSH login to appear to hang in configurations where the motd banner and length are set.
10501 Corrected an issue where “show mac type self” command would fail to show local mac addresses.
10498 Corrected a display issue with the “show config all spantree” command caused by a page break truncating the output.
10535 Added the ability to set the PVID on a port with a VLAN learned via GVRP. A new informational message “INFO: PVID has been set. VLAN membership cannot be set on dynamic VLAN” alerts the administrator that PVID is settable on a dynamic VLAN but VLAN membership is not configurable.
10227 Corrected issue with RADIUS server redundancy which could prevent users from authenticating via the secondary server.
Corrected an issue where the port inlinepower admin state was not persistent.
Corrected an issue with persistence of port advertised capability on combo ports.
Corrected an issue with the “show mac port” command displaying output from multiple ports.
Corrected an issue where Dynamic Egress failed if a rule to discard tagged packets was applied to the port.
Enabled the ability to syslog messages greater than 124 Characters in length. Previously some messages may have been truncated.
Corrected an issue with counting RMON Statistics for 1024-1518 octet packets.
Modified the Span Guard port lockout state to disable the port if the spanguardtimeout is set to zero. This will prevent any control traffic on this port from being processed when locked.
Improved the resiliency of the host process by ensuring control traffic (e.g. BPDUs) gets higher priority during heavy traffic loads.
Modified the SNTP poll interval to be set as a power of 2 to conform to RFC1305.
Jumbo packets are now counted as errors when jumbo packets are disabled on the switch.
Corrected an issue where Policy rule counts could potentially be updated incorrectly when a rule was removed. This could have prevented new rules from being added.

KNOWN RESTRICTIONS AND LIMITATIONS

Known Issues in 6.03.17.0001
There are no new known restrictions or limitations associated with this release.

Known Issues from previous releases
Switching
COS / TOS
6660 Configuring the last two bits of the ToS field is not supported. For example, when a CoS Index is configured to set a ToS value of 255, it will result in only the value 0xFC being set in the matching packets.
Dynamic Egress
Egress assignments made to ports by using Dynamic Egress are only supported on VLANs which have been statically created.
GVRP
3532 GVRP frames are not forwarded when GVRP is disabled.
2031 The D2 switch will propagate GVRP packets containing any known VLANs. All VLANs learned via GVRP will appear in the GVRP MIBs, regardless of whether there are local users attached to those VLANs.
VLAN Tagging
VLAN ID 4094 is not supported and is reserved for other use in the system.
3410 The “set port vlan” command requires that the VLAN(s) specified when executing the command must already be preconfigured statically on the device.
A VLAN cannot be disabled via CLI and/or WebView. SNMP must be used.
Policy / Authentication
TACACS+ using single connect is configurable through the CLI but it is not supported in this release.
The D2 supports CoS-based Inbound Rate Limits for Policy Roles (profiles). Rule-based Inbound Rate Limits (IRLs) are not supported and will be ignored if configured.
Setting an extensive number of policy rules via the CLI can cause momentary loss of CLI and SNMP management.
Policies can only be assigned to ports on VLANs which have been statically created.
A role with CoS and/or PVID configured counts as an L2 rule and a mask. Multiple Roles with CoS and PVID counts only as one rule and one mask globally.
For policy roles that are set to “Deny Traffic” (e.g., Quarantine Role), ARP frames are dropped unless a policy rule explicitly permits forwarding of ARP frames.
Policy roles and rules cannot be applied to ports that are members of a link aggregation group (LAG).
2175 ARP packets are not classified based on policy IP source/destination rules.
3094 If a policy profile has cos-status enabled, only 99 rules can, be supported per policy profile.
13421 Upgrading from firmware 6.03.02 to 6.03.03 from a TACACS+ account causes a console lockup. Workaround: Upgrade from a non TACACS+ user account.
VLAN Authorization
When a VLAN tunnel is applied, traffic is egressed untagged as expected. “Show vlanauthorization” will display the correct VLAN and MAC address; however, “show vlan” and “show port egress” will not display tunnel ports.
MAC Locking
Static MAC locking a user on multiple ports is not supported.

Known Issues from previous releases
It is possible under extenuating circumstances that a violating MACLock user can dot1x authenticate on the port but all other traffic from that user will be dropped.
Statically MACLocked addresses in the Filtering Database show as “other” in the “show mac” response.
The MACLock table may show multiple entries for the same user depending upon the VLAN assignment.
RADIUS
By design, the switch does not allow the Primary and Secondary RADIUS servers to be using the same IP address.
MAC Authentication
10893 On rare occasions with authentication, there is a potential for the MAC address of a user who fails to authenticate to remain unlearned for a period of time.
In some rare cases, the command “set macauthentication portinitialize <port-string>” does not terminate mac-authenticated user sessions.
PWA
On switches that support multiauth, only one PWA authenticated user is supported per port.
Spanning Tree
The “show spantree stats active” command may erroneously display some ports as active. If a port was once active and later goes down, the system will still show the port on the “active” list.
VLAN marking of mirrored traffic – Edge only
MAC addresses will be learned for packets tagged with the mirror VLAN ID. This will prevent the ability to snoop traffic across multiple hops.
Warning: Traffic mirrored to a VLAN may contain control traffic. This may be interpreted by the downstream neighbor as legal control frames. Users should disable any protocols on inter-switch connections that might be affected (i.e., Spanning Tree).
Management
The switch can support up to two concurrent SSH client sessions.
9328 If the host IP address or the router IP interface used for management is in a zero subnet (i.e., 10.0.x.x/16), ARPs will resolve, and the host will be unable to ping devices within the subnet.
9367 ICMP packets containing the record route or timestamp options will not be forwarded by the device.
10997 When auto-negotiation is disabled on an SFP port in a D2 that has a 100Base-FX connection, the CLI will display the incorrect speed for the port and a link may not be established. **Workaround:** After auto-negotiation has been disabled, manually configure the port for 100M via the "set port speed ge.1.2.xx 100" command to establish a 100M link using 100Base-FX MGBICs.
11539 It is highly recommended that DAI be configured on edge ports only due to the potential for the DHCP snooping database to become out of sync during a system reset.
12737 When initiating a telnet session from the console of the device to another device, the telnet session will occasionally fail with the following error message: “telnet: Unable to connect to remote host: Connection timed out”. Executing the command a second time will succeed.
12329 User is unable to set port advertise speeds 10t, 10tfd, 100tx, and 100txfd on combo ports.
WebView (Web-based Management)
Configuration information for LAGs configured via WebView will not be reflected correctly when viewed via the CLI.

Known Issues from previous releases
RMON
When packets are transmitted outbound they are counted under packet sizes 64-1518 in RMON stats but not total Packets or Octets.
Enabling RMON capture on an interface will cause packets to be duplicated on the interface while the functionality is enabled.
Only RMON offset values of 1-1518 are supported.
RMON automatically creates entries for stats using indexes associated with each port. If any of the automatically created indexes are cleared and then associated with a new entry with an index less than 450, the new entries will not be persistent. Upon resetting the device, RMON will automatically create entries for each port using the initial default indexes. To avoid this situation, always use an index of 450 or greater when creating new entries.
Port counters and RMON counter may display differing values.
Packets greater than 1518 will not be counted by the IfInErrors MIB.
SFP
While the bi-directional transceivers will work in the D2, they will only be identified as “Combo RJ45/SFP”

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

For the latest copy of this release notes, go to http://www.extremenetworks.com/support/. To report an issue not listed in this document or in the **Global Knowledgebase**, contact our Technical Support Staff.

IETF STANDARDS MIB SUPPORT

RFC No.	Title
RFC 1213	MIBII
RFC 1493	Bridge MIB
RFC 2613	SMON MIB (portCopyConfig)
RFC 2819	RMON MIB
RFC 2668	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 2933	IGMP MIB
RFC 2271	SNMP Framework MIB
RFC 3413	SNMP Applications MIB
RFC 3414	SNMP Usm MIB

RFC No.	Title
RFC 3415	SNMP Vacm MIB
RFC 3584	SNMP Community MIB

EXTREME NETWORKS PRIVATE ENTERPRISE MIB SUPPORT

Title
ctbroadcast mib
ctenvironment mib
ctRatePolicing mib
ctQBridgeMIBExt mib
ctCDP mib
ctAliasMib
ctTxQArb mib
ctDownLoad mib
ctEntStateOperEnabled and ctEntStateOperDisabled
etsysRadiusAuthClientMIB
etsysRadiusAuthClientEncryptMIB
etsysPolicyProfileMIB
etsysPwaMIB
etsysSyslogClientMIB
etsysConfigurationManagementMIB
etsysMACLockingMIB
etsysSnmpPersistenceMIB
etsysMstpMIB
etsysMACAuthenticationMIB
etsysletfBridgeMibExtMIB
etsysMultiAuthMIB
etsysSntpClientMIB
etsysIeee8023LagMibExtMIB
etsysVlanAuthorizationMIB
etsysCosMIB
etsysResourceUtilizationMIB
etsysMultiUser8021xMIB
etsysTacacsClientMIB

SNMP TRAP SUPPORT

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

RADIUS ATTRIBUTES SUPPORT

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

Attribute	RFC Source
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.

APPENDIX A

Changes and Enhancement History from Previous Releases

Changes and Enhancements in 1.00.04.0001
11606 Resolved an issue with the "set port advertise" command whereby setting speed/duplex on copper ports returned the following error message: "Failure: Unable to set port speed. Advertise speed is not supported on the port".
11607 Corrected a CLI issue with the “clear port advertise” command where default settings were not restored on copper ports.
11624 Corrected a CLI display issue associated with the “set port txq” command. Previously the first 2 queue values would not be displayed when 100% of the traffic was assigned to the highest transmit queue.

Changes and Enhancements in 1.00.03.0002
Resolved an issue which prevented multicast control packets from being forwarded properly through LAG ports.
Corrected an issue in the Policy MIB where the etsysPortPolicyProfileSummaryTable (1.3.6.1.4.1.5624.1.2.6.3.3) failed to return a value for etsysPortPolicyProfileSummaryOperID.
Corrected an issue where the MIB2 ipForwarding=1.3.6.1.2.1.4.1 returned the wrong value for a switch.
Corrected an issue with RMON where packet capture over non-default VLANs only worked in one direction.

Changes and Enhancements in 1.00.03.0002
11126 Corrected a NetSight issue which potentially caused incorrect VLAN tags to be applied to ports.
The following changes were made to the temperature trip points for fan operation: • D2G124-24P – Fans turn on when Sensor 1 temperature reads ≥ 65C • D2G124-24 – Fans turn on when Sensor 1 temperature reads ≥ 69C. • Fans will continue to turn on if Sensor 2 in either model reaches 60C.

Changes and Enhancements in 1.00.02.0002
10795 Fixed a potential SNMP vulnerability identified in US-CERT VU#878004.
11027 Corrected link connectivity issues related to ports 9 and 10.

Changes and Enhancements in 1.00.01.0005
Changes have been made to licensing validation. Customers must agree to the terms defined in the licensing agreement, but now policy functionality will be unlocked simply by issuing the “set license” command. Previously, users were required to obtain a MAC-based generated key on-line.
10436 Corrected an issue where clients failed to reauthenticate after the user configured session-timeout expired.
10479 Resolved a CLI issue whereby class details for DiffServ dstmac were displayed incorrectly.
10579 Corrected an issue where CLI buffer sizes exceeding 1024 lines caused errors in the output display.
10595 Corrected a CLI issue which prevented users from enabling or disabling PoE on port ranges using wildcards.
10596 Corrected an issue where ASM was unable to apply actions to ports.
10291 Resolved an issue where clearing RMON events would cause database corruption.

Changes and Enhancements in 1.00.01.0005
10434 Corrected an issue where default policy was not being applied when maptable response was set to tunnel. This prevented traffic egress on policy ports.
10494 Corrected an issue with „Set cos port-config" whereby adding ports back into the default port group would not remove them from a cos port group.
10618/10656 Resolved an issue where CDP and CiscoDP packets contained incorrect platform information.
10497 Resolved an issue whereby changing the maptable response from tunnel to policy mode would not remove vlan egress settings.
9983 Corrected an issue where 'show inlinepower' displayed incorrect information the first time it was executed after bootup.
10414 Corrected an issue associated with the “SNMPTask" task creation sequence which caused the following error message after a „clear config": "tExcTask: memPartFree: invalid block".

Changes and Enhancements in 1.00.00.0029
Initial customer release.