Omni Switch OS6860/OS6860E

Release 8.1.1.689.R01

The following is a list of issues that have been identified and corrected in AOS software release. This document is intended to be used as a pre-upgrade guide and does not replace the Release Notes which are created for every GA release of software.

Important Notice: For a copy of software release not posted on the Web or if you have any question or concern please contact Alcatel's Technical Support Department.

Problems Fixed Between Builds 498 and 585 2
Problems Fixed Between Builds 586 and 627 5
Problems Fixed Between Builds 628 and 663 6
Problems Fixed Between Builds 663 and 664 9
Problems Fixed Between Builds 664 and 689 9
Under Verification: 10

Alcatel·Lucent Enterprise

Known Issues:.. 14
New Software Features:.. 14

Problems Fixed Between Builds 498 and 585

PR	**197280**	Build:	8.1.1.556.R01
Summary:	DHCP OFFER dropped in trusted ports		
Explanation:	DHCP offer will be forwarded even if IP interface for the client vlan in DHCP Snooping enabled switch is not configured.		

PR	**197648**	Build:	8.1.1.557.R01
Summary:	Interface gre is not the Primary Interface for vlan:5003		
Explanation:	PIM is not supported on GRE Tunnels.		

PR	**197626**	Build:	8.1.1.558.R01
Summary:	OS6860 getting errors "portmgrcmm library(plApi) error(2)"		
Explanation:	Made changes to avoid error messages during port conversion.		

PR	**197816**	Build:	8.1.1.558.R01
Summary:	"Interface ingress-bandwidth” deletion failed in AOS 8.		
Explanation:	Interface Default values will not be shown in snapshot		

PR	**198082**	Build:	8.1.1.559.R01
Summary:	Want to have a messages in swlogs for LPS port shutdown event		
Explanation:	To have swlog message whenever the port goes into shutdown state due to LPS violation.		

PR	**198092**	Build:	8.1.1.560.R01
Summary:	OS 6860 struck and no output seen for basic show commands		
Explanation:	Avoiding infinite loop while reading dhcpBind.db file.		

PR	**198929**	Build:	8.1.1.564.R01
Summary:	aaa test-radius-server server-name type authentication user user-name password password method MD5		
Explanation:	Tunnel Type Attribute is handled properly in the radCli process.		

PR **198934** Build: 8.1.1.564.R01
Summary: OS6860 tail .bash history command disclose the username/passwords
Explanation: Command line containing password will not be stored in bash history.

PR **198799** Build: 8.1.1.565.R01
Summary: OS6900 VC crashed when it looked up for mac address with invalid vid
Explanation: Same mac address with invalid vid is looked up which lead to assert failure.

PR **198999** Build: 8.1.1.565.R01
Summary: The interfaces port 1/1/1-52 link-trap command shows error message.
Explanation: link trap for 52 port can be enabled as range

PR **199150** Build: 8.1.1.565.R01
Summary: Able to enter emergency shell with Alt+b combination on OS6860 switch.
Explanation: Disable the sysrq utility in kernel

PR **198637** Build: 8.1.1.566.R01
Summary: Mac not learning on SDP interface in SPB after the reboot
Explanation: Handled sending the service configuration message to ISIS properly

PR **198935** Build: 8.1.1.567.R01
Summary: BPDU FCS is incorrect while doing packet capture.
Explanation: STP Packet size optimized to be send exact size.

PR **198765** Build: 8.1.1.568.R01
Summary: AOS6860 crashed, analysis required.
Explanation: Avoid vm_insert_page error by unmapping packets from tasks.

PR **199440** Build: 8.1.1.568.R01
Summary: Vulnerability in SSLv3 (POODLE / CVE -2014- 3566)
Explanation: Disable SSLv3 to mitigate POODLE attack

PR **199402** Build: 8.1.1.569.R01
Summary: Not able to telnet or ssh in VC of 2 6860 switches
Explanation: Modify the Captive portal hardware configuration to not drop packets in CP-IP/24 network

PR **198939** Build: 8.1.1.571.R01
Summary: Unable to display correct return attributes which configured on NPS server.
Explanation: To display correct return attributes which are configured on NPS server.

PR **199316** Build: 8.1.1.572.R01
Summary: OS6860 switch crashed with PMD after pushing the policy/Sip configuration via OV, when we do write m

Explanation:	Proper handling of Large fragmented SIP Frames		
PR	**200480**	Build:	8.1.1.574.R01
Summary:	OS6860: Not able to configure interface ALIAS using port range.		
Explanation:	Fix done to change the mipindexlength and passing input to the mipindex dynamically based on the number of ports.		
PR	**199987**	Build:	8.1.1.575.R01
Summary:	OS6860 switch with sip snooping the call is not getting recorded.		
Explanation:	TCP keep alive packets handling and out of order UDP fragments handling issue fixed		
PR	**199433**	Build:	8.1.1.575.R01
Summary:	OS6860 has generated agCmm PMD file without rebooting and configuration loss issue is seen after the		
Explanation:	Handled string copy function in a proper way		
PR	**201018**	Build:	8.1.1.578.R01
Summary:	PGM controls packets dropped by the switch		
Explanation:	Allow requeue operation for slow path packets		
PR	**201022**	Build:	8.1.1.579.R01
Summary:	OS6860 advertises itself as OS6900 in Vendor class identifier (Option 60).		
Explanation:	Vendor Class Identifier changed to "OmniSwitch-OS6860"		
PR	**191901**	Build:	8.1.1.579.R01
Summary:	OS10k switch crashed with generating PMD file.		
Explanation:	Memory leak in source learning task is corrected to free the memory appropriately.		
PR	**201088**	Build:	8.1.1.579.R01
Summary:	OS6860 switch with sip snooping the call is not getting recorded without QoS.		
Explanation:	Fixes the display issue in sip snooping active call records		
PR	**201024**	Build:	8.1.1.581.R01
Summary:	OS 6860E-P24 switch connected to the RYU controller malformed Hello packets seen		
Explanation:	Openflow Hello Packet Element Length changed		
PR	**201055**	Build:	8.1.1.582.R01
Summary:	No BPDU Captured when using command debug stp bpdu-trace show 1 all decode .		
Explanation:	Message from stpCMM to stpNi is sent with respective chassis id in a proper way		

Problems Fixed Between Builds 586 and 627

PR	**200827**	Build:	8.1.1.587.R01
Summary:	The "^" character shifted in case of "?"		
Explanation:	Corrected the issue in positioning ^ for the help condition in cli commands		

PR	**201715**	Build:	8.1.1.588.R01
Summary:	22 seconds packet drop seen when the power is removed from the master unit in VC		
Explanation:	Do not include inactive ports in graceful restart process		

PR	**201477**	Build:	8.1.1.590.R01
Summary:	OS6860: QOS user-port shutdown for bpdu is not working on Edge Ports.		
Explanation:	check if port type is VFL or not before setting flag bit for qos		

PR	**201881**	Build:	8.1.1.592.R01
Summary:	NTP Vulnerability query - CVE-2014-9293 CVE-2014-9294 CVE-2014-9295 CVE-2014-9296 CVE-2013-5211		
Explanation:	Code changes done to fix NTP vulnerabilities CVE-2014-9295 & CVE-2013-5211. Other vulnerabilities (CVE-2014-9293,CVE-2014-9294,CVE-2014-9296) do not affect AOS.		

PR	**201197**	Build:	8.1.1.594.R01
Summary:	Unable to reach the directly connected Gateway from the switch after disabling the SPB sap configuration		
Explanation:	On deleting SAP, delete vlan translation for the port only when it’s not associated with other services and SAP		

PR	**202430**	Build:	8.1.1.597.R01
Summary:	Parity error on AOS6860.		
Explanation:	Parity Error in DLB_LAG_FLOWSET and DLB_LAG_FLOWSET_TIMESTAMP_PAGE table corrected.		

PR	**202611**	Build:	8.1.1.602.R01
Summary:	OS6860 Display issue when configuring Qos policies.		
Explanation:	Corrected the display of webview in Qos tables		

PR	**203410**	Build:	8.1.1.603.R01
Summary:	OS6860: Issue with DHCP		
Explanation:	Update seconds elapsed field in Bootp payload when 6860 sends out Dhcp-discover (i.e. when it acts as dhcp-client)		

PR	**202979**	Build:	8.1.1.604.R01
Summary:	Error while configuring the interface alias with white space in the description field and shortening		
Explanation:	Fix done to handle cli when string contains spaces during auto-fill of first word		

PR **203169** Build: 8.1.1.605.R01
Summary: Switch Suddenly stopped sending out traps
Explanation: Changes has been done to close the file descriptor properly in reactor socket to avoid fd leak.

PR **203490** Build: 8.1.1.607.R01
Summary: OS6860: DHCP traffic denied on User Ports Group
Explanation: Anti-spoofing ignores packets with 0.0.0.0 as source address

PR **201854** Build: 8.1.1.608.R01
Summary: Bvlan having issues while creating on OS6860E.
Explanation: BVLAN configuration issue fixed

PR **204199** Build: 8.1.1.609.R01
Summary: Port does not move to UNP profile if the IPv6 interface is enabled on workstations
Explanation: ipv6 packets to be dropped if classification doesn’t match based on ip-rule

PR **204260** Build: 8.1.1.609.R01
Summary: In reference to PR#201854,Bvlan having issues while creating and issue with MTU becomes 1500 when we
Explanation: To assign BVLAN_DEFAULT_MTU for control bvlan when the same is created using one touch SPB.

PR **204306** Build: 8.1.1.610.R01
Summary: Out of TCAM processors message seen when switch is rebooted with Openflow config
Explanation: Open Flow configuration will use 2

PR **204970** Build: 8.1.1.624.R01
Summary: (HA-VLAN) Static ARP not programmed in slave unit.
Explanation: Configure Slave chassis for HaVlan static ARP

PR **204766** Build: 8.1.1.624.R01
Summary: Issue with traffic on SAP access ports of OS6860
Explanation: Introduced debug command to change the hash algorithm for hardware table used for vlan translation for services configured

PR **201457** Build: 8.1.1.624.R01
Summary: OS6860 SPB SAP counters are not updated properly.
Explanation: SPB statistics issue fixed

Problems Fixed Between Builds 628 and 663

PR **205156** Build: 8.1.1.628.R01

Summary:	Qos configuration changes after the reboot		
Explanation:	Qos user-ports configuration is applied properly across reboot.		
PR	**204950**	Build:	8.1.1.630.R01
Summary:	SSH Vulnerability detected with OS6860 switch.		
Explanation:	Added CLI "ssh strong-ciphers/strong-hmacs enable/disable" to enforce ssh configs persist across reboot		
PR	**204834**	Build:	8.1.1.630.R01
Summary:	Impact analysis on our products with CVE-2015-0291 t1_lib.c in OpenSSL 1.0.2.		
Explanation:	Code changes done to fix openSSL vulnerabilities CVE-2015-0287, CVE-2015-0289, CVE-2015-0292, CVE-2015-0209, CVE-2015-0288		
PR	**205244**	Build:	8.1.1.631.R01
Summary:	Buffer overflow error is seen after configuring longer string for "dn_name" and "search_base" field.		
Explanation:	Fix done to avoid Buffer Overflow in aaa module.		
PR	**205552**	Build:	8.1.1.632.R01
Summary:	OS6860 send wrong trap " New Root Bridge"		
Explanation:	STP trap generated only when root bridge changes.		
PR	**205470**	Build:	8.1.1.633.R01
Summary:	Port number does not display in swlog when a port is assigned to a vlan via UNP profile		
Explanation:	agcmm debug level changed to info to log VPA information along with user port value.		
PR	**195930**	Build:	8.1.1.635.R01
Summary:	Loopback not exported in SPB IPVPN with "ip export all-routes"		
Explanation:	Allow IPv4 Loopback0 to be route-leaked into ISIDs.		
PR	**202995**	Build:	8.1.1.636.R01
Summary:	NTP configuration is not getting applied		
Explanation:	"ntp authentication enable" command is applied last in configuration		
PR	**205911**	Build:	8.1.1.638.R01
Summary:	OS6860E-P24: NTP configuration is lost in running configuration after the switch reboot		
Explanation:	NTP configuration will be processed		
PR	**206087**	Build:	8.1.1.639.R01
Summary:	OS 6860 802.1x not working -radius access request not sent from switch.		
Explanation:	Toggling of UNP port with 802.1x enabled will be properly handled.		

PR	**206038**	Build:	8.1.1.641.R01
Summary:	OS6860: Unknown TCP ports in open.		
Explanation:	Qos Process will listen on 127.0.0.0 networks.		
PR	**206020**	Build:	8.1.1.643.R01
Summary:	OS6860 BPDU shut down is not working from time to time		
Explanation:	Send bogus BPDU(inferior STP BPDU) when link up event is triggered		
PR	**206895**	Build:	8.1.1.644.R01
Summary:	OS6860E VC Crashed		
Explanation:	Linkagg crash has been fixed.		
PR	**206468**	Build:	8.1.1.645.R01
Summary:	The POE feature does not disable on OS6860E switch after reload.		
Explanation:	Lan Power port admin disable will disable POE across reload.		
PR	**207099**	Build:	8.1.1.647.R01
Summary:	Source port number for the DNS reply packets is mentioned as 13568 instead of 53 in the Qos log		
Explanation:	TCP port number will be displayed correctly in the qos log.		
PR	**206424**	Build:	8.1.1.649.R01
Summary:	OS6860 Front LED for PS (main/backup) wrong in certain states		
Explanation:	LED will properly display the status of the Power Supply.		
PR	**206088**	Build:	8.1.1.650.R01
Summary:	Warm start trap not generated with switch OS 6860		
Explanation:	Warm Start trap will be send after bringing up the user ports.		
PR	**207089**	Build:	8.1.1.650.R01
Summary:	OS6860-P48 Swlogs Time difference issue.		
Explanation:	The Swlog time will be synced with that of the System time.		
PR	**206513**	Build:	8.1.1.651.R01
Summary:	LACP flapping seen between AOS6860 and OS10K.		
Explanation:	LACP PDU which are not intended to the Port are dropped.		
PR	**206854**	Build:	8.1.1.652.R01
Summary:	OS6860: Unknown tcp ports 2468, 12318, 34841, 35763, 39333 in open.		
Explanation:	Open TCP ports should accept connection from 127.0.0.0 network.		
PR	**208153**	Build:	8.1.1.655.R01

Summary: Issue with default route when BFD enabled after the OS6860 switch reboot.
Explanation: Static Route with BFD will not be installed if the Gateway is not reachable.

PR **208491** Build: 8.1.1.658.R01
Summary: OS6860: "ERROR: Unable to retrieve LBD snapshot"
Explanation: LBD snapshot will properly display the LBD configuration.

PR **208856** Build: 8.1.1.659.R01
Summary: OS6860 command line issue
Explanation: user password-policy cannot contain username enable command will be persistent across reboot.

Problems Fixed Between Builds 663 and 664

PR **207518** Build: 8.1.1.664.R01
Summary: Switch may hang
Explanation: In AOS 8.1.1.663.R01, a hash collision detection logic has been implemented (PR 205044) but has to be reverted as it may cause system instability under heavy hash collision condition. In very rare situation, a switch that is rebooting may hang and goes for a second reboot.

Problems Fixed Between Builds 664 and 689

PR **208949** Build: 8.1.1.664.R01
Summary: OS6860 Bad password counter is not incrementing for ssh session
Explanation: Password bad attempts counter in the show user cli will also get incremented for failed login attempt from a ssh session.

PR **208344** Build: 8.1.1.670.R01
Summary: OS6860 VLAN 1 ip interface not coming up.
Explanation: Port mirorring with unblocked vlan caused the IP interface bound to this unblocked vlan ID to remain down. Issue fixed.

PR **209237** Build: 8.1.1.671.R01
Summary: 6860-VC: UNP classification does not work when interface is reset
Explanation: Drop EAP packets on ports with 802.1x authentication disabled.

PR **209997** Build: 8.1.1.673.R01
Summary: In OS6860, configuration apply issue
Explanation: Spanning tree warning inadvertantly saved in CLI display. Fixed buffer prepares issue.

PR **208352** Build: 8.1.1.676.R01
Summary: OS6860 PXE boot is not working if we have client & server in different vlan

Explanation: Do not sent the DHCP Reply packet to UDP Relay CMM if the packet is received by IPNI for routing.

PR **210080** Build: 8.1.1.677.R01
Summary: OS6860/6900 UDLD not working when connected to OS6450. The issue is on 6450.
Explanation: Message and Timeout data in UDLD TLV corrected

PR **210462** Build: 8.1.1.679.R01
Summary: List vulnerability failed in OS6860 switch 8.1.1.663.R01
Explanation: OpenSSL package upgrade to 1.0.2d

PR **210354** Build: 8.1.1.680.R01
Summary: 6860E classifying client MAC under UNP MAC rule when UNP IP rule exists.
Explanation: Implementing a mechanism to enforce learning using L3-only packets in UNP

PR **211133** Build: 8.1.1.682.R01
Summary: kernel: [689541.680000] error writing 94 to 13, read back fffffff5/-11 ret -11 count 5
Explanation: Changed kernel log text to avoid being misinterpreted as error log

PR **211284** Build: 8.1.1.686.R01
Summary: Need to leave the debug command enabled after switch restart.
Explanation: New CLI command to enable/disable UNP learning via Layer3 Only packets

PR **210909** Build: 8.1.1.687.R01
Summary: static MAC address configuration lost after rebooting the 6860 VC
Explanation: On LPS ports, prevent conversion of static MAC to Dynamic MAC

PR **212427** Build: 8.1.1.689.R01
Summary: ICMP traffic is block due to DHCP snooping feature enabled.
Explanation: Avoid drop of ACKs for INFORM messages with client address set to 0

Under Verification:

PR **198556** Build: 8.1.1.561.R01
Summary: [TYPE1]Qos user port violation messages in a single line format in the qos log
Explanation: Qos logging for port shutdown event.

PR **197844** Build: 8.1.1.567.R01
Summary: SSH vulnerability/vulnerabilities for 10K
Explanation: CVE-2010-5107 has been fixed.

PR **199038** Build: 8.1.1.569.R01
Summary: slnHwlrnCbkHandler:662 no buffer ALERT, after mac movement
Explanation: Proper Linkagg and Default port validations are taken care

PR **200847** Build: 8.1.1.592.R01
Summary: IPRM not advertising the OSPF ECMP changes correctly to BGP.
Explanation: Checking iprm for the route exists before deleting the network route

PR **201473** Build: 8.1.1.592.R01
Summary: 6860 SPB - SAP entries not displayed in "show mac-learning domain spb" output
Explanation: Handled the length of encapVcID sent from CMM to Ni when requesting "show mac-learning domain spb"

PR **202046** Build: 8.1.1.592.R01
Summary: NTPD Vulnerability: ntpd version 4.2.7 and previous versions allow attackers to overflow several bu
Explanation: Code changes done to fix NTP vulnerabilities CVE-2014-9295 & CVE-2013-5211. Other vulnerabilities do not affect AOS.

PR **202110** Build: 8.1.1.594.R01
Summary: Security vulnerability: Port scanning test provides the information regarding the open "non-well kno
Explanation: Open port vulnerability addressed for application saaCmm and slbCmm.

PR **202371** Build: 8.1.1.600.R01
Summary: DTLS Vulnerability query - CVE-2014-3571 CVE-2015-0206
Explanation: Fixed openssl vulnerabilities CVE-2014-3571 CVE-2015-0206.

PR **203143** Build: 8.1.1.603.R01
Summary: QOS BPDU SHUTDOWN for User Ports should be able to detect loops created using a single port.
Explanation: Added mechanism to send bpdu's with inferior information on ports configured as UNP and User Ports

PR **204856** Build: 8.1.1.632.R01
Summary: When Port have violation shut down, the hardware level is still up.
Explanation: If violation occurs, BPDU shutdown in UNP port will cause the operational status of the port to be down.

PR **194737** Build: 8.1.1.637.R01
Summary: Slave chassis in the VC reloaded, without generating any PMD file.
Explanation: Print output was not stored in buffer. Fix has done for same.

PR **207868** Build: 8.1.1.652.R01
Summary: AOS7 and AOS8 TFTP files transaction.
Explanation: TFTP File transfer can be initiated through SNMP.

PR **205654** Build: 8.1.1.667.R01
Summary: OS6860-P48 MAC aging out for silent devices.

PR **208977** Build: 8.1.1.667.R01
Summary: [TYPE1]IP Phone screen going blank when uplink is disconnected.
Explanation: ifMauAutoNegCapAdvertisedBits bit order is corrected in LLDP MAC-PHY TLV

PR **209034** Build: 8.1.1.667.R01
Summary: Issue with show violation output when violation happens. Tested with restrict, discard, and shutdown
Explanation: Handle Mac-move for pseudoStatic MAC under "mac-move disable" and "LW expired" cases

---

PR **196007** Build: 8.1.1.668.R01
Summary: OS6900 OSPF point-to-point neighboring issue.
Explanation: Change to learn neighbor dynamically in OSPF Point-to-point neighbourship

---

PR **204531** Build: 8.1.1.669.R01
Summary: ARP Poison not working in OS 10K
Explanation: Learn arp from the received GARP REPLY packets

PR **197661** Build: 8.1.1.672.R01
Summary: OS6900: tx loss frames on SPB interface ports
Explanation: Tx Lost frames for the SPB Interface corrected.

PR **209841** Build: 8.1.1.674.R01
Summary: OS6860: Need clarification on STP CLI debug command.
Explanation: Ignore the STP BPDU stats for Aggregates

PR **210682** Build: 8.1.1.679.R01
Summary: This is with reference to the PR#206884 and 207218 OS6860 Lan power issue.
Explanation: Add voltage injection detection for Lanpower

PR **205044** Build: 8.1.1.681.R01
Summary: Opened in reference to PR#201462,OS6860 Hash collision issue
Explanation: Whenever a Hash Collision occurs, log message will be printed in Swlog.

PR **210386** Build: 8.1.1.681.R01
Summary: OS6900: TACACS server missing from configuration
Explanation: Changes done to update the second server IP correctly in tacacs configuration

---

PR	**210445**	Build:	8.1.1.681.R01
Summary:	Authenticated Switch Access "ERROR: Authorization failed. No functional privileges for this command.		
Explanation:	Made changes not to reset user privileges for every Refresh period		

PR	**210492**	Build:	8.1.1.682.R01
Summary:	6860-P48 issue - Device not able to connect - Parity error		
Explanation:	Implemented Third party patch to clear the parity error		

PR	**210473**	Build:	8.1.1.682.R01
Summary:	Parity Errors caused VC malfunction (chassis 2 not reachable)		
Explanation:	Implemented Third party patch to clear the parity error		

PR	**211072**	Build:	8.1.1.684.R01
Summary:	Queries on command show lan power slot 1/1 update-from		
Explanation:	remove UPDATE-FROM token from [show lanpower slot 1/1 update-from] command		

PR	**210769**	Build:	8.1.1.687.R01
Summary:	OS6860 snmp service does not respond after virtualchassis mib exploration		
Explanation:	Removed unsupported MIB tables		

PR	**211220**	Build:	8.1.1.688.R01
Summary:	OS6860: VC of 5 and no interfaces seen other than unit-1 & 5.		
Explanation:	Various VC Improvements: a) cpu queueing for VC protocol packets; b) additional logs for VC topology change; c) fix bug of false chassis deletion		

PR	**206842**	Build:	8.1.1.654.R01
Summary:	Ping loss for about 5 minutes periodically when BPDU shutdown enabled.		
Explanation:	BPDU shutdown enable will not cause ping loss.		

PR	**207850**	Build:	8.1.1.657.R01
Summary:	Some BPDU is forwarding from Linksys to uplink port. It cause the spanning tree port on core switch		
Explanation:	BPDU packets will be dropped when port is in violation.		

PR	**209835**	Build:	8.1.1.675.R01
Summary:	Query on swlogs dg_Ni library(plApi) error(2) plGetModIdFromGport@3404		
Explanation:	Dying Gasp error message enhancement in Swlog.		

PR	**209132**	Build:	8.1.1.667.R01
Summary:	AOS switch is changing the values of AVP L=38 causing the authentication issue.		
Explanation:	Changes to scan the entire AAA Challenge Response list		

PR	**192874**	Build:	8.1.1.577.R01
Summary:	Ref PR# 191901: Wrong socket structure makes infinite loop of flush events from stpNi to SlNi		
Explanation:	Source Learning and STP NI task socket connection optimized in case of reconnect after a disconnect.		

Known Issues:

PR	**211459**
Summary:	OS6860: lpNi LanNi error(2) lpNiPollTimer 2227: Bad Send lpNi LanXtr error(2) lp69xGetPowerSupplyParameter 2130: No buffer for send lanpower errors
Explanation:	Issue caused by loss of communication due to Buffer depletion. Power will still be delivered to the devices , however, show command will not display the correct status.

PR	**208784**
Summary:	Unable to save "dhcp-snooping binding 00:b0:d0:99:43:39 port 7/1/2 address 192.168.11.11 vlan 11" after reboot, the configuration is gone.
Explanation:	DHCP Binding Entries will not be persistent across reboot.

New Software Features:

1. LPS Sticky Mode

Platform: OS6860, OS6860E

Hosted AOS SW Release: 811.585.R01

LPS Sticky/Infinite learning window feature controls the maximum number of Macs that can be learned on a port (based on configuration). The LPS feature limits the number of MACs that can be learned, up to a pre-determined number, plus supports an infinite/learning time window, and provides logging and notification if a rule violation occurs.
LPS Sticky Mode Options:

- Learn-as-static: To allow an automatic conversion of the MAC addresses to static during the learning window. Mac addresses learnt as pseudo static during learning window due to no-aging option should be directly converted to static even if convert to static option is not enabled or not given manually.

- Mac-move: To allow the MAC movement for the pseudo static MAC during the learning window. If a MAC, learnt as pseudo static MAC, is seen on other port in same vlan the MAC should be allowed move to the new port and get learnt as pseudo static MAC. In this case no record or information will be maintained about the original port from where the MAC has been moved.

- Infinite learning window: To allow the configuration of all the options during the infinite learning window.

Usage:

- The two new options, mac-move and learn-as-static, shall be added into the existing command.
  ->port-security learning-window <num-of-minutes> [{ no-aging <enable|disable>} |{convert-to-static <enable | disable>} | {boot-up <enable|disable>} | ***{mac-move <enable|disable>} | {learn-as-static <enable|disable>}****]*

  By default, no-aging, convert-to-static, learn-as-static and mac-move options are disabled and boot-up option is enabled. (i.e.) when specified “port-security learning-window 1”, this is same as “port-security learning-window 1 no-aging disable convert-to-static disable learn-as-static disable mac-move disable boot-up enable”.

  User can use all, any or none of flags with “port-security learning-window <num>” command.

  The option mac-move can be enabled only if the “no-aging” option is enabled. Similarly if mac-move is enabled, we can’t disable “no-aging” option.

  Unlike 6.x behavior, the option learn-as-static is not dependent on the no-aging option. The command implementation is applicable for both sticky mode/infinite learning-windows with options.

  Convert-to-static option is not allowed to be configured with infinite learning-window .When user tries to configure, the error will be thrown.
  Static MAC’s are supported on 802.1X ports

- To display the configuration of port-security and table-entries
  ->show port-security

- To display the configuration of port-security for all ports
  ->show port-security brief

- To display the configuration of port-security learning-window
  ->show port-security learning-window

- To display the whole configuration of port-security
  ->show configuration snapshot da-unp

Examples:

```
->port-security learning-window 0
->port-security learning-window 0 no-aging enable
->port-security learning-window 0 learn-as-static enable
->port-security learning-window 0 no-aging enable learn-as-static enable
->port-security learning-window 0 no-aging enable learn-as-static enable mac-move enable
->port-security learning-window 1 no-aging enable learn-as-static enable mac-move enable
->port-security learning-window 1 no-aging disable
```

```
->port-security learning-window 1 learn-as-static disable
->port-security learning-window 1 mac-move disable
->port-security learning-window 1 mac-move disable learn-as-static disable
->port-security learning-window 1 no-aging disable learn-as-static disable mac-move disable

-> show port-security
                  Port:  1/1/3
                    Admin-State      :          ENABLED,
                    Operation Mode   :            ENABLED,
                    Max MAC bridged:                 1,
                    Trap Threshold   :           DISABLED,
                    Violation        :         RESTRICT,
                    Max MAC filtered:                 5,
                    Low MAC Range    :      00:00:00:00:00:00,
                    High MAC Range   :      ff:ff:ff:ff:ff:ff,
                    Violating MAC    :              NULL

                         MAC           VLAN      MAC TYPE        OPERATION
                  ------------------------+--------+-----------------+-----------------
                  00:00:00:00:00:01          1          static        bridging

->show port-security brief
                  Slot/                   Max      Max      Nb Macs   Nb Macs     Nb Macs     Nb Macs
                   Port      Operation Mode   Bridge   Filter   Dyn Br    Dyn Fltr    Static Br   Static Fltr
                  ----------+------------------+--------+--------+---------+-----------+-----------+------------
                     1/1/3        ENABLED       1        5       0          0         1          0
                     2/1/2        ENABLED       1        5       0          0         1          0

->show port-security learning-window
                  Learning-Window          = 3 min,
                  Convert-to-static        = DISABLE,
                  No Aging                 = ENABLE,
                  Boot Up                  = ENABLE,
                  Learn As Static          = ENABLE,
                  Mac Move                 = ENABLE,
                  Remaining Learning Window = 176 sec,

-> show configuration snapshot da-unp
                  ! DA-UNP:
                  port-security  learning-window  20  no-aging  enable  convert-to-static  enable  learn-as-static
                  enable mac-move enable
                  port-security port 1/1/3 admin-state enable
                  port-security port 2/1/2 admin-state enable
```

2. Dual Home Link Active-Active

Platforms: OS6860/OS6860E

Hosted AOS SW Release: 8.1.1.627.R01

The Dual Homed Link uses two links with a number of VLANs split between them from the common pool of vlans, in such a way that any vlan is not associated with both of the redundant links at the same time to avoid formation of loops and also VLANs are still connected to the core when one link fails. STP is disabled on both the DHL links implicitly.

There is only one DHL session per switch and the DHL session contains two links namely linkA and linkB. The administrator has to configure the vlans on the links which will become DHL links, in such a way that at least one vlan has both the DHL links as members and these vlans are treated as common pool of vlans. From the common pool of vlans, the administrator can decide on the vlans that will operate on each DHL link as per the need and unless administrator specifies the vlans that operate on linkB, all the vlans will operate on linkA only. Also the common vlans will be treated as protected Vlans and the un common vlans where only one DHL link is a member of a vlan but not both will be treated as un protected vlan. When the DHL session is active, traffic is forwarded on the DHL links on protected Vlans but not on un protected vlan.

When a physical link that is part of the DHL fails or is brought down, software will modify the VLAN memberships and forwarding values according of the remaining port so that the VLANs of the link whose primary port was just lost will remain connected to the core. When a failed link is brought up, a recovery delay timer may be used to delay the switchover of the resumption of traffic for the DHL who’s primary port it was that recovered. The two core devices being uplinked to should be static members of all VLANs in both groups on both ports.

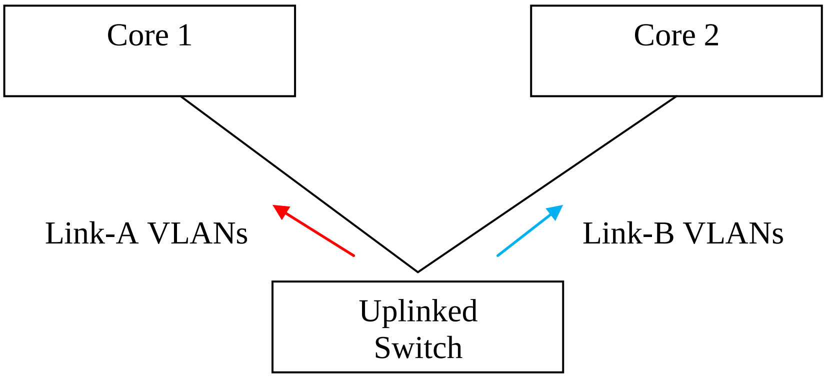

Figure 1: DHL normal state

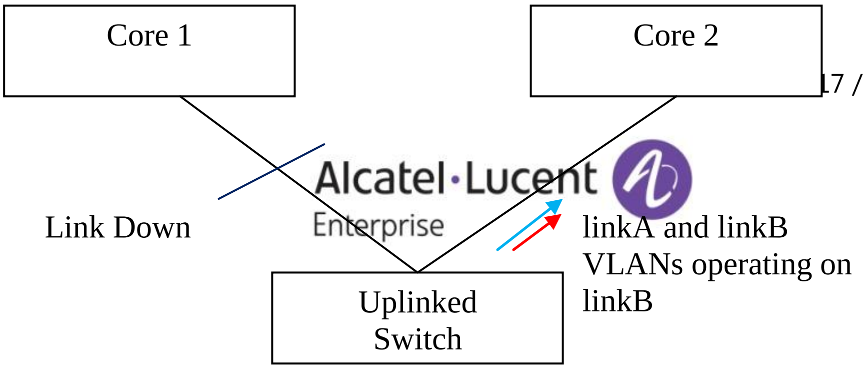

Figure 2: DHL failover state

Usage:

1) This command is used to configure DHL session

   dhl <dhl_num> [name <string>]

   Example: - dhl 123 new

2) This command is used to enable/disable DHL

   dhl <dhl_num> admin-state {<enable>|*<disable>}*

   Example: - dhl 123 admin-state enable

3) This command is used to link port to DHL

   dhl <dhl_num> linkA { port <slot/port> | *linkagg <aggid>} linkB { port <slot/port >*| *linkagg <aggid>}*

   Example :- dhl 123 linkA linkagg 50 linkB linkagg 60

4) This command is used to map VLAN on linkb and have both links active on configured VLANs.

   dhl <dhl_num> vlan-map linkB {<vlan> | *<vlan-vlan>}*

   Example: - dhl 123 vlan-map linkB 10

5) This command is used to configure mac flushing technique

   dhl <dhl_num> mac-flushing {<none> | *<raw>* | *<mvrp>}*

   Example: - dhl 123 mac-flushing raw

6) This command is used to configure preemption time

   dhl <dhl_num> pre-emption-time <dhl_num>

   Example: - dhl 123 pre-emption-time 70

Sample Configuration

```
-> dhl 123
-> dhl 123 name new
-> dhl 123 linka port 1/1/49 linkb port 1/1/51
-> dhl 123 vlan-map linkb 21-26
-> dhl 123 admin-state enable
-> show dhl
Legends:  PE - Pre-Emption
 Session           Session               Admin   Oper     PE      MAC        Active MAC
   ID                Name               State   State   Time   Flushing     Flushing
                                                (sec)  Technique    Technique
----------+--------------------------------+-------+------+-------+----------+--------------
      123                          new     up     up     30      none         none

Total number of sessions configured = 1

-> show dhl 123
DHL session name       : new
  Admin state                : up
  Operational state        : up
  Pre-emption time(sec)   : 30
  Mac Flushing             : none
  Active MAC flushing     : none
  LinkB Vlan Map          : 21-26
  Protected Vlans         : 1, 11-26
    LinkA:
      Port                   : 1/1/49
      Operational State     : up
      Unprotected Vlans     : none
      Active  Vlans         : 1, 11-20
    LinkB:
      Port                   : 1/1/51
      Operational State     : up
      Unprotected Vlans     : none
      Active  Vlans         : 21-26
```

Limitations:

- Maximum of one DHL session can be created per switch.
- DHL and the following features will operate independently of each other and DHL will not try to move the configuration from one DHL port to the other DHL port.
  - Static MAC address
  - Static multicast MAC address, Static multicast groups, multicast max group per port
  - Policy rules using source port condition
  - Port mirroring
  - Source learning
  - Havlan

- A port configured as DHL link cannot be configured for linkagg
- DHL ports cannot not be configured as UNI or VPLS access ports but DHL ports can be connected to VPLS access ports.

- DHCP snooping must be independent of DHL. User is advised not to enable DHCP snooping for DHL port as it is not needed on uplink port. .
- The Edge features AAA, learned port security, link OAM and group mobility should not be configured on DHL ports.
- DHL convergence is sub 50ms only for Fiber ports (OS6860E U/OS6860 U), same NI and a maximum of 16 VLANs and may differ for other scenarios.
- DHL ports should not be part of ERP ring.
- Two different default vlans for the DHL links cannot be configured.
- Configuration of vlan as default on one link and the same vlan as tagged on other link should not be done. For example consider the below configuration scenario

linkA		linkB
vlan 200	default vlan	tagged vlan
vlan 100	tagged vlan	default vlan

In the above scenario if an untagged packet has to go out on linkB, the vlan classified will be 100 and assume the core has default vlan 200 and it can reach linkA on default vlan 200 and hence it can form a loop.

- When the DHL links are changed on the fly, the user is advised to follow the below procedure to automatically kick in the mac-flushing technique to avoid state-mac issue.

. 1) admin disable/link down the link first that is going to be replaced
2) add the new link to DHL session in admin disabled/link down state
3) enable the link that is added to DHL session

In the above process at step 1 and step 3 the VLANs are moved across the links and mac-flushing mechanism will kick in.

3. Interface Violation Recovery

Platforms: OS6860/OS6860E

Hosted AOS SW Release: 811.627.R01

In the earlier solution, once a port is shut down by an application, unless the application clears the violation, the port remains down and will require a user to manually clear the violation for the port to have a chance to come up again. Interface Violation Recovery mechanism to be implemented to try to automatically clear the violation.

Interface violation recovery enhancement will provide the following functionalities:

- Ability to configure the recovery timer on per port or global basis.

- Ability to configure the maximum number of recovery retry on per port and global basis. If Maximum recoveries are reached, the port will be permanently shut down. A port can also be configured to enable infinite recovery retry.

- If enabled, violation SNMP Trap is sent every time an interface is shut down by a feature. When Recovery SNMP Trap is enabled, SNMP Trap must be generated for every method used to recover the port with an indication of how the port was recovered.

Usage :

1) This command is used to configure globally the maximum number of recovery retry before the port is permanently shut down.

violation recovery-maximum {infinite | *<(0-50)>}*

Example: violation recovery-maximum 12

2) This command is used to configure the per port maximum number of recovery retry used in auto recovery before the port is permanently shut down.

violation {<chassis/slot/port | *[-port2]>* | *<slot>} recovery-maximum {infinite* |*default* |*<0-50>}*

Example: violation 1/1/1 recovery-maximum 12

3) This command is used to configure globally the maximum retry time

violation recovery-time <30-600>

Example: violation recovery-time 40

4) This command is used to configure per port recovery time where recovery is re-activated automatically, if it has been shut down by any feature/application.

violation {<chassis/slot/port | *[-port2]>* | *<slot>} recovery-time {default* | *<30-600>}*

5) This command is used to show the global recovery maximum, trap enable/disable and recovery time

show violation-recovery-configuration {<chassis/slot/port | *[-port2]>* | *<slot>}*

6) This command is used to show the runtime violation status, violation source, recovery time and maximum recovery attempts for the specified port(s).

show violation {<chassis/slot/port | *[-port2]>* | *<slot>}*

Limitations:

- Violation Recovery Mechanism shall not be supported on link aggregates but on the member ports of aggregate instead.
- During VC-takeover violated ports in old primary would be listed even when NI is down
- Port Violation cannot be applied
  - When, a port is already in permanent shutdown state.
  - When a port is already shut down by a feature (shutdown reason).
  - When a port is not operationally UP

4. MIB Addition for bits per second

Platforms: OS6860, OS6860E

Hosted AOS SW Release: 811.627.R01

In CLI, InBits/s and OutBits/s on a particular port can be viewed by issuing the command "show interfaces counters". But there is no such OID to view the same in snmp. So added new MIBs to check the number of bits transmitted or received per second in a particular port.

The MIB details are as below:
inBitsPerSec - "The average number of Bits Received per second"
outBitsPerSec - "The average number of Bits Transmitted per second"

MIB objects inBitsPerSec and outBitsPerSec for the interfaceBitsTable which is an expansion of ifEntry.

Added SNMP Object Identifiers:

interfaceBitsTable: 1.3.6.1.4.1.6486.801.1.2.1.5.1.1.7.1
inBitsPerSec: 1.3.6.1.4.1.6486.801.1.2.1.5.1.1.7.1.1.1
outBitsPerSec: 1.3.6.1.4.1.6486.801.1.2.1.5.1.1.7.1.1.2

Limitations:

None

5.SNMPv3 auth password and privacy password differently

Platforms: OS6860, OS6860E

Hosted AOS SW Release: 811.688.R01

Introduction:

The existing AOS implementation supports SNMPv3 users with both hashing and encryption such as SHA+DES/MD5+DES/SHA+AES. However, in the existing implementation only one password is supported which is used for both authentication and encryption. This enhancement is to provide support for separate Auth Key and Priv Key. To support two different passwords, a new option ***priv-password*** has been added to the existing user creation CLI.

CLI Usage:
user username [password password] [expiration {day | date}] [read-only | read-write [families... | domains...| all | none]] [no snmp | no auth | sha | md5 | sha+des | md5+des | sha+aes]**[priv-password password]** [console-only {enable | disable}]

Usage Guidelines

- The priv-password token is be accepted only when SNMP level with encryption is configured for the user. If SNMP level with encryption is not selected and priv-password is configured, then CLI command is rejected with error.
- If priv-password is not configured for the user with encryption SNMP level, then user “password” parameter is used for priv-password (both for authentication/encryption).
- Minimum length of the priv-password is 8 and maximum length for priv-password is 30 characters.
- Password policy is not applicable for the new optional parameter “priv-password”.
- Existing password is still used for authenticating switch access through other methods such as telnet, ftp, ssh etc.
- When the SNMP level for an existing user with priv-password configured is changed from one encryption level to another encryption level , then the previously configured priv-password will not be used with the new SNMP level. Priv-password needs to be configured again when SNMP level is changed for an existing user.

Examples:

```
-> user snmpv3user password pass1pass1 priv-password priv1priv1 read-write all
sha+aes

-> show user snmpv3user
User name = snmpv3user,
Password allow to be modified date = None,
Account lockout = None,
Password bad attempts = 0,
Read Only for domains = None,
Read/Write for domains = All ,
Snmp allowed = YES,
Snmp authentication = SHA,
Snmp encryption = AES
Console-Only = Disabled
```

MIB Objects
aaaUserTable
aaauSnmpPrivPassword

LDAP

To support separate Auth Key and Priv Key through LDAP, two new attributes **bop-md5privkey** & **bop-shaprivkey** have been added to existing LDAP schema. If the LDAP server returns these two new attributes for users with SNMP level SHA+DES/MD5+DES or SHA+AES the switch will them for the encryption key. If the LDAP server returns a user with SNMP level SHA+DES/MD5+DES or SHA+AES without these attributes the switch will continue to use the existing auth key(bop**_md5key** & **bop_shakey**) for both authentication and encryption..

6. UNP Classification Rules Enhancement

Platform: OS6860, OS6860E

Hosted AOS SW Release: 811.686.R01

On an UNP Port, any first packet received from an unknown user is used for learning. If there are any IP-based UNP Classification rules configured on the switch, but the first packet received from the user doesn't carry IP-Address Information, UNP won't use IP-Based rule for learning the MAC. Instead the MAC would be attempted for learning using any other means as per the UNP configurations on the port. Post learning an user MAC on the UNP port, even if an IP-based packet from the user is received on the port, the user won't be attempted for re-learning using the IP-based classification rules configured on the switch.

In order to facilitate an user to be learnt on UNP Port through its IP packets only using any of the IP-based UNP classification rules configured on the switch, a new global mode "force-l3-learning" for UNP is introduced. Once this mode is enabled, only IP packets from the users are used for learning an user provided atleast one of the following IP-based UNP classification rules exist on the switch:

1. IP Rule,
2. IP + Port Rule,
3. IP + Group-ID Rule,
4. IP + Port + Group-ID Rule,
5. IP + MAC + Port Rule,
6. IP + MAC + Group-ID Rule, and
7. Extended Rule using IP condition

Note that once "force-l3-learning" mode is enabled and any one IP-based classification rule exists, the following behavior would be enforced on receiving the traffic from an user-

1. If the first packet falls under any of the following category, it would be dropped in software and won't be used for learning:
   a. L2 frames
   b. Invalid ARP/GARP request/reply – one with sender IP: 0.0.0.0 or 169.254.0.0/16
   c. IP Packet with src-ip 0.0.0.0, except for DHCP packets with srcIP=0.0.0.0

2. If the first packet is any of the following packet, they would be used for learning

a. An IP packet with non-zero src-IP
b. A Valid ARP/GARP request/reply
c. DHCP packets, even if the src-IP is 0.0.0.0

This new global mode “force-l3-learning” could be enabled on the switch in any of the following ways:

1. As debug only
2. As an UNP configuration which can be saved into config file and retained across reboots.

Usage:

1. **As Debug Only:** If this mode is used, the configuration can be saved into config file, and wont be available across reboots. This is meant for debugging.

   a) CLI:
   -> debug unp force-l3-learning {ENABLE | DISABLE}

   Where,
   • ENABLE: To activate the mode
   • DISABLE: To use normal mode, where MAC learning would happen using any first packet received from a user on UNP Port
   • By default, this mode will be set to “DISABLE”

2. **As an UNP Config:** This UNP configuration could be saved in config file and would be persistent across switch reboots.

   a) CLI:
   -> unp force-l3-learning {ENABLE | DISABLE}

   Where,
   • ENABLE: To activate the mode
   • DISABLE: To use normal mode, where MAC learning would happen using any first packet received from a user on UNP Port
   • By default, this mode will be set to “DISABLE”

   b) SHOW:

- To display the configured mode :

```
-> show unp global configuration

Mode : Edge
  Auth Server Down UNP              = -,
  Auth Server Down Timeout          = 60,
  Redirect Port Bounce              = Enabled,
  Redirect Pause Timer              = -
  Redirect http proxy-port          = 8080
  Redirect Server IP                = -
  Allowed IP                        = -
  Force L3-Learning              = Enabled
```

- To display the mode in configuration snapshot

```
-> show configuration snapshot da-unp
! DA-UNP:
unp edge-profile abc
unp vlan-mapping edge-profile abc vlan 10
unp force-l3-learning enable
unp port 1/1/11 port-type edge
unp port 1/1/11 default-edge-profile abc
unp classification ip-address 10.0.0.1 mask 255.0.0.0 edge-profile abc
```