Omni Switch 6250/ 6450

Release 6.6.4.309.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.

Alcatel·Lucent
Enterprise

Problems Fixed Between Builds 178 and 192

PR	**182150**	Build:	6.6.4.181.R01
Summary:	Inconsistent QoS Manager when programming egress policy rules		
Explanation:	Error will not be thrown when the order of configuring the egress policy rules are changed.		

PR	**182388**	Build:	6.6.4.188.R01
Summary:	Unable to save ipmvlan-config on port		
Explanation:	MIP Overflow is handled properly for e-service ipmvlan commands		

Problems Fixed Between Builds 193 and 208

PR	**183151**	Build:	6.6.4.194.R01
Summary:	simple ping from the WLAN controller console to the OS6250/6450 is only 20% successful however from		
Explanation:	Checksum is calculated properly for an ICMP packet received from different vendors.		

PR	**183629**	Build:	6.6.4.196.R01
Summary:	unable to create QOS Rule with Register profile		
Explanation:	QoS Port nested command with register keyword is handled properly		

PR	**182715**	Build:	6.6.4.200.R01
Summary:	OS6450 will enable authentication even when we use wrong password/correct username is entered at cli		
Explanation:	Authentication will be successful only when the correct password is entered.		

PR	**182659**	Build:	6.6.4.201.R01
Summary:	Tacacs+ security issue with OmniSwitch.		
Explanation:	Tacacs Authorization replies will be processed in order with the help of unique reference for each transaction which will avoid security issue due to stale replies.		

PR	**184123**	Build:	6.6.4.203.R01
Summary:	Fan not running all the time on secondary & other units with RunFanAtFullSpeed flag.		
Explanation:	On Boot up of the stack "RunFanAtFullSpeed" value from AlcatelDebug.cfg will be sent to all units of stack which are operational.		

Problems Fixed Between Builds 209 and 221

PR	**183277**	Build:	6.6.4.210.R01
Summary:	Issue with Command::ethernet-service nni 1/10 tpid 0x88a8.		
Explanation:	Fix done to change the tpid on nni port based on the configuration made for the tpid either 8100 or 88a8.		

PR	**186960**	Build:	6.6.4.213.R01
Summary:	OS6450 is the client sending DHCP decline to the server.		
Explanation:	Do not send dhcp decline if stored ip address and received ip address are same if multiple ack's are received.		

PR	**186300**	Build:	6.6.4.213.R01
Summary:	Show fan output not giving the exact status of the fan.		
Explanation:	Fix done to show proper running FAN status for OS6450		

PR	**187706**	Build:	6.6.4.216.R01
Summary:	Group Mobility not working correctly.		
Explanation:	To check if the VLAN has been configured properly or not before creating VLAN		

PR	**187156**	Build:	6.6.4.216.R01
Summary:	Malformed BPDU (wrong length) for default VLAN in XNI modules- BPDU dropped in firewall		
Explanation:	Added a control variable to set the BPDU length on 10Gig ports ,to force the length field of the BPDU to be equal the standard length 39.		

PR	**188429**	Build:	6.6.4.219.R01
Summary:	LLDP management addresses issue with OS6450 switch and unable to change the Management address.		
Explanation:	To correctly update the LLDP local management address on LoopBack0 interface deletion .		

Problems Fixed Between Builds 222 and 244

PR	**188451**	Build:	6.6.4.222.R01
Summary:	Switch got crash again with Mozilla Firefox(25.0.1) when we FTP the switch.		
Explanation:	Provided defensive mechanism to avoid crash		

PR	**183025**	Build:	6.6.4.222.R01
Summary:	Unknown policy issue with 802.1x Authentication		
Explanation:	Changes done to resend the client MAC , if stuck in unknown policy during auth process due to bulk authentication and IPC congestion.		

PR **189170** Build: 6.6.4.223.R01
Summary: Gbic "type" information missing in the Inventory in OV for 6450 & 6850E
Explanation: Changes are done to display GBIC type information in OV.

PR **190330** Build: 6.6.4.225.R01
Summary: Port goes to shut down after learned the first Mac-address
Explanation: Add a MAC as filter on an LPS port, if it is blocked by 802.1x (provided port is a 802.1x+LPS port)

PR **190741** Build: 6.6.4.225.R01
Summary: +++ slc_lpsDisablePort[1162] LPS IN INCONSISTANT STATE STOP TESTING
Explanation: Before sending LPS configurations to NI , validate if the NI is in UP state . Send configurations only to UNIs.

PR **190680** Build: 6.6.4.225.R01
Summary: Specific "system contact" command raises boot.cfg.1.err on next reboot
Explanation: Changes have been made to store string in boot.cfg in double quotes irrespective of special symbols (',' '?' '!' , which will consider as delimiter)

PR **190576** Build: 6.6.4.225.R01
Summary: ip helper dhcp-snooping option-82 command not saved in boot.cfg
Explanation: error will be thrown if dhcp-snooping related configurations are done before enabling snooping

PR **190532** Build: 6.6.4.226.R01
Summary: OS 6450 DHL issue with the 802.1q vlan
Explanation: Code changes done so that adding a new tagged VLAN to a DHL port does not affect the traffic on the default VLAN.

PR **191088** Build: 6.6.4.227.R01
Summary: 6.6.4.R01 Qos Error (13) messages
Explanation: The error messages during init are handled properly, and won’t display.

PR **190930** Build: 6.6.4.227.R01
Summary: Port s was not going to permanent shutdown after the maximum number of violation.
Explanation: Port moves to permanent shutdown state after maximum number
of recoveries configured.

PR **191947** Build: 6.6.4.233.R01
Summary: OS6450 crashed with tCsCSMtask2, tCS_PRB and Vrrp tasks suspended.
Explanation: Defensive check added in order to avoid crash because of invalid memory access.

PR	**189885**	Build:	6.6.4.236.R01
Summary:	PVST+: Two root ports if linkagg are on different NIs		
Explanation:	STP will converge with PVST+ when linkaggs are configured across NI's.		

PR	**191915**	Build:	6.6.4.236.R01
Summary:	IPMVLAN nic error down(605) bcd_ipms_routing_down(0, 250)		
Explanation:	Multicast status for per vlan is enabled in HW during NI init.		

PR	**192313**	Build:	6.6.4.237.R01
Summary:	OS6450 crashes if SSH username and password are set to more than 64 characters.		
Explanation:	Check has introduced if Username or Password is greater than 64 character then return without login.		

PR	**193137**	Build:	6.6.4.238.R01
Summary:	Clarification in Allowing only ping and trace route access to particular user		
Explanation:	Ping and Trace route Support for read only users		

PR	**182755**	Build:	6.6.4.238.R01
Summary:	OV traps seen Vs switch logs events discrepancies.		
Explanation:	Rectifying discrepancy of timestamp between OV and the switch.		

PR	**192803**	Build:	6.6.4.238.R01
Summary:	OS6450/OS6900 mac address is not learning for VLAN 1(tagged) (reference PR#191087)		
Explanation:	Stop deleting vlan 1 from linkagg port if vlan 1 is a tag vlan on that port.		

PR	**192738**	Build:	6.6.4.241.R01
Summary:	Switch crashed with the suspension of the task "RADIUS Cli" and throws the error " exception handler: ex		
Explanation:	Do not process if message size is greater than the infrastructure capability		

PR	**193332**	Build:	6.6.4.242.R01
Summary:	OS6450 issue with multicast streaming		
Explanation:	Lag in Ip multicast convergence, when one client sends leave group(If only two flows is present in it) in IPMVLAN is rectified.		

Problems Fixed Between Builds 245 and 268

PR	**190933**	Build:	6.6.4.245.R01
Summary:	"Server not reachable" message filled in the SWLOGS		
Explanation:	Server not reachable messages will not be printed in SWLOG when server is responding for accounting packets.		

PR	**194446**	Build:	6.6.4.247.R01
Summary:	Appearing Error Message while changing the admin password in web view mode. Submission failed.		
Explanation:	Fix done to avoid Error Message while changing the admin password in web view mode.		

PR	**194549**	Build:	6.6.4.247.R01
Summary:	"ip helper dhcp-snooping bypass option-82-check enable" is lost after a reload		
Explanation:	Added "ip helper dhcp-snooping bypass option-82-check enable" cli after dhcp snooping enable/disable in snapshot		

PR	**193178**	Build:	6.6.4.249.R01
Summary:	OS6450 switches loosing connectivity randomly.		
Explanation:	Do not update the port based on ARP request packets		

PR	**192812**	Build:	6.6.4.251.R01
Summary:	Flood rate limit is not limiting the broadcast packets.		
Explanation:	ARP Broadcast storm is not controlled.		

PR	**194646**	Build:	6.6.4.251.R01
Summary:	Multiple issues with DHCP Snooping and IP helper		
Explanation:	If dhcp offer packet is received in client vlan by a relay agent, it will be dropped. In this specific customer scenario, since the gateway is made another switch instead of relay agent, offer packet is routed by that switch and sent to relay agent in client vlan. As a work around for this scenario, if allowRoutedReplyOnClientPort is set to 1 , offer packet will not dropped if it is received on client vlan.		

PR	**194702**	Build:	6.6.4.253.R01
Summary:	QoS policy list "egress" delete/disable issue.		
Explanation:	Disable/Delete particular list works fine.		

PR	**195688**	Build:	6.6.4.254.R01
Summary:	show configuration snapshot gives no output and error message returned from mip_msg_forward.		
Explanation:	Buffer freed during failure condition		

PR	**195208**	Build:	6.6.4.254.R01
Summary:	NI 3 stack got crashed		
Explanation:	Added more debug logs to isolate the root cause of the NOL crash		

PR	**196011**	Build:	6.6.4.254.R01
Summary:	test-oam display results inconsistent in "show" commands.		
Explanation:	Fix done to show the consistent throughput value for the test-oam statistics command.		

PR **194326** Build: 6.6.4.255.R01
Summary: I2C_do_transaction: i2cread get fail! tmp_len[20] errors filled in SWLOGS
Explanation: Code changes have been made to check GBIC presence before reading SFP's EEPROM during boot up.

PR **194561** Build: 6.6.4.255.R01
Summary: CP user mac-addresses are not learnt however authentication is successful.
Explanation: Fix done to add the captive portal authenticated mac addresses in the mac address table.

PR **195139** Build: 6.6.4.257.R01
Summary: Fan 2 in an OS6450 is not monitored.
Explanation: Commenting the Trap, because not running fans are considered as not present as per the current design.

PR **196127** Build: 6.6.4.257.R01
Summary: OS6250 policy based port mirroring issue
Explanation: Policy mirroring works fine across different slots.

PR **197152** Build: 6.6.4.260.R01
Summary: OS6250-P24 Link trap not appearing on console
Explanation: Fix done to display the interface's link trap on the console by enabling the trap

PR **197065** Build: 6.6.4.262.R01
Summary: Arp not getting learn in directly connected 802.1x non-supplicant device.
Explanation: Wrong vlan classification on mobile ports due to stale entry in vlan_mac table is fixed.

PR **188806** Build: 6.6.4.262.R01
Summary: No IP connectivity after removing a VLAN from protected VLAN list in an ERP ring
Explanation: Deletion of protected vlan in flat mode doesn’t t change STP status of the erp ports in other protected to blocking

PR **196244** Build: 6.6.4.262.R01
Summary: OS6450: showing incorrect input transceiver value.
Explanation: Changes have been made to display the Actual Input Power value when there is no fiber link connected on SFP and also when link status changes from UP to down

PR **197797** Build: 6.6.4.264.R01
Summary: [TYPE1] Getting the error message "Out of TCAM processors on 1/0(0)Out of TCAM processors on 1/0(0)"
Explanation: Out of TCAM processors Error wont be thrown if TCAM is available

Problems Fixed Between Builds 269 and 285

PR	**197245**	Build:	6.6.4.269.R01
Summary:	[TYPE1] OS6450 error: Unknown uport 50 in the slot 1 with gport 3		
Explanation:	Fix done to avoid invalid error message.		

PR	**197528**	Build:	6.6.4.269.R01
Summary:	Customer Need a Show command for TACACS server status		
Explanation:	Fix done to display the server status (up/down) of all configured tacacs servers in the setup.		

PR	**198019**	Build:	6.6.4.271.R01
Summary:	[TYPE1]OS6250 Switch stack of 4 Units-Crash Analysis-tNetTask (f8e2a98) @ 50 SUSPEND		
Explanation:	Reduce severity level of halTestTrace to avoid memory corruption		

PR	**194636**	Build:	6.6.4.272.R01
Summary:	OS9000E-synchronization issue after issuing the "interfaces clear-violation-all" command in AoS 6.4.		
Explanation:	Modified the behavior of show configuration status to sync with cmm configuration status		

PR	**198851**	Build:	6.6.4.272.R01
Summary:	Unable to configure dhcp snooping source filter on mobile port		
Explanation:	Allowed to configure the ISF on mobile port when the port is not in forward state.		

PR	**198943**	Build:	6.6.4.272.R01
Summary:	[TYPE1] OS6450 switch send DHCP decline to the server		
Explanation:	Switch won t send DHCP decline if switch s IP address (My IP address) is same as Your IP address or Client IP address in the acknowledgement packet.		

PR	**198717**	Build:	6.6.4.272.R01
Summary:	OS6450 Switch Stack Reboot Analysis-Due to taNiEsmDrv task-Continuous crash.		
Explanation:	Code changes done to avoid possible memory corruption in HAL module		

PR	**200070**	Build:	6.6.4.274.R01
Summary:	status of the running configuration in show running-directory is not changed after lan power		
Explanation:	Running configuration status is changed accordingly when the lan power is configured		

PR	**199583**	Build:	6.6.4.274.R01
Summary:	OS6450 is only filtering the bpdu and not shutting down the port.		
Explanation:	In Qos User Port option shutdown will take precedence over option filter when		

configured for bpdu

PR	**200124**	Build:	6.6.4.277.R01
Summary:	Problem with command "ip managed-interface" after reload.		
Explanation:	IP managed-interface configuration remains the same after the reload		

PR	**200569**	Build:	6.6.4.277.R01
Summary:	OS6250 Dhcp server cannot assign ip and need reload 3x6250 stack switch for DHCP to work.		
Explanation:	Memleak/IPC pool depletion is fixed. DHCP client gets IP from DHCP server		

PR	**200346**	Build:	6.6.4.280.R01
Summary:	High CPU seen while snmp walk towards a OS6450-P48 whose uplink is connected to SFP/SFP+ port.		
Explanation:	Code changes to handle properly for the SPF ports to avoid looping during snmp walk.		

PR	**201472**	Build:	6.6.4.280.R01
Summary:	SNMP snmp object for the captive-portal pass-through..		
Explanation:	Code changes done to access the captive-portal pass-through from the snmp object		

PR	**201146**	Build:	6.6.4.280.R01
Summary:	OS6450 unable to rrm the ktrace file		
Explanation:	Code changes are done by using an array of size that can hold maximum filename length including pathname.		

Problems Fixed Between Builds 286 and 309

PR	**201092**	Build:	6.6.4.286.R01
Summary:	Unit 4 in the stack of 5 switches has crashed numerous times.		
Explanation:	Qds efp buff is released upon performing shutdown/filter action is performed on pvst frame.		

PR	**201347**	Build:	6.6.4.286.R01
Summary:	OS6250 Power supply type display issue		
Explanation:	Fix done to show proper power supply type details		

PR	**202449**	Build:	6.6.4.289.R01
Summary:	OS6250: Switch crashing continuously with boot.cfg		
Explanation:	Code changes done to accept the vlan description of length 32 characters.		

PR	**202675**	Build:	6.6.4.290.R01
Summary:	3xOS6450 stack does not synchronize and Write memory does not work		
Explanation:	Handle MIP OVERFLOW for SSAPP		

PR	**202629**	Build:	6.6.4.290.R01
Summary:	6XOS6450: On switch ports receiving invalid LBD packets.		
Explanation:	Enabled the systrace logging for the error messages in case of errors encountered for Invalid LBD packets.		

PR	**203548**	Build:	6.6.4.291.R01
Summary:	OS6450 wrong linkagg port details in "MAC address is full" message		
Explanation:	Code changes done to log the mac-address-table full message properly for the linkagg.		

PR	**203353**	Build:	6.6.4.294.R01
Summary:	OS6450 switch crashed with ktrace file.		
Explanation:	Semaphore implementation to restrict the simultaneous access to MAC control block for loop avoidance		

PR	**203703**	Build:	6.6.4.295.R01
Summary:	IP based vlan classification rule (mobile VLAN) is not working in 6.6.4.285.R01		
Explanation:	Avoid svlan cvlan mapping check for AAA and mobile ports		

PR	**200402**	Build:	6.6.4.295.R01
Summary:	On OS6450 stack getting error: hal_qos_read_block_counter:89: operation on non-initialized application		
Explanation:	Qos Rules with Port group split mode is validated properly in the Qos CMM		

PR	**204101**	Build:	6.6.4.296.R01
Summary:	OS6250 Power supply type display issue		
Explanation:	Fix done to show proper power supply status for OS6250 switches.		

PR	**202977**	Build:	6.6.4.296.R01
Summary:	OV 411 not receiving Link notification traps		
Explanation:	Fix done to send traps out of the switch when the switch was reloaded with no aaa authentication and later configured with aaa authentication.		

PR	**204237**	Build:	6.6.4.297.R01
Summary:	Unable to display serial number of external Power supply in stack from OV2500 inventory page.		
Explanation:	Display serial number of Backup Power supply in secondary and idle units		

PR	**201474**	Build:	6.6.4.297.R01
Summary:	Qos profile (up=4 dscp=36) not created error message is been displayed in swlogs continuously.		
Explanation:	Prevent deletion of the QOS object which is in use		

PR	**204755**	Build:	6.6.4.299.R01
Summary:	Impact analysis on your products with CVE-2015-0291 t1_lib.c in OpenSSL 1.0.2.		
Explanation:	OpenSSL Vulnerability - CVE-2015-0287,CVE-2015-0289,CVE-2015-0292,CVE-2015-0209,CVE-2015-0288		

Under Verification:

PR	**166633**	Build:	6.6.4.37.R01
Summary:	Missing link after polling switch in Omnivista 3.5.2 version.		
Explanation:	Prevent mismatch of chassis ID on CMM and NI after takeover		

PR	**177150**	Build:	6.6.4.66.R01
Summary:	Issue with DHCP snooping, dropping the DHCP ACK frame		
Explanation:	DHCP Request packet will be relayed to only the server-ip ,if it carries in his contents. This implementation is controlled by debug variable "dhcp_isc_enable". This is disabled by default, to enable this feature set this variable in AlcatelDebug.cfg		

PR	**174214**	Build:	6.6.4.105.R01
Summary:	DHCP offer not received when client is connected to NI 2 of a stack		
Explanation:	Clients in the vlan for which ip interface's forwarding state is disabled will not get IP, unless relayUcastReply = 1		

PR	**181003**	Build:	6.6.4.186.R01
Summary:	Delay on port activating with LLDP-MED configuration on OS6450.		
Explanation:	When IP phone is connected to switch1 on port 1/4 and port 1/24 of switch1 is connected to the switch2 1/10. When the IP phone gets up, the mac address of the IP phone is getting learned properly on the port 1/4 of the switch1 and uplink port 1/10 of switch2.then when we connect IP phone to to the port 1/4 of switch2. the mac address of the IP Phone is not getting on the Port till the mac on the uplink port gets aged out. Once the mac is getting aged out ,it is get learned on the connected port.ie the Mac movement is not happening properly when we have connect to IP phone . So Changes have been done for proper mac movement handling.		

PR	**181685**	Build:	6.6.4.186.R01
Summary:	Stack split with taStp task suspended		

PR	**182391**	Build:	6.6.4.200.R01
Summary:	In OS6850 aaa accounting command server1, server2 local Local parameter is not working.		
Explanation:	As Per cli guide code change have been done to accept aaa accounting command server as LOCAL		

PR	**182667**	Build:	6.6.4.200.R01
Summary:	Remote address 0.0.0.0 is reported in accounting command packets sent from switch to server		
Explanation:	Sftp accounting packets will have the ip address of the client.		

PR	**182918**	Build:	6.6.4.200.R01
Summary:	Messages from TACACS+ server are not reported to end user in the console output		
Explanation:	Changes have been done to intimate the end user with server responds message.		

PR	**183457**	Build:	6.6.4.200.R01
Summary:	BPDU guard/ filter issue with Omniswitch		
Explanation:	"UserPort Shutdown BPDU" will shutdown the User Port on receiving BPDU With DA MAC 01:00:0c:cc:cc:cd"		

PR	**183031**	Build:	6.6.4.201.R01
Summary:	aaa accounting command local not printing any commands in swlogs		
Explanation:	aaa accounting command works fine after reload and accounting messages are logged in switch log .		

PR	**182765**	Build:	6.6.4.205.R01
Summary:	EXIT command issue with Omni Switch.		
Explanation:	Changes have been done to intimate accounting command information for exit command to tacacs server even there is no configuration		

PR	**183430**	Build:	6.6.4.209.R01
Summary:	UNP with policy list is not getting matched.		
Explanation:	Now ARP replies forwarded through the switch.		

PR	**186423**	Build:	6.6.4.215.R01
Summary:	OS6450: swlog showing wrong port number.		
Explanation:	The fix contains correction of port number in swlog for SFP plug out on fixed SFP plus port and Stacking ports.		

PR	**186887**	Build:	6.6.4.217.R01
Summary:	Spanning tree issue with Omni Switch with MSTP protocol when we disable cist on ports.		
Explanation:	Fix done to display the correct status of the STP operational status, after disabling the cist on port.		

PR	**187275**	Build:	6.6.4.219.R01
Summary:	I2C read error is overwhelming the switch, need to tone down the retries		
Explanation:	Implemented a proper check to reduce the number of i2c read error messages based on the retry mechanism.		

PR **187933** Build: 6.6.4.220.R01

Summary: Multiple simultaneous crashes (stacked and standalone)

Explanation: Drop the relay packet if size is more than 8192 bytes

---

PR **185859** Build: 6.6.4.222.R01

Summary: Stack splits when enable qos rules to protect user port.

Explanation: Added some delay for port up/down when clear-violation all is executed. With this change stack split won’t happen.

PR **190534** Build: 6.6.4.226.R01

Summary: Switch crashed with tCsCSMtask2, tCS_PRB and SsApp tasks suspended, when 'cd' command was issued.

Explanation: Check the number of directories entered by the user in CLI and throwing an error If path includes more than maximum number of directories allowed.

PR **189171** Build: 6.6.4.227.R01

Summary: OS 6250 stack reboot issue

Explanation: Debug added in watchdog pmd - stack reboot issue

---

PR **191527** Build: 6.6.4.229.R01

Summary: error in identification of the external power supply is seen as internal in Model: OS6450-P48

Explanation: Cosmetic issue fixed such that correct values are updated while extracting any of the power supply from the unit

---

PR **189848** Build: 6.6.4.233.R01

Summary: SFP showing incorrect DDM value.

Explanation: Fix done to show proper DDM value

PR **190451** Build: 6.6.4.239.R01

Summary: Dying-gasp syslog doesn’t contain switch IP or hostname

Explanation: Sending dyinggasp message to syslog server along with hostname.

PR **191435** Build: 6.6.4.239.R01

Summary: With copy working certified LLDP error messages seen and then synchronization was successful.

Explanation: Code changes done to not optimize checksum calculation if certify process is in process.

PR **192221** Build: 6.6.4.245.R01

Summary: OS6450: want to know if it is possible to get the "total power consumed" and the "total power available

Explanation: Enhanced the 'show lanpower' o/p to have total power consumption and total power remaining info

PR	**192927**	Build:	6.6.4.245.R01
Summary:	Need to create a user for SNMP without any CLI access.		
Explanation:	Code changes are done to close the SSH session for the user having no read-write permissions.		

PR	**193688**	Build:	6.6.4.246.R01
Summary:	ALU branded SFP-GIG-T (triple speed) is not working with 100Mbps / 10Mbps.		
Explanation:	Code change done to accept the ALU Branded triple speed copper SFP part number as triple speed SFP.		

PR	**193566**	Build:	6.6.4.246.R01
Summary:	Switch crashed with the suspension of the task "tSLNAdrLrn"		
Explanation:	severity level increased in a function to avoid crash		

PR	**191968**	Build:	6.6.4.246.R01
Summary:	Dying gasp trap format not similar to other traps		
Explanation:	Dying gasp trap (syslog server) format modified to be in sync with the other traps.		

PR	**194186**	Build:	6.6.4.246.R01
Summary:	OS6850E: 802.1x issue for IP-Phones using mobile-tag rule.		
Explanation:	Fix done to update the vlan tag in the mac-address table when mobile tag is enabled.		

PR	**193612**	Build:	6.6.4.247.R01
Summary:	Write memory flash synchronization and show configuration snapshot command output issue with OS9700		
Explanation:	Sflow Display Commands will not increase memory utilization		

PR	**194278**	Build:	6.6.4.248.R01
Summary:	OS6450: Rouge DHCP RELEASE packet forwarded through the TRUSTED port of the switch.		
Explanation:	Fix done not to forward Rouge DHCP RELEASE packet on the TRUSTED port of the switch, when this packet is ingresses from un-trusted port, and does not match on binding table.		

PR	**192437**	Build:	6.6.4.259.R01
Summary:	[TYPE1]6450: POE does not work on above port #10 for Third party Phone 7960		
Explanation:	6450: POE does not work on above port #10 for Third party Phone 7960 when all port s are connected with non poe devices.		

PR	**199241**	Build:	6.6.4.273.R01
Summary:	OS6250 is not forwarding the traffic 10.123.0.1 ip address used by the captive portal.		
Explanation:	Code changes done to update the Captive portal IP properly in the Hardware.		

PR **198726** Build: 6.6.4.275.R01
Summary: OS6450 stack was unreachable.
Explanation: Code changes done to log actions in exception handler module.

PR **200234** Build: 6.6.4.280.R01
Summary: LLDP traps are generated by the 6850E switches
Explanation: Code changes have been done to avoid the traps which are generated by processing Special LLDP packets.

PR **199797** Build: 6.6.4.273.R01
Summary: OS6450 stack crash analysis required
Explanation: Code changes done to handle Vlan Stacking NI - CMM communication failure during IPC congestion.

PR **201262** Build: 6.6.4.280.R01
Summary: Issue with the led status in the port 1/1 in the stack of OS6450.
Explanation: Code changes done to fix LED issues in user ports while stacking for 6450 switches.

PR **204081** Build: 6.6.4.299.R01
Summary: 2xOS6450-P48 Stack Crash with task
Explanation: Increased the debug level in hal-traces to avoid the memory corruption

PR **169401** Build: 6.6.4.37.R01
Summary: Clients not getting the IP address when NAP is enabled
Explanation: Allowed Bootp length in Udp-Relay is 1464

PR **181004** Build: 6.6.4.186.R01
Summary: Switch crash while enabling mobile tag.
Explanation: Fix for preventing crash while enabling mobile tag

PR **181045** Build: 6.6.4.182.R01
Summary: MIB walk for DhcpSnoopingPortIpSourceFiltering does not show all the ports.
Explanation: Mibwalk shows the status of all mobile ports if snooping is enabled globally

PR **181549** Build: 6.6.4.191.R01
Summary: SSH vulnerabilities in OS9800: SSL Version 2 (v2) Protocol Detection which reportedly suffers from s
Explanation: Disabled the ssl-v2 support due to vulnerabilities

PR **182564** Build: 6.6.4.191.R01
Summary: OS6450 - IP connectivity issue after upgrading stack to 6.6.3.495.R01
Explanation: Changes done to resolve IP connectivity issue on User Ports.

PR 177069 Build: 6.6.4.70.R01
Summary: ERP changed to protection status when NI hot swapped
Old PR#175082
Explanation: Whenever the message is received for ERP NI to ERP CMM.ERP CMM will check whether the message received from the NI which is in down state or up state .If we are receiving the message from the ERP NI which is already down. We are not processing the information further.

PR 173649 Build: 6.6.4.13.R01
Summary: Swlog logging messages on high CPU status for CMM / NI. Reference PR# 162618
Explanation: Additional Changes added to the current swlog to display if CMM/NI side task is affected while during an CPU spike

PR 195257 Build: 6.6.4.255.R01
Summary: DHCP offer packet is not forwarded by OS6450 udp relay
Explanation: Per vlan rtr mac destined changes

PR 195083 Build: 6.6.4.251.R01
Summary: OpenSSL vulnerability CVE-2014-0224 and CVE-2014-0160
Explanation: OpenSSL vulnerability CVE-2014-0224 and CVE-2014-0160 has been handled.

PR 191795 Build: 6.6.4.231.R01
Summary: Static route not showing the snapshot but however throwing the message "Static route already exists"
Explanation: Including the entry causing mip overflow in show configuration snapshot ip-routing.

PR 194230 Build: 6.6.4.249.R01
Summary: OS6450 not sending traps related to SFP.
Explanation: A new trap TRAPID_sfpNotificationTrap defined for SFP insertion and removal

PR 193082 Build: 6.6.4.246.R01
Summary: OS6450: DHCP snooping issue.
Explanation: Code changes done to check ip address along with mac and port while deleting the binding entry when release packet is received.

PR 188378 Build: 6.6.4.233.R01
Summary: OS6250 Collision is noticed in GUI not in CLI.
Explanation: Corrected discrepancies in Rx collision counter under GUI RMON statistics

PR 167885 Build: 6.6.4.75.R01
Summary: MIB or OID to monitor port utilization (InBits/s and OutBits/s) on switch
Explanation: Code changes done to add new MIB OID to monitor port utilization of out bit was implemented

PR	**182768**	Build:	6.6.4.205.R01
Summary:	Not all commands are sent to TACACS+ server to be authorized from the OmniSwitch.		
Explanation:	We have done changes for whoami and history size. We have added these commands to session management families.		

PR	**195079**	Build:	6.6.4.247.R01
Summary:	Issues with qos configuration.		
Explanation:	Setting the auto phone default priority as Trusted.		

PR	**184393**	Build:	6.6.4.271.R01
Summary:	After power cycle the snmp snmp access is allow for few minutes without aaa authentication default		
Explanation:	Fix done to disallow the access to the snmp server immediately after power cycle, when there is no aaa authentication snmp configuration.		

PR	**184016**	Build:	6.6.4.210.R01
Summary:	Unable to retrieve entire Mac-address table per port through SNMP		
Explanation:	Fix done to retrieve all the static mac entries on LPS port through the snmp.		

PR	**188601**	Build:	6.6.4.233.R01
Summary:	Unable to see snmp traps when enabling dying gasp on switch.		
Explanation:	adding dying gasp trap support for snmp version 1 (v1)		

PR	**199440**	Build:	6.6.4.275.R01
Summary:	Vulnerability in SSLv3 (POODLE / CVE -2014- 3566)		
Explanation:	Disable SSLv3 to mitigate POODLE attack		

PR	**201881**	Build:	6.6.4.287.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	**200505**	Build:	6.6.4.277.R01
Summary:	in OS6450 we notice request packets in two VLANS.		
Explanation:	Discard the unicast DHCP request packet if the destination mac is a VRRP mac and with no interface for incoming vlan.		

PR	**170018**	Build:	6.6.4.80.R01
Summary:	OS9702 dhcp offer dropped when dhcp snooping is enabled		
Explanation:	Don t drop Dhcp-Offer when received on client port but not on client vlan. This behavior is controlled by debug flag "allowRoutedReplyOnClientPort". When it is set to 1: Then we allow switch to receive Bootp-Reply packet in the client port under the		

condition that the Vlan is different.

PR	**182718**	Build:	6.6.4.205.R01
Summary:	Max command lengths are 250 for accounting and 259 for authorization		
Explanation:	The argument max length as per Tacacs+ packet format can support max of 255, thus if the argument length is more than 255, it is truncated to 255, so that accounting is succeeded.		

PR	**180605**	Build:	6.6.4.184.R01
Summary:	Ping delay to and from OS6250 or OS6450 experiences very high variation		
Explanation:	Software delay during the hardware to software processing is handled according to the switch behavior to have accurate ping delay in SAA		

PR	**176235**	Build:	6.6.4.188.R01
Summary:	OS6250 LED problem:Some LEDs are not flashing though the link is up		
Explanation:	When the unit s stacking LED is on, recover the switch to normal state where the port LEDs would be ON after 30 seconds. Also the issue with stack push button is resolved with FPGA version 14.		

PR	**197501**	Build:	6.6.4.262.R01
Summary:	OS6450 showing many lbdProcessMsg:459 messages in swlogs		
Explanation:	Setting appropriate debug level for LDB switch log message		

PR	**183666**	Build:	6.6.4.215.R01
Summary:	DHCP discover from extended module port like 1/51 is not forwarded to linkagg port		
Explanation:	After Initialization uplink ports will not lose their vlan membership.		

PR	**186600**	Build:	6.6.4.220.R01
Summary:	psNotOperational Power supply is inoperable, Object: power Supply 2, Index: 65		
Explanation:	Changes done to send trap only when power supply is present and non-operational.		

PR	**185970**	Build:	6.6.4.215.R01
Summary:	DHCP snooping trusted port and binding table		
Explanation:	Implemented the cli "show ip helper dhcp-snooping ip-source-filter binding ".This command is used to display the binding entries for the clients connected in ip-source-filtering enabled ports.		

PR	**189941**	Build:	6.6.4.245.R01
Summary:	"qos user-port shutdown bpdu" - shutdown is not triggered by PVST+ BPDUs until 1x1 PVST+ compatibility		
Explanation:	The corresponding hardware entry is made active regardless of PVST+ mode is enabled or not.		

PR	**188855**	Build:	6.6.4.228.R01
Summary:	lacp agg actor port priority command accepting value beyond 0-255		

Explanation: The check for the bounds of lacp agg actor port priority has been changed to 0 to 255.

PR **159876** Build: 6.6.4.102.R01
Summary: HTTP code redirection from 301 permanent redirect to 307 temporary redirect
Explanation: Allow temporary http redirection 307 for avlan clients. This is controlled by debug flag tempRedirect.

PR **181456** Build: 6.6.4.187.R01
Summary: OS 6250 hanged with exception in task taEthOAM_NI, tSLNAdrLrn, Ipedr
Explanation: Added a defensive check to check for the pointer value of encoded TLV.

PR **181521** Build: 6.6.4.184.R01
Summary: Locally configured routes are displayed with EMP interface when we configured with 6.4.5.447 R01
Explanation: A condition is introduced to display the interface of routes with gateway 127.0.0.1 as "Loopback' in routing database.

PR **179716** Build: 6.6.4.215.R01
Summary: Third party GBPTControl frames (DA mac 01:00:0c:cd:cd:d0) tunneled by software in 6.6.3.R01
Explanation: Implemented CLI command to enable and disable MAC tunneling as below: ethernet-service mac-tunneling enable/disable (usage: To enable or disable the mac-tunneling feature). show ethernet-service mac-tunneling (usage:To know the status of the mac-tunnel feature like whether the feature is enabled or disabled and applied or not).In 6.6.X releases the uni profile treatement should be tunnel for following protocols in order to tunnel along with the above command in order to tunnel the DA MAC 01:00:0c:cd:cd:d0
PAGP
UDLD
CDP
VTP
DTP
PVST
VLAN
UPLINK

PR **181650** Build: 6.6.4.185.R01
Summary: VLANs to see each other traffic when in "bridge" is in "mode flat" on OS6250 & OS6450
Explanation: Code correction done for VLAN 1 traffic to be received only by port configured for VLAN 1.

PR **175606** Build: 6.6.4.18.R01
Summary: 6250-P24 stack units reboot (except Primary unit) and PMD file generated
Explanation: Prevent the condition of spurious interrupts when insertion and extraction of power

supplies happen at the same time.

PR **177338** Build: 6.6.4.37.R01

Summary: OS6250 RIP interface stopping sending of route updates under particular conditions

Explanation: The customer specific workaround is controlled by debug variable you can set this is in dshell or in AlcatelDebug.cfg
debug set ripRedistMaxAllowedRoutes 5
5 denotes the number of routes you want to redistribute to RIP from local route or static route. Even if we reach 256 routes from RIP learning, these 5 routes will be redistributed to RIP.
Note: Do not set this variable to more than 10 as it can increase the memory usage beyond the limit of 256 route to a large extent.

PR **198081** Build: 6.6.4.273.R01

Summary: [TYPE1]High CPU due to the task "taIpni 145" and high packet loss is noticed.

Explanation: Changes made to configure the static routes properly to make sure routing of packets done in H/W.

PR **198143** Build: 6.6.4.271.R01

Summary: Security issue due to console privilege escalation.

Explanation: Code changes done to disable Ctrl + <key> combinations in console by default.

PR **192072** Build: 6.6.4.238.R01

Summary: SAA shows negative value for Max RTT & Max jitter

Explanation: Do not update the aggregate record if the latest iteration value is -1.

PR **193984** Build: 6.6.4.247.R01

Summary: OIDs displaying different information between 6.6.3.478 and 531.

Explanation: Data type is displayed as integer instead of counter 32. Made necessary changes.

PR **192174** Build: 6.6.4.249.R01

Summary: How to restrict the admin user ID to have console only access.

Explanation: Allows restriction of admin user to have console only
access to switch

PR **191007** Build: 6.6.4.228.R01

Summary: Communication issue between idle switch in Stack of OS6250 and OS6900.

Explanation: Changes done to configure a linkagg port as designated member in the hardware to process the packet from remote UNIT.

PR **190178** Build: 6.6.4.229.R01

Summary: OS6450 switches in stack crashed with suspended tasks: tCsCSMtask2 & Vrrp .

Explanation: Defensive check added in order to avoid crash because of invalid memory access.

PR **189500** Build: 6.6.4.234.R01

Summary: DHCP packets getting dropped on the trusted ports.
Explanation: Dhcp packet without End option also be processed, if the port is configured as trust.

PR **189884** Build: 6.6.4.228.R01
Summary: Switch losing its connectivity to the network , 10 mins after applying the QOS rule
Explanation: Router mac is configured properly when loopback0 interface is created. Now the ARP gets resolved properly.

PR **199979** Build: 6.6.4.274.R01
Summary: UNIT 1 in the stack of 3 switches lost console access along with network loss due to high memory usage
Explanation: Code changes to free the memory allocated by the taUdldNi task properly.

PR **198586** Build: 6.6.4.297.R01
Summary: OpenSSH version upgrade query. OS6850E.
Explanation: CVE-2010-5107, CVE-2011-5000, CVE-2010-4755 : Vulnerabilities for OpenSSH 5.0

PR **202046** Build: 6.6.4.287.R01
Summary: NTPD Vulnerability: ntpd version 4.2.7 and previous versions allow attackers to overflow several buffer
Explanation: Code changes done to fix NTP vulnerabilities CVE-2014-9295 & CVE-2013-5211.

PR **156663** Build: 6.6.4.245.R01
Summary: Authentication failure trap sent after snmpv3 session establishment
Explanation: Authentication failure Trap not required for snmpv3 time window errors.

PR **167944** Build: 6.6.4.69.R01
Summary: SLB Cluster IP is not able to ping from Secondary unit of the 6850 stack
Explanation: Flush old proxy arp for SLB cluster ip after takeover

---

PR **182219** Build: 6.6.4.215.R01
Summary: DHCP server showing the lease time as 0 while configured as infinity.
Explanation: Changes done to display the lease time correctly when infinite lease time is set in server

---

PR **183168** Build: 6.6.4.210.R01
Summary: Crash issue with Omni switch.
Explanation: Defensive check has been added to validate the path during FTP session on browser

---

PR **182027** Build: 6.6.4.181.R01
Summary: QoS value is showing negative value
Explanation: alaQoSQueuePacketsSent count always be positive.

PR **183211** Build: 6.6.4.201.R01
Summary: with aaa accounting command local having more than 255 character crashes the

	switch		
Explanation:	As per our analysis the root cause of the issue is whenever aaa send command message to server for processing the accounting request, the aaa command accounting will use the maximum size of command length which is 512.but when aaa command accounting is configured as local, it is using the buffer of size 255 because of this local accounting server is not able to hold the entire values of accounting command which also makes the switch to crash.so changes have been made to increase the buffer size as same as accounting command		

PR	**180822**	Build:	6.6.4.210.R01
Summary:	Query upgrading SSH Version to 5.2		
Explanation:	The orders of selection of the ciphers are changed so that it will consider AES CTR mode and arcfour ciphers are not vulnerable to this attack.		

PR	**182292**	Build:	6.6.4.188.R01
Summary:	The switch configured with tacacs+ server gets crashed when tried to telnet to switch.		
Explanation:	Packet with size exceeding the buffer size caused the crash , fix done to increase the buffer size to accommodate such packet(s).		

PR	**183032**	Build:	6.6.4.211.R01
Summary:	Unexpected crash noticed with Omni Switch.		
Explanation:	check added for pointer validity for sending buffer of radius auth request		

PR	**181112**	Build:	6.6.4.184.R01
Summary:	In SAA statistics RTT Avg values are smaller than RTT Min in case of ICMP Packet loss		
Explanation:	Code changes have done to correct the calculation of avg rtt value for all the received packets in case of ICMP loss.		

PR	**182637**	Build:	6.6.4.200.R01
Summary:	Accounting packets sent to all the servers configured with tacacs		
Explanation:	Tacacs accounting packet will be sent only to first active Server		

PR	**180957**	Build:	6.6.4.269.R01
Summary:	Duplicate primary and secondary switch were noticed after we reload the entire stack		
Explanation:	Fix done to unblock AOS tasks when unable to write output on to the tty driver's write buffer.		

PR	**179754**	Build:	6.6.4.187.R01
Summary:	Fan temperature co-relation queries and to modify the level at which fan starts cooling.		
Explanation:	Added a global variable "RunFanAtFullSpeed" through which fan speed can be adjusted irrespective of temperature for 6450-U24 model either by cli/AlcatelDebug.cfg.		

PR	**181695**	Build:	6.6.4.185.R01

Summary: OS6450 Stack issue: Primary CMM MAC is not getting synchronized correctly to IDLE Unit.
Explanation: IDLE unit Interface MAC is correctly synced with the Primary CMM MAC in the hardware table.

PR **195237** Build: 6.6.4.250.R01
Summary: Port stealing attacks are not prevented by DHCP snooping IP-source filter
Explanation: ip helper DHCP snooping ip-source-filter will block the gratuitous ARP packets when sent by the attacker with spoofed MAC addresses

---

PR **197425** Build: 6.6.4.275.R01
Summary: Randomly switches losses the SSH and Console access to the switch
Explanation: Forcefully deleting sftp task after waiting for certain time at sshd task

---

PR **185296** Build: 6.6.4.205.R01
Summary: TACACS Authorization not working properly when server becomes unreachable and then becomes reachable
Explanation: Tacacs authorization will be handled properly during the change in server status from unreachable to reachable.

PR **186071** Build: 6.6.4.215.R01
Summary: OS6250 configuration changes has not save flash memory.(old PR#183686)
Explanation: Fix done for Mip overflow in Ethernet services.

PR **185665** Build: 6.6.4.214.R01
Summary: "show Ethernet-service uni-profile ieee-drop-all l2pt-statistics" triggers an error
Explanation: Fix done to stop the error for expected behavior while accessing l2pt-statistics for uni profile IEEE_FWD_ALL and IEEE_DROP_ALL.

PR **192052** Build: 6.6.4.234.R01
Summary: OS6450: Need to know TACACS server status in the Omni switch.
Explanation: Tacacs server down messages will be logged in swlog

---

PR **193460** Build: 6.6.4.245.R01
Summary: OS6450 crash with taUDLDni and NIsup tasks suspended.
Explanation: UDLD NI Crash on TTL timer expiry is resolved

PR **191452** Build: 6.6.4.228.R01
Summary: QoS does not work when ICMP type configured in policy condition.
Explanation: Hardware entry is properly configured; Now QoS works fine with ICMP types in policy condition.

PR **190641** Build: 6.6.4.227.R01
Summary: MDNS packet with size of 1509 not get flooded with "ip multicast enabled"
Explanation: Code changes are done for Writing hardware register entries in all hard ware entries

for Control Packets.

PR **190230** Build: 6.6.4.237.R01
Summary: VRRP tracking commands getting cleared on a stack of OS6850E switches when primary unit reloads.
Explanation: Validation of slot availability is avoided during reload and takeover

PR **188377** Build: 6.6.4.219.R01
Summary: NTP issue with Omni switch.
Explanation: Controlling the snapshot of NTP configuration to store the IP address

PR **199925** Build: 6.6.4.275.R01
Summary: Configuring full transparent Ethernet-service on the omni switch.
Explanation: Introduced the command "captive-portal pass-through enable/disable"

PR **198970** Build: 6.6.4.275.R01
Summary: NI 2 in the Stack of 3X6450 swicth is running on the code 6.6.4.221.R01 rebooted.
Explanation: Code changes done to log actions in exception handler module.

PR **202371** Build: 6.6.4.289.R01
Summary: DTLS Vulnerability query - CVE-2014-3571 CVE-2015-0206
Explanation: Fixed openssl vulnerabilities CVE-2014-3571 CVE-2015-0206.

PR **203975** Build: 6.6.4.297.R01
Summary: Need clarification on power utilization and PoE (lanpower) info Switch OS6450 P10 & OS6450-P10L
Explanation: Updated power supply to 150W and PoE max power to 120W for 6450-P10L

PR **203897** Build: 6.6.4.294.R01
Summary: 6450 - QOS not dropping MultiCast streams while Active Policy Rule is matched
Explanation: Multicast policy rule with destination port can be configured in Default List

PR **205215** Build: 6.6.4.307.R01
Summary: 6450 lanpower fails to start after power outage
Explanation: Correction for lanpower startup failure due to power budget unavailability

PR **205150** Build: 6.6.4.309.R01
Summary: Alcatel-Lucent OmniSwitch 6450 Web Interface Weak Session ID CVE-2015-2804
Explanation: Increased Session ID strength in web Interface to prevent session guessing attacks

Known Issues:

PR	**198904**
Summary:	OS6450 is not forwarding the OSPF hello packet to other port with Ethernet-service.
Explanation:	Enable/disable the ip multicast routing status in hardware on vlan basis. By default it should be disabled for all vlans.

New Software Features:

1. CPE Test head

Introduction:

CPE test head feature shall now support bi-directional traffic functionality. This bidirectional functionality is achieved via unblocking the loopback mode in the CPE test head feature. In this mode Generator and Analyzer DUT will be same and remote DUT will configure as a Loopback DUT. The remote device shall reflect the traffic back to the originating device. The originating devILice shall count and drop the reflected traffic. This shall help measuring the network performance of customer traffic across network at a single end point. This feature shall support up to eight concurrent streams configured under test groups.

The CPE Test Head feature include one way test with the ability to report the results from the remote device on the unit initiating the test. This would also automate the way in which the test is triggered on the remote device. This feature shall add option to trigger the start at the remote end from the sender side via a proprietary protocol. Also the generator device for the test shall have a mechanism to gather Rx-Ingress test counters from the remote device and store it in a local database at the end of the test.

The CPE Test Head shall measure RTT and jitter during the test head operation. The L2 SAA test shall run between two supporting Omni switches. The L2 SAA tests shall run alongside the data traffic tests. The test results shall be available at the initiating device. This feature shall be available to both unidirectional and bidirectional tests.

Platforms Supported:
Omni Switch 6450
Omni Switch 6250

Commands usage:

test-oam <string> role {generator | analyzer | loopback}

Syntax Definitions

String The name of an existing CPE test.

Role The DUT shall have one role configured for a test-oam group as Generator, analyzer or loopback.

Generator Configures the switch as the test generator.

Analyzer Configures the switch as the test analyzer

Loopback Configures the switch as the loopback.

test-oam <string> { [vlan <vid>] [port <slot/port>] [packet-size <size of packet in bytes>] start|stop} [fetch-remote-stats**]**

While the fetch-remote-stats option is used, the test at the remote end shall be triggered from the generator side, stats shall be collected at the end of the test and finally test shall be stopped after receiving the test results.

Syntax Definitions

String The string is an identifier of the traffic test. Up to 32 tests can be configured. The string Can be of length 1to 32 characters long.

<slot/port> The port to be used in the testing. Depending on the role this port shall have different Interpretation. Generator -> port generating the frame. Loopback -> this port shall be the Port where Loopback of the traffic shall take place. Analyzer -> Port configuration is not Required.

<Size of packets in bytes> the size of packets in bytes, it can be of size from 64 byte to 9212 Bytes. It shall also include the size of CRC. Default value is 64.

Start Enables the test.

Fetch-remote-stats When this option provided, remote start/stat feature is enabled. User shall be Able to start the test at the remote end from the generator side and also shall be Able to collect the RxIngress counter results from remote at the end of the test.

test-oam <string> L2-SAA [priority <vlan-priority>] [count <num-pkts>] [interval <inter-pkt-delay>] [size <size>] [drop-eligible {true|false}]

While the cli is configured, the Testoam shall run SAA tests in parallel with the test streams.

Syntax Definitions

String The string is an identifier of the traffic test. Up to 32 tests can be configured. The string can be of length 1to 32 characters long

vlan-priority This is to specify both the internal priority of the Mac ping and the 802.1p value on the vlan tag header. Default is 0

count The number of packets to send in one ping iteration. Default value is 5.

inter-pkt-delay Delay between packets sent during a ping iteration in milliseconds. Default value is 1000ms.

size The size of the payload to be used for the MAC- ping iteration. Default value is 36 bytes

drop-eligible This is to specify both the internal drop precedence of the MAC ping and the CFI bit on the vlan tag header. Default is false.

Usage Guidelines

L2-SAA test shall derive the source mac, destination mac and the vlan id from the testoam configuration for individual test streams. The user shall be able configure a different SAA profile for each individual stream. Default L2 SAA configs shall be applied when no optional parameters are provided.

test-oam statistics flash-logging <enable/disable>

Syntax Definitions

enable This will enable the logging of test-oam statistics to the file.
disable This will disable the logging of test-oam statistics to the file.

Limitations:

When Test stream rate is configured as line rate, the remote statistics (the traffic statistics which gets reflected back from remote DUT configured as LOOPBACK) will differ from the traffic statistics generated from the DUT configured as GENERATOR.

2. Buffer Management on OS6250 and OS6450

Introduction:
This feature Enhancement provides the facility to increase the buffer size or change the profile for reducing the drops in the traffic. The OS6250/6450 comes with pre-canned buffer settings for all ports. This means that each queue on each port is statically set with a guaranteed number of buffers and descriptors.
In order to accommodate intermittent bursts, the switch supports a shared pool of buffers and descriptors that allows a queue to use a shared resource when its guarantee resource is exceeded. Neither the queue guaranteed resources or the shared resources are configurable. This implementation gives a limited buffering capability to support burst of traffic without discarding traffic. For some customers who are using specific applications, this is a major limitation.

Taking this into consideration, this enhancement attempts to overcome the limitation by increasing the buffering capacity, i.e. the ability to modify the number of buffers in the shared pool. The enhancement also adds the ability to change the default buffer profile assigned to the ports.

Platforms Supported:
Omni Switch 6450
Omni Switch 6250

Commands usage:

qos register shared-buffers <integer>

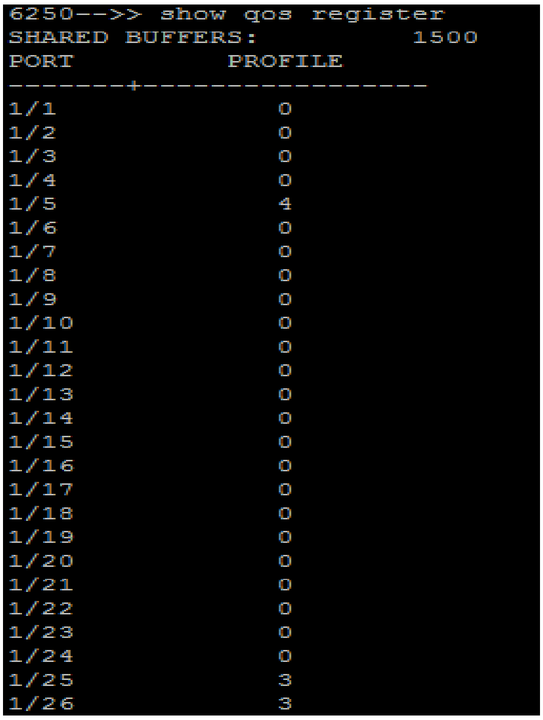
Syntax Definitions

Integer	The Integer specifies the number of shared buffers
Range	{0 – 4095}
Default	1500 [applied since switch boot up]

qos port <slot/port> register profile <integer>
Syntax Definitions

Integer	The Integer specifies the profile to be applied
Range	{0 – 7}
Default	0 for Network Port 1 for CPU Port 2 for Stack / Cascading Port 3 for Uplink Port 4 for CCFC Port

show qos register



```
6250-->> show qos register
SHARED BUFFERS:          1500
PORT           PROFILE
-------+----------------
1/1              0
1/2              0
1/3              0
1/4              0
1/5              4
1/6              0
1/7              0
1/8              0
1/9              0
1/10             0
1/11             0
1/12             0
1/13             0
1/14             0
1/15             0
1/16             0
1/17             0
1/18             0
1/19             0
1/20             0
1/21             0
1/22             0
1/23             0
1/24             0
1/25             3
1/26             3
```

Limitations:

Hardware Limitations

The buffer settings are limited and do not expose the entire ASIC configuration
The number of Tail Drop profile is not exposed. The content of the internal profiles is not displayed nor can the internal profiles be modified
The Tail Drop settings (enable/disable, random tail drop) are not exposed and stay to their default value
The Global System Limits (buffer, descriptor) are not exposed and stay to their default value
The Resource Sharing settings (resource sharing for DP1, resource sharing for individual queue) are not exposed and stay to their default value
The Per Port Limits (buffer limit, descriptor limit) are not exposed and stay to their default value

Software Limitations

If the Port Profile assignment fails in hardware, an error is displayed on the console and also reported in QOS logs. There may be a mismatch in port profile assignment displayed in the “show qos register” command output and the value applied in hardware.

3. 1K ARP Support in OS6450 & OS6250

Introduction:

This Feature is implemented to increase the ARP entries limit to 1K(1024).During the boot up based upon the role of the devices Metro / Non Metro the ARP limit is decided. If it is a non-Metro device the number of ARPs is limited to 1024 entries.

1K ARP support based on the model type and installed license during boot-up
- For OS6250-M model, no changes and ARP is limited to 256
- For OS6250/6450 without a metro license, support 1K ARP
- For OS6250/6450 with metro license, no changes and ARP is limited to 256

Earlier, the number of ARP for Metro as well as Non-Metro was limited to 256.

Platforms Supported:

Omni Switch 6450, 6250 (Non-Metro)

Limitations:

512 ARPs would be supported in Hardware, while remaining 512 ARPs would be added only in software and not in Hardware. Traffic for ARPs resolved in software would only be routed in software, so these traffics would cause CPU spike and packet loss.

4. TACACS Command Based Authorization

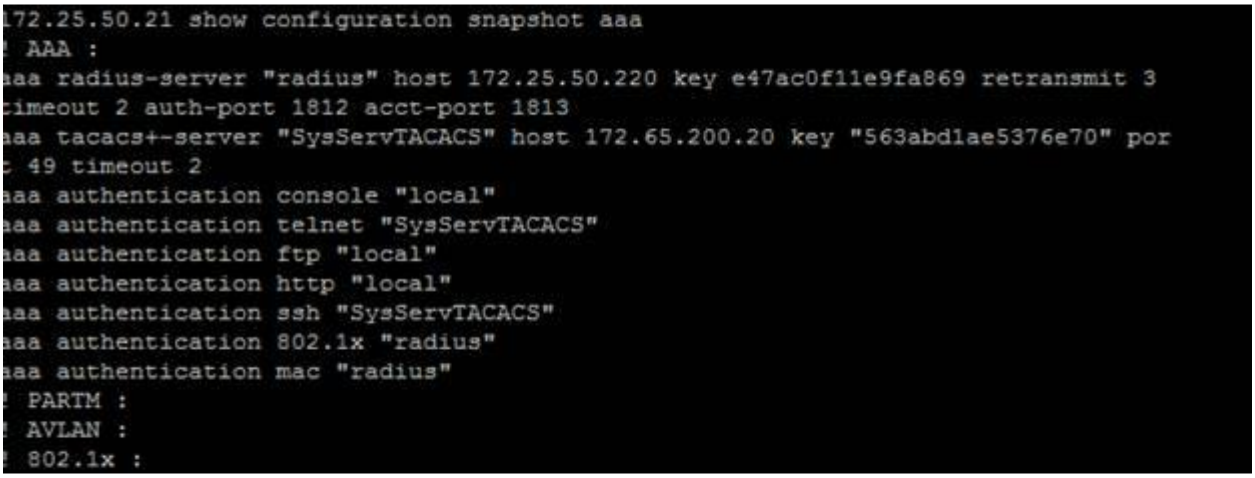
Introduction:

Prior to this enhancement command authorization in TACACS is done based on partition-management family that the command belongs to. According to the new feature, after authentication, once command based authorization is enabled then every cli command that the user executes on the switch is sent to the TACACS+ server. So TACACS+ server will do the authorization for the whole command and send the RESPONSE message to the TACACS+ client. If command based authorization is disabled then PM family for the command is sent for the authorization.

Platforms Supported:
Omni Switch 6250, 6450

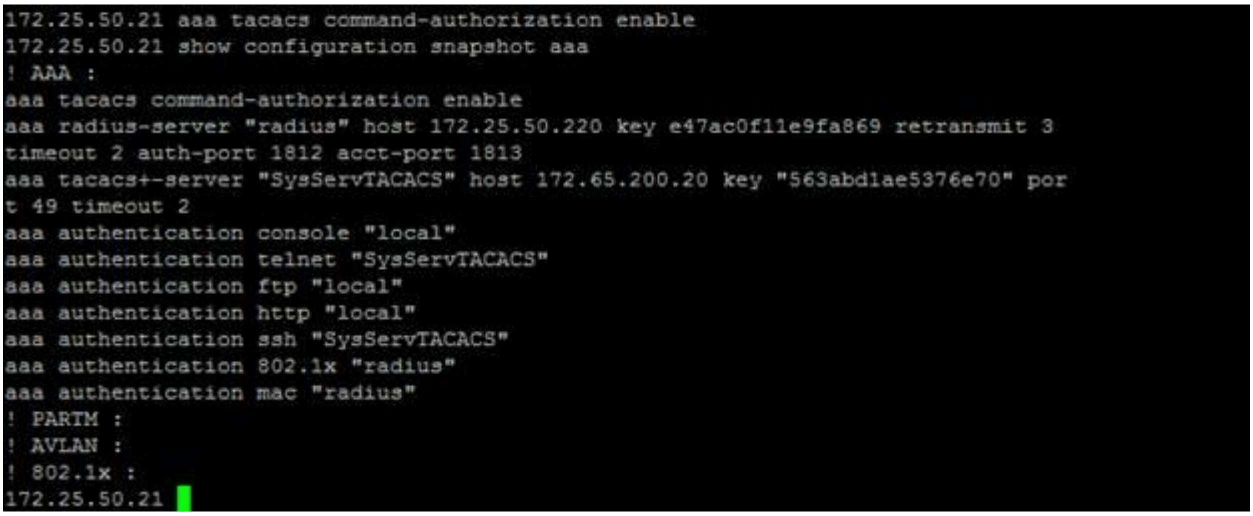
Commands usage:
aaa tacacs command-authorization {enable/disable}
By default command authorization is disabled

Configuration snapshot:
1. aaa tacacs command-authorization disable



```
172.25.50.21 show configuration snapshot aaa
! AAA :
aaa radius-server "radius" host 172.25.50.220 key e47ac0f11e9fa869 retransmit 3
timeout 2 auth-port 1812 acct-port 1813
aaa tacacs+-server "SysServTACACS" host 172.65.200.20 key "563abd1ae5376e70" por
t 49 timeout 2
aaa authentication console "local"
aaa authentication telnet "SysServTACACS"
aaa authentication ftp "local"
aaa authentication http "local"
aaa authentication ssh "SysServTACACS"
aaa authentication 802.1x "radius"
aaa authentication mac "radius"
! PARTM :
! AVLAN :
! 802.1x :
```

2. aaa tacacs command-authorization enable



```
172.25.50.21 aaa tacacs command-authorization enable
172.25.50.21 show configuration snapshot aaa
! AAA :
aaa tacacs command-authorization enable
aaa radius-server "radius" host 172.25.50.220 key e47ac0f11e9fa869 retransmit 3
timeout 2 auth-port 1812 acct-port 1813
aaa tacacs+-server "SysServTACACS" host 172.65.200.20 key "563abd1ae5376e70" por
t 49 timeout 2
aaa authentication console "local"
aaa authentication telnet "SysServTACACS"
aaa authentication ftp "local"
aaa authentication http "local"
aaa authentication ssh "SysServTACACS"
aaa authentication 802.1x "radius"
aaa authentication mac "radius"
! PARTM :
! AVLAN :
! 802.1x :
172.25.50.21
```

Limitations: Snmp and http are not supported in Command based authorization

5. Disable/ Enable the console session

Introduction

This feature Enhancement provides the facility to enable/disable the console cli session so that access to the switch configuration shell through the console port can be in a controlled manner as required. By default this facility (console access) will be enabled. This can also be stored in configuration file so that console access control can be applied even after reboot.

Recovery Procedure
If both the console cli session is disabled in the configuration file on both working and certified directory and if the telnet/ssh/web view session is not available to the switch, to get access to the switch console cli session user have to stop the switch in miniboot by setting the boot flags to 0x1000 and once the switch stops in miniboot user shall delete the configuration file and reboot the switch to get console access to the switch. Earlier, there was no provision to control the access for console cli session.

Platforms Supported
Omni Switch 6250, 6450

session console {enable disable}

Usage Guidelines:
By default, the cli console shell is enabled. The command shall be accepted only via Telnet/SSH session, and not through console sessions to the switch. When it is disabled, even the switch log output to the console shall be disabled. Command shall be stored to the configuration file using write memory. Command shall be used only on standalone unit, even if used in stack only primary unit console CLI session shall stay disabled.

Limitations:
None

6. The possibility to carry standard VLAN and 802.1q via NNI

Introduction:
This feature Enhancement provides the ‘Standard VLAN support on NNI ports’ will allow any standard (non-service) VLAN to be associated to NNI ports. This allowed association can be of type untagged or 8021q tagged. However, there is an exception for VLAN 1, which shall not be associated as untagged member to a NNI port. This will allow the customers to configure 802.1q services, QinQ service and untagged services using the same uplink NNI port. This will also allow the customer to use an untagged management VLAN to manage the switch via NNI ports.

With the implementation of this feature, the following will be the changes on the behavior of the switch:

The standard VLAN configuration (both untagged and 802.1q tagged association) will now be allowed on an NNI interface binded with a service VLAN.
The binding of service VLAN to NNI interface will now be allowed when the interface (physical or linkagg) is already tagged with standard VLAN.
802.1q VLAN tagging to an NNI interface will not be allowed if the interface is set with TPID other than 0x8100.
Any modification with respect to TPID will not be allowed if the NNI interface is 802.1q tagged.

There would also be significant changes with respect to the default VLAN of the NNI interface (both physical and LAG):

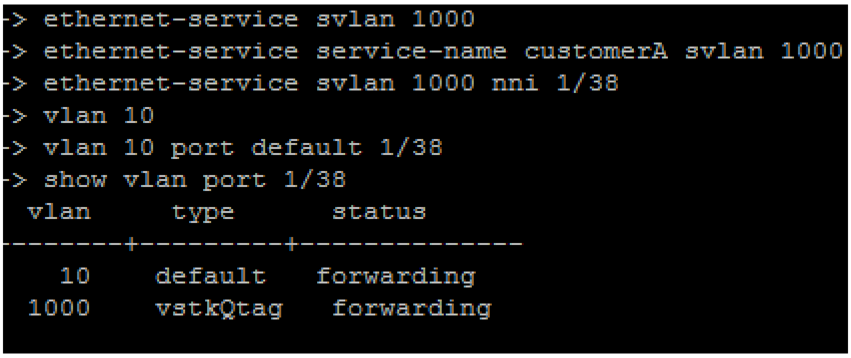
If an interface is already an untagged member of a standard VLAN other than VLAN 1, then on making it an NNI interface, there should not be any change with respect to the default VLAN of the interface. (Currently, the default VLAN changes to 4095).

If the default VLAN is removed from the NNI interface, then the default VLAN should be changed to 4095
It implies, from the above two points, that it shall not be possible to configure VLAN 1 as default VLAN of an NNI interface.

Platforms Supported:
Omni Switch 6450
Omni Switch 6250

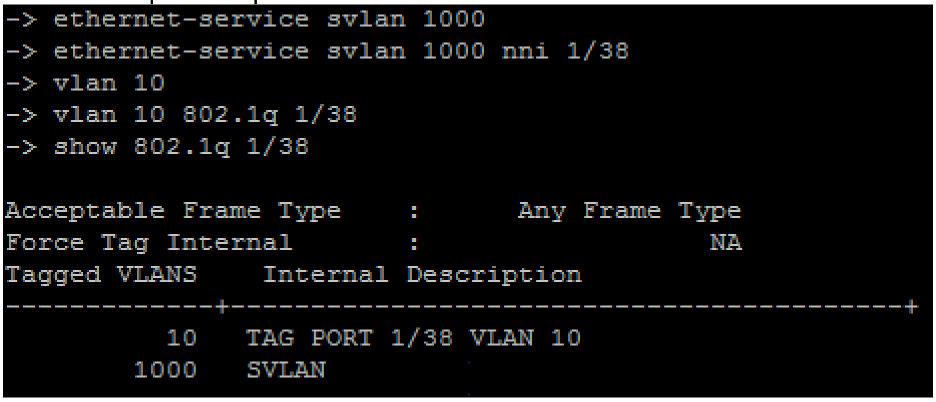
Commands usage:

Show the standard VLAN of an NNI interface:



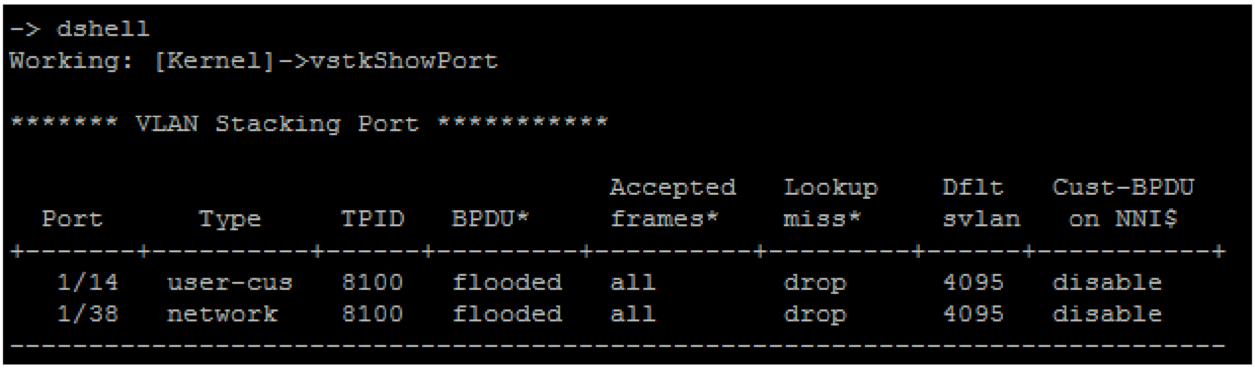
```
-> ethernet-service svlan 1000
-> ethernet-service service-name customerA svlan 1000
-> ethernet-service svlan 1000 nni 1/38
-> vlan 10
-> vlan 10 port default 1/38
-> show vlan port 1/38
 vlan     type      status
--------+---------+--------------
   10    default   forwarding
 1000    vstkQtag   forwarding
```

Show 802.1q on NNI port:



```
-> ethernet-service svlan 1000
-> ethernet-service svlan 1000 nni 1/38
-> vlan 10
-> vlan 10 802.1q 1/38
-> show 802.1q 1/38

Acceptable Frame Type     :       Any Frame Type
Force Tag Internal        :                   NA
Tagged VLANS     Internal Description
-------------+-----------------------------------------+
          10    TAG PORT 1/38 VLAN 10
        1000    SVLAN
```

Show the default VLAN of an NNI interface:



```
-> dshell
Working: [Kernel]->vstkShowPort

******* VLAN Stacking Port ***********

                                      Accepted   Lookup    Dflt   Cust-BPDU
  Port      Type     TPID   BPDU*     frames*    miss*     svlan   on NNI$
+-------+----------+------+---------+----------+---------+------+------------+
   1/14   user-cus   8100   flooded   all        drop      4095   disable
   1/38   network    8100   flooded   all        drop      4095   disable
------------------------------------------------------------------------------
```

Limitations:
None

7. Increased number of Telnet/ Syslog & NTP

Introduction:
This enhancement has increased the number increased of telnet sessions from 4 to 6, no of syslog servers increased from 3 to 12 and no of NTP servers increased from 3 to 12

Platforms Supported:
Omni Switch 6450, 6250 (Non-Metro)

Commands usage:
No new CLI introduced for this.

Limitations:
None

8. LLDP Power via MDI Enhancement

Introduction:
This feature enhancement facilitates to support the link layer classification in order to interoperate with newer class 4 PD’s(Powered Device) , because these devices require a response to the LLDPDU power via MDI TLV before they will draw additional power from PSE(Power). Earlier the maximum power is set to the maximum allowed power for the detected Power Class of the Power Device connected on the port. The Power Class detection is done via hardware by the POE controller. POE Devices in general can draw any amount of power up to the maximum power that is set for the port. In any condition, the maximum power that the PD can request from the PSE cannot exceed the maximum allowed power for the Power Class in which the PD(Powered Device) is detected, But these newer class 4PD’s(Powered devices) requires to draw additional power than the maximum power set for the port Hence this feature is introduced.

Platforms Supported:
Omni Switch 6250, 6450

Commands usage:

```
  lldp {slot/port | slot | chassis} tlv dot3 power-via-mdi {enable | disable}
```

Syntax Definitions:

```
  slot/port Slot number for the module and physical port number on that module
  slot The slot number for a specific module.
  enable Enables 802.3 TLV LLDPDU transmission.
  disable Disables 802.3 TLV LLDPDU transmission.
```

Usage Guidelines:

- The LLDPDU must be enabled and set to transmit before using this command.
- If this command is applied to a slot or chassis, then the existing configuration related to this command is lost.

Limitations: None

9. SSH Access to Read-Only Users

Introduction:
This feature Enhancement provides the facility to Establish a SSH Session for a Read-Only Users through Switch as Local Server, Radius Server,LDAP,TACACS.This SSH Read-Only Session allows to view the SSH Specific show commands .
Earlier it is not possible to SSH to a switch and access for a user unless he has read-write permissions. This is the current default behavior. But telnet to switch does not validate the permissions of the user and therefore switch becomes accessible.

Platforms Supported:
Omni Switch 6450, 6250

Commands usage:

```
user {username} read-only ssh password {maximum 8 }
```

Syntax Definitions:
Read-only :Specify the User Privilege
Ssh: The type of Service and Family the Belong to
Defaults
Parameter Default
Read only for families None

Usage Guidelines
Read-Only user configuration must specify the SSH family
Creating a user with Family as “none “ will not permit access to SSH

Show users:
Displays information about the all the user configuration
Alcatel-Lucent ESD – IP Networking – Service Release – 6.6.3.509.R01 - 9/11/2013

Examples:
User name = goog,
Password expiration = None,
Password allow to be modified date = None,
Account lockout = None,
Password bad attempts = 0,
Read Only for domains = ,
Read only for families = ssh ,
Read/Write for domains = None,
Snmp allowed = YES,
Snmp authentication = NONE,
Snmp encryption = NONE

Limitations: None

10. Stack split protection Helper

Introduction:
This enhancement provides facility to detect a stack split via the device acting as helper, called as SSP Helper (Stack Split protection Helper).For the device to act as helper we need to explicitly enable the helper mode, and it should be connected to the stack via linkagg.

The basic functionality of the helper would be to transmit the received health PDU to other ports in the linkagg associated with SSP. When enabled all the linkagg ports associated with the SSP would be programmed for receiving the SSP PDUs. When the SSP PDU is received the Helper NI would send SSP PDU to all other ports in Linkagg. When Helper receives SSP PDU with protection mode, it would immediately send an acknowledge of Protection mode receive and forward the protection mode PDU to all SSP ports.

Platforms Supported:
Omni Switch 6450

Commands usage:

stack split-protection helper {enable/disable}

Description: Helper Status Enable/Disable

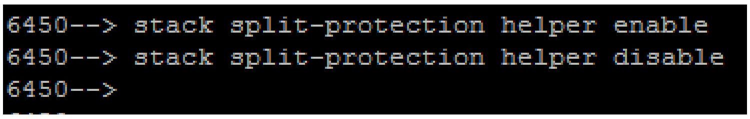
stack split-protection helper linkagg <linkagg-id>

Description: Linkagg-id on which to apply the SSP protocol on linkagg member ports for helper device.

show stack split-protection helper status

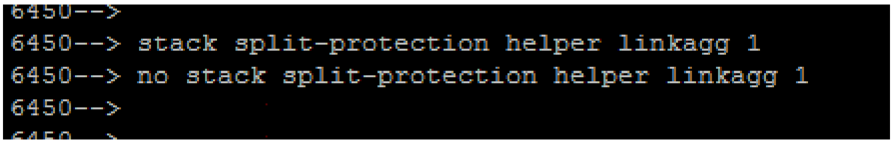
Description: This command shows SSP Helper status of the Link Aggregation ID assigned.

Configuration Snapshot:
1. Show stack split-protection helper enable/disable:



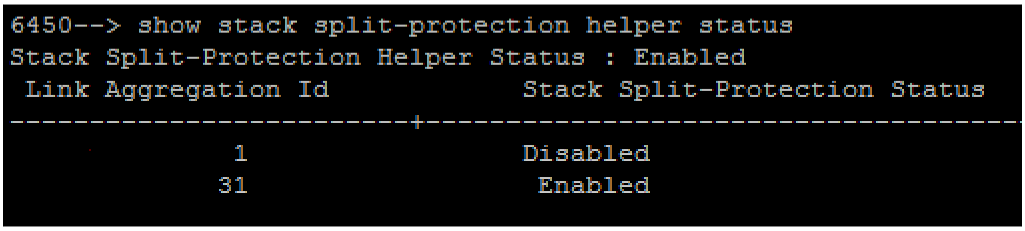
```
6450--> stack split-protection helper enable
6450--> stack split-protection helper disable
6450-->
```

2. Show stack split-protection helper linkagg <linkagg-id>:



```
6450-->
6450--> stack split-protection helper linkagg 1
6450--> no stack split-protection helper linkagg 1
6450-->
```

3. show stack split-protection helper status:



```
6450--> show stack split-protection helper status
Stack Split-Protection Helper Status : Enabled
 Link Aggregation Id            Stack Split-Protection Status
-------------------------+------------------------------------
              1                 Disabled
             31                  Enabled
```

Limitations:
None

11. Enable/Disable the MAC–Tunneling

Introduction:
Prior to this enhancement the mac tunneling feature can be enabled/disabled by setting the variable in AlcatelDebug.cfg. The functionality remains same but introduced the cli to enable and disable the mac tunneling feature. If the mac tunneling is enabled the destination mac in the frame is replaced with tunnel mac. If status is disabled there will not be any change in destination mac of the Frame.

Platforms Supported:
Omni Switch 6450
Omni Switch 6250

Commands Usage:

ethernet-service mac-tunneling {enable/disable}

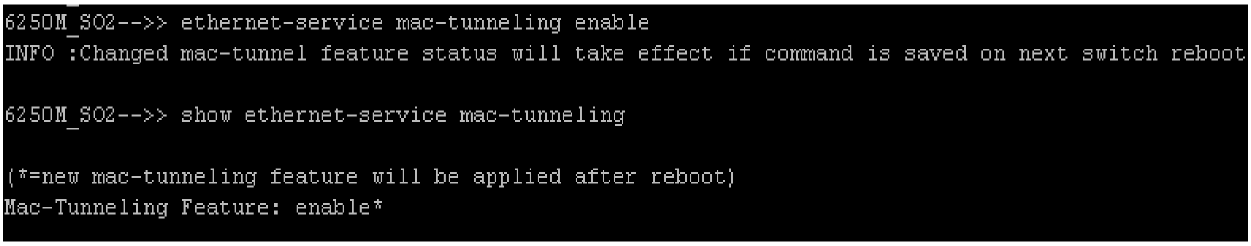
Usage guidelines

- By default, mac-tunneling is enabled.
- The command will take effect only after write memory and reload of the switch.

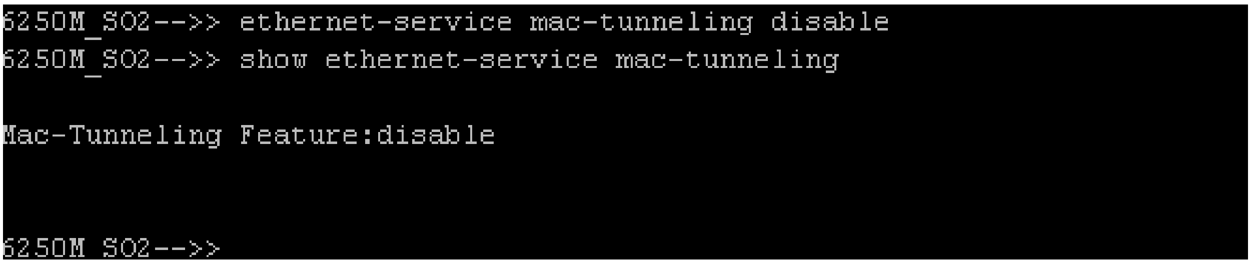
While changing the status the below info message will be displayed. (INFO :Changed mac-tunnel feature status will take effect if command is saved on next switch reboot)

show ethernet-service mac-tunneling

Display the status of mac-tunneling feature.



```
6250M_SO2-->> ethernet-service mac-tunneling enable
INFO :Changed mac-tunnel feature status will take effect if command is saved on next switch reboot

6250M_SO2-->> show ethernet-service mac-tunneling

(*=new mac-tunneling feature will be applied after reboot)
Mac-Tunneling Feature: enable*
```



```
6250M_SO2-->> ethernet-service mac-tunneling disable
6250M_SO2-->> show ethernet-service mac-tunneling

Mac-Tunneling Feature:disable


6250M_SO2-->>
```

Limitations:

The command will take effect only after write memory and reload.

12. DHCP snooping binding table for IP source filtering enabled ports

Introduction:
Prior to this, command will display the ports or vlans on which the ip source filtering is enabled. Added additional option “binding” to display the binding table for ip source filtering enabled ports. The binding table output is same as the output of show ip helper dhcp-snooping binding but it will show binding table for ip source –filtering enable ports.

Platforms Supported:
Omni Switch 6450
Omni Switch 6450

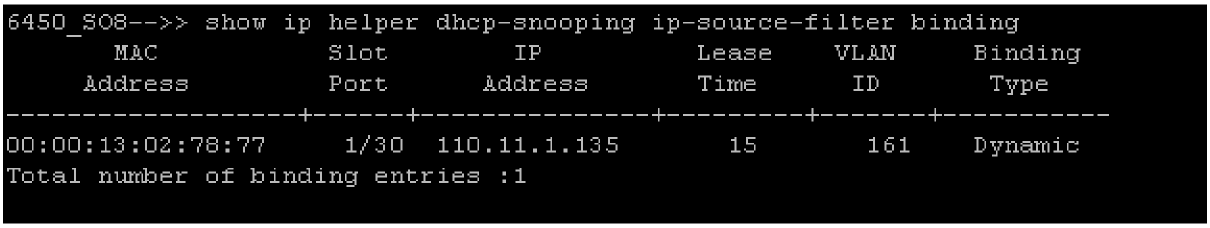
Command Usage:
show ip helper dhcp-snooping ip-source-filter {vlan| port |binding**}**

Syntax Definitions:
vlan Displays the VLANs on which the IP source filtering is enabled port
Displays the ports on which the IP source filtering is enabled binding
Displays the binding table for the ports on which the IP source filtering is enabled

Usage Guidelines:

- The show output displays only those ports or VLANs on which IP source filtering is enabled or binding table for ip source filtering enabled ports.
- This command also displays the status of the link aggregate ports when source filtering is enabled at VLAN or port level.

Snapshot:



```
6450_S08-->> show ip helper dhcp-snooping ip-source-filter binding
       MAC            Slot         IP            Lease     VLAN      Binding
     Address          Port       Address         Time       ID        Type
-------------------+------+---------------+---------+-------+-----------
00:00:13:02:78:77      1/30  110.11.1.135       15        161     Dynamic
Total number of binding entries :1
```

Limitations:
None

13. Per-Port Rate Limiting:

Introduction:
This feature enhancement facilitates to configure policy rule that specifies rate limiting as action for a group of ports or individual ports as per our requirement. For this enhancement new attribute “split & non-split” has been added for a policy port group to specify whether the group needs to be treated as a list of individual port or not respectively. This feature provides the following two modes to be applied as a part of the policy source port group:

1. Non-split: When used with this mode, the rule for rate limiting is applied for the group of ports. This is the default behavior for the source port group.

2. Split: When used with this mode, the rule for rate limiting is actually applied for each of the individual ports.

However, the action is not restricted to rate limit the incoming traffic, action could be anything other than the keyword “share”. Moreover, other actions can also be applied in addition to rate limiting, such as changing the dscp value, etc. Any incoming traffic in access of the applied bandwidth to an individual port will be dropped.

Before this enhancement, on configuring a policy rule that specifies a rate limiter as action and a source port group as condition, the rate limiter is actually applied for the group of ports, not each individual port.

Platforms Supported

Omni Switch OS6250M(Metro), OS6450

Commands usage

policy port group <name> [mode {non-split | split}] <slot/port> <slot/port1-port2>

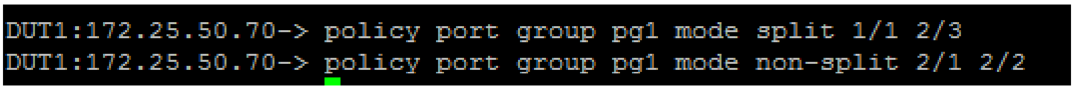
Syntax Definitions

split In this mode, the rule for rate limiting is actually applied for each of the individual ports.

non-split In this mode, the rule for rate limiting is applied for the group of ports. This is the default behavior for the source port group.

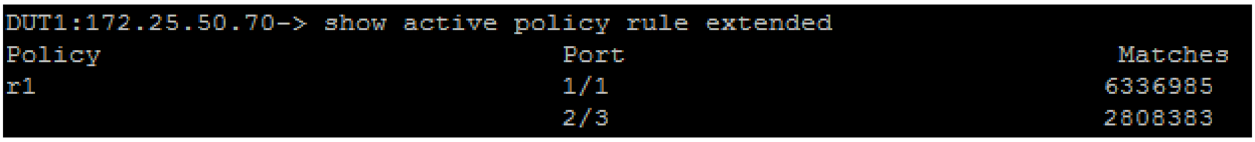
Usage Guidelines

When the port group is configured in the split mode, the rule needs to be split into multiple sub-rules.
Depending on the policy condition for the rule, each sub-rule may consist of multiple entries
The rate limiter is to be shared between the entries for the same sub-rule.



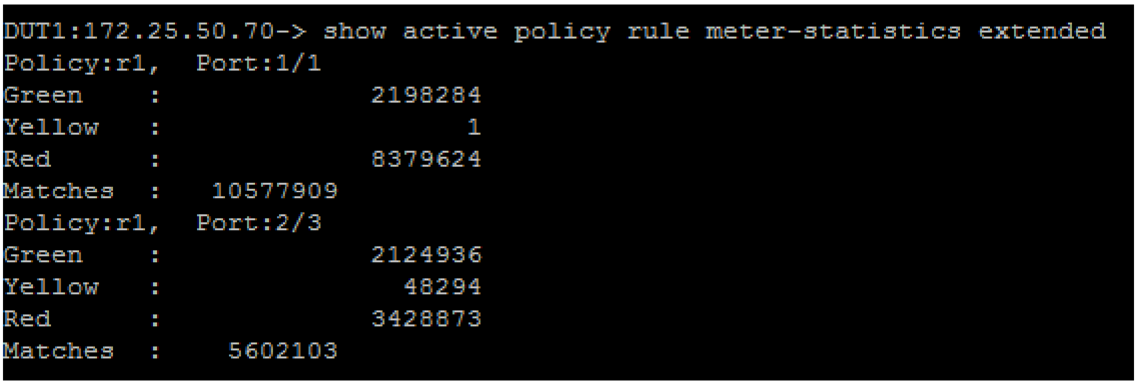
```
DUT1:172.25.50.70-> policy port group pg1 mode split 1/1 2/3
DUT1:172.25.50.70-> policy port group pg1 mode non-split 2/1 2/2
```

show active policy rule r1 extended:



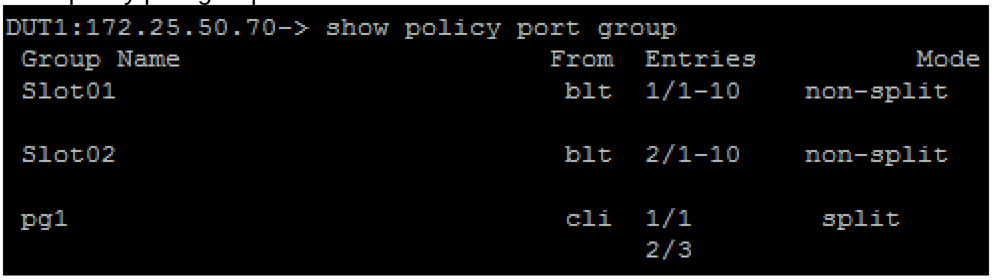
```
DUT1:172.25.50.70-> show active policy rule extended
Policy                             Port                              Matches
r1                                 1/1                              6336985
                                   2/3                              2808383
```

show active policy rule r1 meter-statistics extended:



```
DUT1:172.25.50.70-> show active policy rule meter-statistics extended
Policy:r1,  Port:1/1
Green     :             2198284
Yellow    :                   1
Red       :             8379624
Matches   :   10577909
Policy:r1,  Port:2/3
Green     :             2124936
Yellow    :               48294
Red       :             3428873
Matches   :    5602103
```

show policy port group:



```
DUT1:172.25.50.70-> show policy port group
 Group Name                        From  Entries          Mode
 Slot01                             blt  1/1-10    non-split

 Slot02                             blt  2/1-10    non-split

 pg1                                cli  1/1         split
                                         2/3
```

Limitations:
The scope of this feature is limited to source port group can be attached to only default policy list. Any rule with the source port group in the split mode attached to policy list will throw an error.

14. Tri Speed (10/100/1000) SFP Support on OS6450 U24

Introduction:
This feature Enhancement provides the ‘Tri speed SFP support on OS6450 U24’.The Copper Small Form Pluggable(SFP)s Finisar FCLF 8521-3 and Finisar FCLF 8521 P2BTL are compatible with Gigabit Ethernet(1000 Mbps), Fast Ethernet (100 Mbps) and Ethernet(10 Mbps).

Platforms Supported:
Omni Switch 6450

Commands usage:
show interface: show configuration snapshot interface

Syntax Definitions
Configuration snapshot interface verify the configuration of the interface

Limitations:
None

15. Config File Management

Introduction:

The configuration file management feature is to modify the configuration file label corresponding to the directory it resides, without affecting any functionality. Earlier when configuration file is retrieved from working and certified directories of Omni switch, they all have the same label as in old directory in the beginning of file regardless if you retrieve the file in working or certified directory. So after retrieving, it’s difficult to find from where the configuration file belongs.

The operations of existing configuration file management system:

While performing certify and/or synchronization or restoration process in Omni switch the configuration file of source directory will be copied to the destination directory based on the below conditions.

a) If the configuration file doesn't exist in the destination directory.

b) The file exists but differs in size and/or time stamp.

If any of the above condition is true, the configuration file will be copied to the destination directory and the timestamp of source directory configuration file will be re-applied on the copied configuration file in destination directory.

After the source configuration file contents copied to destination configuration file, the label in destination configuration file will be modified and the time stamps of source configuration file will be re applied.

Platforms Supported:

Omni Switch 6450
Omni Switch 6250

Commands usage:

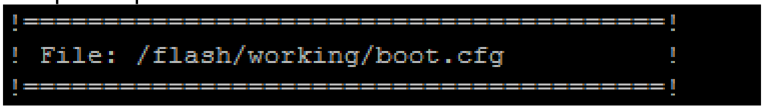
While executing the commands in the below table configuration file header should be updated showing the directory it is located and re-apply the source directory configuration file timestamp.

Command	Process Involved
copy working certified	certify process
copy flash-synchro	certify and flash synchronization
copy working certified flash-synchro	certify and flash synchronization
write memory flash-synchro	Save configuration, certify and flash synchronization
copy certified working	Restoring process
show running-directory	Synchronization status

Table 1 - Commands involved in verifying the implementation

Expected Outcome:
After issuing certify/synchronization commands mentioned in table 1, the process should complete without any errors and the label inside the boot.cfg file of certified directory should contain certified directory in the label.

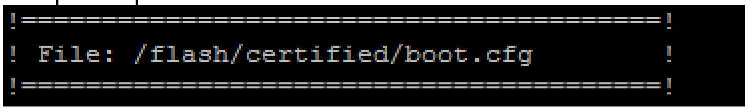
Sample output:



```
!=========================================!
! File: /flash/working/boot.cfg           !
!=========================================!
```

After issuing commands for restoring the files (mentioned in table 1), the process should complete without any errors and the label inside the boot.cfg file of working directory should be remain unchanged.

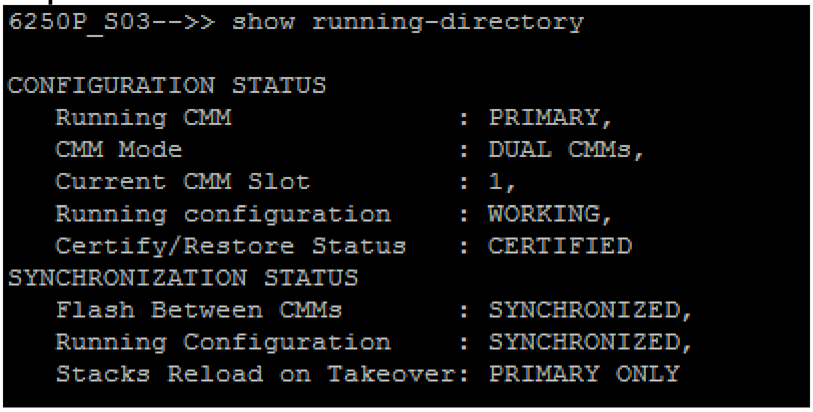
Sample output:



```
!=========================================!
! File: /flash/certified/boot.cfg         !
!=========================================!
```

There should not be any functional impact on existing synchronization status determining logic.

Sample output:



```
6250P_S03-->> show running-directory

CONFIGURATION STATUS
   Running CMM                : PRIMARY,
   CMM Mode                   : DUAL CMMs,
   Current CMM Slot           : 1,
   Running configuration      : WORKING,
   Certify/Restore Status     : CERTIFIED
SYNCHRONIZATION STATUS
   Flash Between CMMs         : SYNCHRONIZED,
   Running Configuration      : SYNCHRONIZED,
   Stacks Reload on Takeover: PRIMARY ONLY
```

Limitations: None

16. Ethernet-OAM Remote Fault Propagation

Introduction:
Remote Fault propagation (RFP) propagates connectivity fault events into the interface that is attached to a MEP. Once the fault is detected for a MEP, the MEP's interface is shutdown. Unlike other violation mechanisms that keep the link up when an interface is shutdown, this fault propagation mechanism will effectively shutdown the link so that the remote end of the interface also detects a link down.The feature is

configurable on per MEP basis and is supported only for UP MEPs. Remote Fault Propagation detects only Loss of connectivity and Remote MAC defect.

Platforms Supported:
Omni Switch 6450
Omni Switch 6250

Commands usage:
ethoam endpoint <mep-id> domain <md-name> association <ma-name> rfp {enable|disable}
Above CLI shall enable or disable RFP on MEP

Syntax Definitions
<mepid> A small integer, unique over a given Maintenance Association, identifying a specific Maintenance association End Point. MEP-ID is an integer in the range 1-8191.
<md-name> Domain name.
<ma-name> Association name.

Usage Guidelines
The domain and association must be created before RFP can be enabled.
The end point must be configured in the MEP list, before it can actually be created.
The MEP must be an UP MEP. If down MEP is specified, CLI returns with an error.
The admin state of the MEP must be enabled in order to report faults.
RFP cannot be enabled on virtual UP MEP since it is not associated with a physical interface.
If RFP is enabled on an UP MEP created on a linkagg, then detection of RFP violation will shutdown the individual member ports. No new ports should be added to or removed from the linkagg at this time. This will not be blocked from configuration, but is left to the user.
It is recommended that if RFP is enabled on a port, then any other violation feature (Link Mon or LFP) should not be configured.
It is recommended that if RFP is enabled on a port, then automatic recovery is disabled for that port.
If Link Mon is configured on a RFP enabled port, then the WTR timer must be less than the CCM interval.

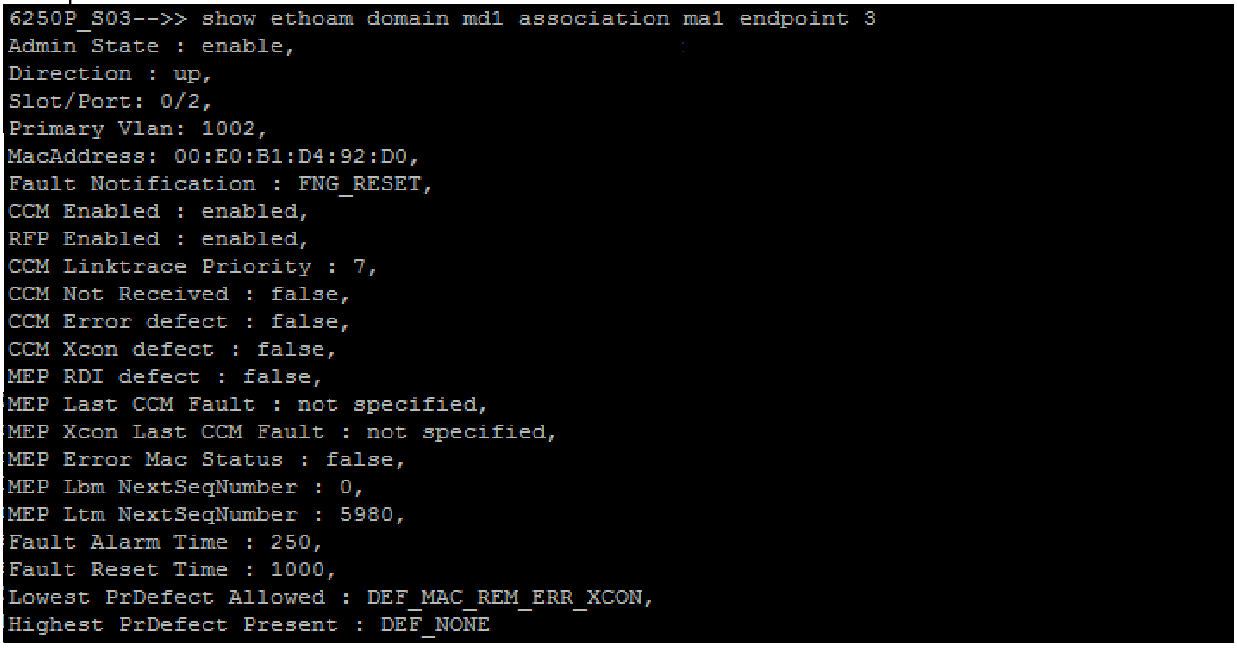
Example:

```
ethoam endpoint 3 domain md1 association ma1 rfp enable
```

show ethoam domain <md-name> association <ma-name> endpoint <mep-id>

Syntax Definitions
<mepid> A small integer, unique over a given Maintenance Association, identifying a specific Maintenance association End Point. MEP-ID is an integer in the range 1-8191.
<md-name> Domain name.
<ma-name> Association name.

Example:



```
6250P_S03-->> show ethoam domain md1 association ma1 endpoint 3
Admin State : enable,
Direction : up,
Slot/Port: 0/2,
Primary Vlan: 1002,
MacAddress: 00:E0:B1:D4:92:D0,
Fault Notification : FNG_RESET,
CCM Enabled : enabled,
RFP Enabled : enabled,
CCM Linktrace Priority : 7,
CCM Not Received : false,
CCM Error defect : false,
CCM Xcon defect : false,
MEP RDI defect : false,
MEP Last CCM Fault : not specified,
MEP Xcon Last CCM Fault : not specified,
MEP Error Mac Status : false,
MEP Lbm NextSeqNumber : 0,
MEP Ltm NextSeqNumber : 5980,
Fault Alarm Time : 250,
Fault Reset Time : 1000,
Lowest PrDefect Allowed : DEF_MAC_REM_ERR_XCON,
Highest PrDefect Present : DEF_NONE
```

Limitations: None

17. SSH Key size increase from 512 to 1024

Introduction
Currently the SSH key size 512. The SSH key size for certificate generation will be increased from 512 to 1024 for additional security. The switch uses default certificate for establishing its identity when acting as web server (receiving http/https requests). This certificate is generated once and stored in the flash as wv-cert.pem.

Since the certificate is stored persistently in flash, to allow the new key size to take effect the certificate needs to be regenerated. This means the certificate file needs to be deleted and switch rebooted in order to use this feature post upgrade to this release. The new certificate will be generated with increased key-size

Platforms Supported: OS6450/ OS6250

Limitations
This key size increase is only applicable to AOS auto generated certificate. Customers using their own certificates need to ensure that they are generated with proper key size.

18. Multicast Dynamic Control (MDC)

Platforms: OS6250,OS6450

In AOS, IPv4 and IPv6 multicast protocols are by default always copied to CPU. The high CPU usually impacts the normal operations of the Omni Switch protocols such as LACP, ERP.

In Order to resolve this high CPU issue, this feature is introduced to control the processing of the IPv4 multicast protocols.

The processing of all IPv6 multicast protocols is globally controlled by the presence of an IPv6 Interface.

- No IPv6 interface configured
  All protocols in the ff02:0::/32 range are transparently forwarded and not copied to CPU.
- At least one IPv6 interface configured
  All protocol packets in the ff02:0::/32 range are copied to CPU on all vlans irrespective on which vlan IPV6 interface is enabled.

MLD packets are copied to CPU based on the global ipms status. When IPMS is globally enabled, MLD packets are copied to CPU. When IPMS is globally disabled, MLD packets are not copied to CPU.

Command Usage:
1. To enable/disable multicast dynamic-control drop-all status
ip multicast dynamic-control drop-all status [{enable|disable}]

Guidelines: By default this status is disabled. If it is enabled, all ipv4 multicast packets including ipv4 multicast well-known protocol packets will be dropped. IPv4/IPv6 multicast protocol packets are given below in Note section.

To enable/disable ipms globally (in IPv4)
ip multicast status {enable|disable}
To enable/disable ipms globally (in IPv6)
ipv6 multicast status {enable|disable}

Note:

- If this command is entered without any enable/disable option, disable action will be applied.
- Below are the well-known IPv4/IPv6 multicast protocol packets,

VRRP:	224.0.0.18/32 + IP protocol 112
RIPv2:	224.0.0.9 + UDP port 520

Examples

ip multicast dynamic-control drop-all status enable
ip multicast dynamic-control drop-all status disable
ip multicast status enable
ip multicast status disable
ipv6 multicast status enable
ipv6 multicast status disable

```
->show ip multicast
Status                                        = enabled,
Querying                                      = enabled,
Proxying                                      = disabled,
Spoofing                                      = disabled,
Zapping                                       = disabled,
Querier Forwarding                            = disabled,
Flood Unknown                                 = disabled,
Dynamic control status                        = disabled,
Dynamic control drop-all status               = disabled,
Buffer Packet                                 = disabled,
Version                                       = 2,
Robustness                                    = 7,
Query Interval (seconds)                      = 125,
Query Response Interval (tenths of seconds)     = 100,
Last Member Query Interval (tenths of seconds)  = 10,
Unsolicited Report Interval (seconds)         = 1,
Router Timeout (seconds)                      = 90,
Source Timeout (seconds)                      = 30,
Max-group                                     = 0,
Max-group action                              = none
Helper-address                                = 0.0.0.0
```

```
->show configuration snapshot ipms
! IPMS :
ip multicast dynamic-control drop-all status enable
```

Limitations

- The proposed solution does not address the DOS attack concern
- Injecting a high rate of well-known protocol on a port will still cause a high CPU.
- Dynamic-Control “drop-all” feature should not be enabled if a routing protocol or VRRP is configured on the Omni-Switch as protocol packet will be dropped.

19. C-Vlan insertion with Loopback0 interface

Platforms: OS 6250, OS 6450

The basic idea of this feature is to convert the untagged frames into double tagged frames in the provider network so as to make ICMP between the endpoints to work. The frames should be always untagged on the customer network. This will be ensured using double push and double pop operations. The double push will happen on the UNI port in order to push the configured CVLAN as well as the SVLAN in the egressing packet. The double pop must be applied on the NNI port in order to remove both the tags when the packet is egressed from the UNI

Usage

To enable/disable ethernet-service untagged-cvlan-insert enable| disable
ethernet-service untagged-cvlan-insert [*enable/disable*]

To enable/ disable svlan
ethernet-service svlan *svid1*[-*svid2*] nni {*slot/port1*[-*port2*] | linkagg *agg_num*}
no ethernet-service svlan *svid1*[-*svid2*] nni {*slot/port1*[-*port2*] | linkagg *agg_num*}

To configure an CVLAN ip interface
ip interface *name* [address *ip_address*] [mask *subnet_mask*] [cvlan *num*] [vlan *num*]

To configure a loopback0 interface
ip interface *Loopback0* [address *ip_address*]

Examples

```
ethernet-service untagged-cvlan-insert enable
ethernet-service svlan 10
ethernet-service svlan 10 nni linkagg 1
ip interface test address 10.10.10.2/31 vlan 10 cvlan 20
ip interface "Loopback0" address 10.10.10.5

-> show ethernet-service untagged-cvlan-insert
Cvlan insertion for untagged packets      : Enabled

-> show ip interface cvlan
Total 1 CVLAN interfaces
        Name                IP Address     Subnet Mask   Status Forward  Device  CVLAN
--------------------------------+---------------+---------------+------+-------+-------+--------
test                        10.10.10.2      255.255.255.254     UP     YES vlan 10   20
```

Limitations

- Enabling “Cvlan insertion for untagged packets” feature on the switch would imply that the existing legacy behavior of UNI and NNI ports will no longer hold good
- Control traffic other than IP traffic destined to the switch out of scope of this feature
- The “show ip interface” will not display the mapped interfaces.
- The feature is meant for all IP traffic which is supported by the switch. Any other traffic which in-turn goes through the same interface will also be double tagged.
- As CVLAN-SVLAN is a one to one mapping, only one interface which uses the same SVLAN can hold the CVLAN. When we try to create another interface using the same SVLAN, and try to give a CVLAN value, it is expected to throw an error.
- CVLAN tag is supported only for normal interfaces and not for dhcp-client ip addresses

20. SSH PORT

Platforms: OS6450,OS6250

Introduced SW Release: 664.301.R01

In the existing implementation, AOS uses the default SSH TCP port (port 22) to establish an SSH session.

With the new implementation, when the user configures the TCP port number for SSH session, it will be saved in the switch file “/flash/network/sshConfig.cfg”. In order to use the configured port number while establishing the SSH session, the switch must be rebooted.

While the switch boots up, if the file “/flash/network/sshConfig.cfg” exists, it will be parsed to read the TCP port number that should be used to establish the SSH session, otherwise the default SSH TCP port shall be used.

Usage
Command to configure TCP-PORT number for establishing SSH Session.

```
ssh tcp-port <port-number>
```

<port-number >in the range 0-65535

Example: ssh tcp-port 35

Note: Well-known reserved TCP port numbers and the IP ports which are internally used in AOS are excluded in assigning to SSH TCP port.

Limitations

- Switch must be rebooted after configuring the TCP port number so as to use the configured TCP port number when establishing SSH sessions.

- Well-known reserved TCP port numbers(ports 20,21,23,25,69,80,161,389,443) and the IP ports which are internally used(defined in system_ipport.sh) are excluded in assigning to SSH TCP port. Error will be thrown when these ports are tried to be configured for SSH port.

21. TWAMP

Platforms: OS6450,OS6250

Introduced SW Release: 664.298.R01

Two-Way Active Measurement Protocol (TWAMP) provides a standard technique to measure network performance metrics. Unlike ICMP Ping, TWAMP also measures round trip delay/Jitter apart from the RTT. Moreover TWAMP does not require clock synchronization between the two devices. The initial release will support the TWAMP Server and/or Reflector Implementations of TWAMP in Unauthenticated Mode only for IPv4.

Following are the functionality provided by the feature.

- AOS S/w implements TWAMP server/reflector functionality specified in RFC 5357.
- Supports establishing TCP control session between TWAMP client/controller and the AOS switch that would function as TWAMP Server/Reflector
- Supports SERVWAIT functionality in case of TCP control session failure.The SERVWAIT time value can be configured by the user.
- Supports the following commads from the TWAMP client.
    a) Request-TW-Session
    b) Start-Sessions
    c) Stop-Sessions

- TWAMP server would transmit a test packet to the Session-Sender in response to every received packet
- AOS S/w also implements a REFWAIT timer functionality to monitor inactivity in test sessions.
- loopback0 IP address configured on the switch will be taken as the IP address of the TWAMP Server.

Usage

1) Command to enable TWAMP server.

```
-> twamp server [port <port-number>] [inactivity-timeout <mins>] [allowed-client <ipv4-address><ip-mask> … ]
```

Example: twamp server port 862 inactivity-timeout 10 allowed-client 10.10.10.1

2) Command to display TWAMP server

-> show twamp server info

Example: show twamp server info

```
TWAMP Server
Port: 862
Inactivity timeout: 15
Allowed-Client:
200.200.200.2 / 255.255.255.255
```

3) Command to show the TWAMP server connections

-> show twamp serverconnections

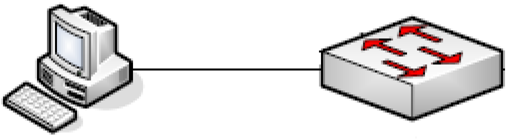
Example: show twamp server connections

```
Client IP      Conn Status      Time of Last Run      Pkts Sent      Pkts Received   Session Identifier
-----------------------------------------------------------------------------------------------------------
200.200.200.2   SETUP_DONE           0      0            0           96969696d83c6bea0fe502a0a01de548
200.200.200.2   SETUP_DONE           0      0            0           96969696d83c6bea0fe502a0af889d1e
```

Sample Use Cases

1. Respond to TCP Open messages from various clients and establish TWAMP ControlConnection

The DUT should be enabled for TWAMP server functionality
DUT should have configurations for TWAMP server like the TWAMP port number ,allowed-client IP address
TWAMP packets should be sent from ixia which acts like a TWAMP client



DUT

→ twamp server port 862 inactivity-timeout 10 allowed-client 10.10.10.1

Limitations
1) Time-stamping is not available in hardware on all platforms. Hence time-stamping is done in software on all platforms, namely Kite-2, Etna, Stackable Etna, Fuji, Fuji-2 and Garuda.

2) The TWAMP operations will use software based timestamps and hence will not provide precise measurement of network delay.

3) The TWAMP Server/ reflector will not use the DSCP of the Control- Client's TCP SYN in ALL subsequent packets on that connection (control and test packets).

4) The statistics displayed in "show twamp server connections" command is updated on a regular time interval only

22. Network Address Translation

Platforms: OS6250, OS6450

Introduced SW Release: 664.308.R01

Network Address Translation (NAT) is a feature that allows an organization's IP network to appear from the outside to use different IP address space than what it is actually using. Thus, NAT allows an organization which uses private addresses (local addresses), and therefore not accessible through the Internet routing tables, to connect to the Internet by translating those addresses into globally routable address space (public addresses) which are accessible from Internet. NAT also allows organizations to launch readdressing strategies where the changes in the local IP networks are minimum. NAT is also described in RFC 1631

Network Address Translation (NAT) is used for rewriting a source or destination IP address to another address. A single address may be rewritten, or an entire subnet or list of IP addresses may be rewritten to a group of addresses.

Following are the functionality provided by the feature:

1) Static NAT is where the mapping of local and global addresses is unanimous.

2) Dynamic NAT is a mapping of local addresses in a pool of global addresses. This means that the mapping between global addresses and local addresses is not unanimous and depends of the execution conditions.

3) NAPT (Address Port Translation) is mapping between local addresses and a unique global address. In this case a translation of the transport protocols ports (UDP, TCP) is carried out.

Usage

- To enable NAT policy condition for a source or destination ip/network

CLI: policy condition “condition_name” source| destination ip<ipv4 ip> mask <mask>

The source/destination ip/network should be an interface ip on the NAT device which needs to be NAT’ed.

- To enable NAT policy action

CLI: policy action “action_name” source|destination rewrite ip<ipv4 ip> mask <mask>

The rewrite ip should be an interface ip on the device

- To configure a rule to map a NAT condition with an action

CLI: policy rule “rule_name” condition “condition_name” action “action_name”

- To enable qos at the global level
  qos enable

- To apply qos at the global level
  qos apply

- To delete a NAT policy rule
  no policy rule “rule_name”

- To delete a NAT policy condition
  no policy condition “condition_name”

- To delete a NAT policy action

no policy action “action_name”

- To show the NAT policy configuration
  show configuration snapshot qos

- To check the NAT traffic flow
  show qos nat flows

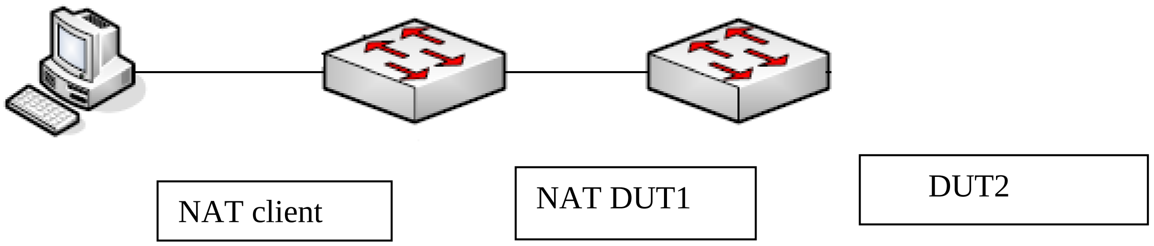
Example

```
->policy condition nat source ip 99.99.99.0 mask 255.255.255.0
->policy action nat source rewrite ip 9.9.9.2
->policy rule nat condition nat action nat
->qos apply

->show configuration snapshot qos
! QOS :
policy condition nat source ip 99.99.99.0 mask 255.255.255.0
policy action nat source rewrite ip 9.9.9.2
policy rule nat condition nat action nat
qos apply.

->>show qos nat flows
Proto   Inbound Private         Inbound Public          Outbound              Inbound          Outbound
                                                                               Rx/Tx            Rx/Tx
------+--------------------------+------------------------+-------------------------+-------------------+-------------------+
TCP     100.100.100.2:0          30.30.30.1:0          99.99.99.2:0       51746/51746       10821/10821
```

Sample Use Cases

1) Create a policy rule (trans_rule1) on the switch that will rewrite the destination address

1. The policy nat will rewrite the source address for any traffic from the 10.0.0.0 network to the Internet friendly address, 143.209.92.42
2. Traffic destined for the 10.0.0.0 network will be rewritten to the original IP addresses based on the dynamic TCP/UDP port assignment



NAT DUT1:

```
->policy condition internal source ip 10.0.0.0 mask 255.0.0.0
->policy action external source rewrite ip 143.209.92.42
->policy rule nat condition internal action external
```

Limitations

1. NAT feature is not supported in stacks.
2. This feature is CPU intensive, sessions like webview(HTTP), SSH, Telnet, FTP would not be working when the traffic rate crosses 1300pps (both forward + reverse direction combined).
3. DNS transaction not supported.
4. No support for reserved ports- L4 reserved ports would not supported for NPAT.