I have modified Intermediate Release

Omni Switch 9E, 6850, 6855 & 6400

Release 6.4.4.743.R01

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

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

Problems Fixed Between Builds 343 and 373

PR **157874** Build: 6.4.4.344.R01

Summary: 6850:If port 1/1 of a DUT is part of DHL A-A, default vlan change on any other port is not set in HW

Explanation: If port 1/1 is configured as part of a Dual-Home Link Aggregate (Active-Active), either as a physical port or part of a link aggregate, the default VLAN cannot be changed on any other port in the switch.

PR **158065** Build: 6.4.4.345.R01

Summary: 802.1x aaa device status is wrong when CP user session timeout

Explanation: Corrected show aaa-device non-supplicant users table when cp session timeout happens.

PR **158173** Build: 6.4.4.346.R01

Summary: Both default vlan ports go to forwarding on DHL active/active

Explanation: Preventing VPA updating based on STP for DHL Enabled ports.

PR **158147** Build: 6.4.4.347.R01

Summary: tCS_PRB and taIPni task suspended on OS6850 stack.

Explanation: ICMP Request is processed in CMM only for packets which are destined to one of the configured interface.

PR **157273** Build: 6.4.4.349.R01

Summary: Stack of 6850 not able to issue some CLI command.

Explanation: Clear the buffers after the processing of MIP messages from an Invalid session

PR **158097** Build: 6.4.4.350.R01

Summary: Warning message for duplicate static MAC configured on LPS port

Explanation: Warning message for duplicate LPS mac

PR **155432** Build: 6.4.4.350.R01

Summary: Need trap implementation when MAC movement happens

Explanation: Trap is implemented for a MAC movement under UDP Relay binding context.

PR **158162** Build: 6.4.4.351.R01

Summary: Non-supplicant user will get the default VLAN's dhcp IP address

Explanation: Handling of Arp packets corrected when the port is in CP-In Progress state and Supplicant-Bypass feature is enabled.

PR **158080** Build: 6.4.4.351.R01

Summary: Trans bridging is not supported for Linkagg

Explanation: Corrected agg check logic in vlan stacking mip test

PR **155533** Build: 6.4.4.351.R01

Summary: BCM show BLK state for mobile port

Explanation: Retry Mechanism in GM and debugs added in GM and STPNI.

PR **155410** Build: 6.4.4.352.R01
Summary: huge netsec configuration result in no output when issue show configuration snapshot
Explanation: Correcting the Previous group name passed to avoid MIP OVERFLOW in NETSEC

PR **158718** Build: 6.4.4.354.R01
Summary: feasibility to have cpLoginFail.html when CP authentication fail
Explanation: 1. Now we can see the https:// instead of http:// in status page.
2. When accessing customized cpLogin page, in the Url we can see the cp-vendor name given in the switch.
3. IF cpFail.html present in the switch, we can see an error message for cp authentication fail turns.

PR **158719** Build: 6.4.4.354.R01
Summary: aaa certification name " " should be available for customer's cpLogin.html file
Explanation: Corrected the captive portal logout page re-direction during authentication failure scenario

PR **156623** Build: 6.4.4.355.R01
Summary: NI CPU high taIP6NI and bcmRx task are going high.
Explanation: Nd6 unreached control mechanism in ipv6

PR **157631** Build: 6.4.4.356.R01
Summary: How to disable the gratuitous ARP.
Explanation: Introduced control over sending of gratuitous arps for ips configured for interfaces in the switch. This is done by help of existing variable "ipedrArpPoisonLrn", when set to 0 will stop the sending of gratuitous arps over the network.

PR **158648** Build: 6.4.4.359.R01
Summary: aaa supplicant entries has not been updated when domain user logon/log off
Explanation: Process deletion on a mobile port immediately

PR **158650** Build: 6.4.4.359.R01
Summary: certificate password is not working if the passphrase is
Explanation: Corrected issue seen in aaa certificate-password

PR **159226** Build: 6.4.4.359.R01
Summary: 802.1x non-supp status not updated in Web View GUI
Explanation: correcting the dot1x supplicant / non-supplicant user table in web view

PR **159157** Build: 6.4.4.359.R01
Summary: OS6850 doesn’t seem to generate alarm/trap when a remote endpoint is down.
Explanation: Changed the Priority behavior of the Fault Notification of ethoam

PR **159225** Build: 6.4.4.360.R01
Summary: cosmetic issue in "show aaa-device all users"
Explanation: Corrected the client ip address when cp user logout.

PR	**134952**	Build:	6.4.4.360.R01
Summary:	Captive Portal "logout page" cannot be redirected to.		
Explanation:	Captive portal logout page is accessible after authentication.		

PR	**157438**	Build:	6.4.4.360.R01
Summary:	OS 9E NTP date, year with time not showing correctly.		
Explanation:	Couple of year back DST For AEST has changed corrected in Code also.		

Problems Fixed Between Builds 374 and 410

PR	**159264**	Build:	6.4.4.375.R01
Summary:	ifDescr not in non-default VRF context		
Explanation:	VRF dependency on MIP_IFTABLE is removed. As this is IETF V2 Table		

PR	**160591**	Build:	6.4.4.376.R01
Summary:	9700E generated cs_systemX.pmd file after few days of upgrade to 6.4.4.342R01		
Explanation:	Defense check in OSPF module before updating forwarding address during a interface disable is added		

PR	**157396**	Build:	6.4.4.376.R01
Summary:	OS6850: Latency of approx. 1 Sec in authorization with TACACS.		
Explanation:	Reduced delay in tacacs+ command authorization to 100 ms.		

PR	**160463**	Build:	6.4.4.377.R01
Summary:	dshell cd "/flash/working" cause Synchronization commands will not be accepted due to low flash		
Explanation:	From dshell, "cd" will validate if the operation is done for a valid directory, else returns error.		

PR	**158234**	Build:	6.4.4.378.R01
Summary:	Transparent-bridging works only after a reload		
Explanation:	Added taskDelay of 5 ticks between vstk port creation and tunnel bind		

PR	**158236**	Build:	6.4.4.378.R01
Summary:	ERROR: Authorization failed. No functional privileges for this command		
Explanation:	Added check for syntax check mode for tacacs authorization		

PR	**160662**	Build:	6.4.4.378.R01
Summary:	BFD with VRRP does not work		
Explanation:	Link-Agg events processed in BFD is synced with BFD session state in NI		

PR	**160173**	Build:	6.4.4.378.R01
Summary:	SNMP traps with chasEntPhysOperStatus = 0 upon slot unpowered		
Explanation:	Corrected the trap generation to handle the state Operational status zero , during slot power off		

PR **149830** Build: 6.4.4.379.R01
Summary: Unable to login after changing the admin user password to xxxxxxx"!"
Explanation: Check for Password with special symbol

PR **160783** Build: 6.4.4.380.R01
Summary: OS9702E: ERP-Ring run into a infinite subnet broadcast Loop after switches reboots
Explanation: ERP - Peer NI communication information/status is corrected

PR **160837** Build: 6.4.4.381.R01
Summary: OS9702E: Adjacent ERP-RING port are blocking after switch reboot
Explanation: Restore ERP ring to IDLE after the initial port flap of Ring ports during Reboot.

PR **161011** Build: 6.4.4.382.R01
Summary: DVMRP not switching back to the primary path
Explanation: Fix is provided when dvmrp fails to switchback on primary path.

PR **159960** Build: 6.4.4.383.R01
Summary: OS6850E: Not Duplex CMMs, Flash Synchro aborted!!
Explanation: Added Debugs to extract information during flash access

PR **160791** Build: 6.4.4.384.R01
Summary: OS6850: Problem in QoS no trusted port.
Explanation: Changed mechanism to copy web hostname from http request header

PR **160737** Build: 6.4.4.386.R01
Summary: OS6850: Problem in QoS no trusted port.
Explanation: Qos port trust configuration to remain intact even after Reboot

PR **159452** Build: 6.4.4.386.R01
Summary: OS6855 : Temperature sensor error messages
Explanation: Recover the I2c Bus from lockup when a bad SFP is inserted.

PR **160717** Build: 6.4.4.387.R01
Summary: Fail to load logo and banner in CP status page
Explanation: Logo and Banner are Corrected in CP status page

PR **158212** Build: 6.4.4.389.R01
Summary: "depth" in a sap-profile is not applied on OS6400 platform
Explanation: Value configured in the depth field of sap-profiles is properly programmed in the hardware counter-Bucket Size

PR **159498** Build: 6.4.4.389.R01
Summary: Show commands not working after switch were upgraded.
Explanation: Handled the MIP OVERFLOW condition in lldp during the execution of the cli show configuration snapshot.

PR **158582** Build: 6.4.4.393.R01
Summary: Switch crashed with PMD. Task LLDPMgr suspended.
Explanation: Added Slot/Port Validity Check to Prevent LLDP List Crash

PR **160497** Build: 6.4.4.398.R01
Summary: 802.1X not connecting all users after reboot of 6850 (ref PR#156204)
Explanation: Ignore packet received on dot1x port for ip task to be ready after reload

PR **160902** Build: 6.4.4.398.R01
Summary: Stack of 3xOS6850 - synchronization failure in an environment with a non-default time zone
Explanation: Increase task Delay to make sure HSM date/time update is done before flash synchro

PR **159993** Build: 6.4.4.399.R01
Summary: 802.1x issue after upgrade to 6.4.3
Explanation: Pass message to all Nis when mobile entry is deleted

PR **161347** Build: 6.4.4.403.R01
Summary: crash on radius server not reachable message "Excep in task: RADIUS Cli PC : 0x2607b78 "
Explanation: We did fix to restrict the typecasting only for authentication requests. So accounting requests will not have any chance to go and access the wrong location.

PR **161417** Build: 6.4.4.403.R01
Summary: OS6850E-48X Rebooting Frequently
Explanation: When ZcRcv API receive invalid buffer pointer, it assigns Payload value as one ,this might cause the crash if processed further .Added a check to validate payload pointer before processing it.

PR **162320** Build: 6.4.4.403.R01
Summary: DHCP snooping is not working in slot 7 on a stack of 8 units of 6850.
Explanation: Reset Udprelay-CMM to NI socket completely on NI down events

PR **162030** Build: 6.4.4.403.R01
Summary: Boot.cfg.1.err created despite good OSPF passive interface configuration.
Explanation: Error check for ospf configuration is avoided during boot-up

PR **162442** Build: 6.4.4.403.R01
Summary: OS6850-P48L port becomes 1gig capable after upgrade to 6.4.4.373.R01
Explanation: Added proper check for Lite OS6850 48 port during port initialization

PR **161670** Build: 6.4.4.405.R01
Summary: OS6850E-48x lose OSPF neighbor-ship after the primary linkagg port is admin down
Explanation: Corrected port numbers of Stacking/Uplink ports on a 48 6850E device

PR	**158840**	Build:	6.4.4.406.R01
Summary:	XFP information is not seen in OV inventory report.		
Explanation:	Corrected the module IDs for XFP's and modified the description in mib file		

PR	**160039**	Build:	6.4.4.407.R01
Summary:	After upgrade to 6.4.3.779.R01, vlan 1 traffic is not passing through tagged port		
Explanation:	Clear untagged port bitmap alone for all vlans while initializing stp task		

PR	**161499**	Build:	6.4.4.407.R01
Summary:	ethernet-service sap-profile shared ingress-bandwidth is not working after 1g/s		
Explanation:	Allowing configuration of ingress bandwidth greater that 1G in hardware		

PR	**162368**	Build:	6.4.4.407.R01
Summary:	DHL is still forwarding of linkagg is not blocking DVMRP packet		
Explanation:	Only Layer2 Control packets are accepted on DHL blocked ports and all other packets are dropped on DHL blocked ports.		

Problems Fixed Between Builds 411 and 441

PR	**163169**	Build:	6.4.4.414.R01
Summary:	OS6850 - LLDP issue seen on few nodes		
Explanation:	Correcting lldp filter issue due to loopback detection enabled		

PR	**163369**	Build:	6.4.4.415.R01
Summary:	The owner value of the SAA is incorrectly manage by the switch		
Explanation:	SAA Owner commands handled properly during boot up		

PR	**160626**	Build:	6.4.4.416.R01
Summary:	Tac_plus/TACACS+: ERROR: Authorization failed. No functional privileges for this command		
Explanation:	Retry mechanism for TACACS server communication time errors		

PR	**162821**	Build:	6.4.4.416.R01
Summary:	OS6850 - in 6.4.4 ERP re-convergence time is about 5-10 sec		
Explanation:	Correcting ERP flag to correct re-convergence time in stacked environment		

PR	**160928**	Build:	6.4.4.416.R01
Summary:	OS6400 - New error message needed when TACAS server unreachable		
Explanation:	New error message has been introduced for TACAS server unreachable issue.		

PR	**162513**	Build:	6.4.4.416.R01
Summary:	OS6850 - Need log when Loopback-Detection is effective		
Explanation:	Log added during handling of shutdown event - LBD		

PR	**162439**	Build:	6.4.4.417.R01
Summary:	RADIUS Cli task crashed when interfaces 1 admin down with 1000 supplicants were authenticated.		

Explanation: Checks added to avoid unwanted crash when the server becomes not reachable.

PR **163167** Build: 6.4.4.417.R01
Summary: ICMP reply with checksum error
Explanation: Checksum is calculated properly for an SAA ICMP packet received from different vendors.

PR **162757** Build: 6.4.4.420.R01
Summary: PIM-DM have to re-enable status when we add a dense group
Explanation: Deleting static dense group needs to delete corresponding sg/forwarding entries.

PR **163973** Build: 6.4.4.422.R01
Summary: OS6850 is generating a keep-alive packet out of the linkagg to MCLAG switches, pings are dropped
Explanation: Keep alive messages are not send out on daughter module ports of OS6850E

PR **162618** Build: 6.4.4.423.R01
Summary: Implementation of the new swlog when CPU over/below the threshold
Explanation: Implementation of new swlog when Cpu crosses the above/below threshold value

---

PR **160756** Build: 6.4.4.425.R01
Summary: Decrementing Counter values for the OID (.1.3.6.1.2.1.2.2.1.11.13600002)
Explanation: total packet counter incremented when packet is received

---

PR **164266** Build: 6.4.4.426.R01
Summary: OS 6850 with captive portal configuration to remove extra files which cause slow downloading
Explanation: Remove .gif background images in Captive Portal Webpage

---

PR **164268** Build: 6.4.4.426.R01
Summary: To remove the useless messages with Captive portal in OS 6850
Explanation: Remove unwanted messages in captive portal webpage

---

PR **156355** Build: 6.4.4.427.R01
Summary: Send a traps when the free flash space is less than 5MB
Explanation: Trigger Chassis low flash trap when free flash less than min set level (3MB)

PR **164110** Build: 6.4.4.429.R01
Summary: OS6850 - L3 and L2 traffic are blocked after deleting any protected-vlan in ERP ring
Explanation: Block the STG for ring ports only when last ERP VLAN is deleted from STG but update STP for all PVLAN DEL

PR **162810** Build: 6.4.4.429.R01
Summary: Bypass icon and the non-supplicant status
Explanation: code change to disable bypass icon when cpdisableBypass.inc file is available in /flash/switch directory

---

PR **164378** Build: 6.4.4.430.R01

Summary: Additional request to remove sentences on CP progress status and logout page
Explanation: Additional request are provided to remove sentences on CP progress status and logout page

---

PR **164267** Build: 6.4.4.430.R01
Summary: With Captive portal configuration on OS 6850, we need to have two step logout processes.
Explanation: Simplified captive portal logout process

PR **159019** Build: 6.4.4.432.R01
Summary: 802.1x and IPMVLAN not working after reboot.
Explanation: Fix done to 802.1x and IPMVLAN to function properly even after reboot.

PR **163865** Build: 6.4.4.433.R01
Summary: random ip multicast traffic drops by OS6850E/OS6250 in ipmvlan environment
Explanation: Random multicast drops due to membership age out resolved.

PR **162433** Build: 6.4.4.434.R01
Summary: 100% CPU in unit 1 of stack of 6850 switches due to bcmRX and UdpRelay
Explanation: Prevent DHCP OFFER Packet being sent on Primary Port if received from the Secondary Port

---

Problems Fixed Between Builds 442 and 463

PR **164386** Build: 6.4.4.442.R01
Summary: Unknown error Cpsm(123):DHL CMM : port state = 8. don't care : Error messages during boot up
Explanation: Fix done not to throw error on boot up.

PR **164814** Build: 6.4.4.442.R01
Summary: MSTI instance 5 missing after reloads.
Explanation: Handling mip overflow issue in MSTP configuration

---

PR **160997** Build: 6.4.4.442.R01
Summary: OS6850-48X switch crashed by suspending tCsCSMtask2 & QoS tasks
Explanation: Debug statement modified not to carry unwanted string

---

PR **161551** Build: 6.4.4.442.R01
Summary: NTP Server address configuring with the unicast address ending with ".255" address is not working.
Explanation: Corrected the Validation for bcast address in ntp client/server

---

PR **158526** Build: 6.4.4.442.R01
Summary: taErpNI (ee90770) @ 100 SUSPEND lckd=0 CE stk ee90770-ee8e000
Explanation: Defense fix added for erp ring timer element in case of invalid memory access

---

PR **164517** Build: 6.4.4.443.R01

Summary: Occasional spikes on 6850E stack (bcmRX, taUdpRelay,
Explanation: Disabling interrupts for Combo ports on CPLD for OS6850E-U24x.

PR **158694** Build: 6.4.4.445.R01
Summary: bcm_switch_control_set(x,19,0) in AlcatelDebug.cfg
Explanation: Debug cli to disable unknown multicast packets to CPU is introduced. By default it is enabled.
To disable the following Command can be used
debug ip set ipv4ControlProtocolDisable 0
****
NOTE: disabling this flag will modify switch not to accept any multicast control packets 224.x.x.x
So protocols using these Multicast control address will not work
****

PR **163998** Build: 6.4.4.447.R01
Summary: OS6850 stack failure Error -5 is thrown due to temporary congestion in the IPC.
Explanation: tt of top three CPU hog tasks added in stackDebug.log

PR **165488** Build: 6.4.4.450.R01
Summary: CPU staying at 100 % after upgrading to 6.4.4.441R01 Ipmem task utilizing more
Explanation: Proper handling of TPCE errors in different NI flavors

PR **165255** Build: 6.4.4.458.R01
Summary: onex Crash when debugging and EAP failure for no reason
Explanation: Fixed crash seen when onex sends message to secondary

PR **154137** Build: 6.4.4.458.R01
Summary: APPID for stack Manager
Explanation: Added the STACKMGR Keyword in the APPID List of swlog/sys trace CLI

Problems Fixed Between Builds 464 and 502

PR **162981** Build: 6.4.4.464.R01
Summary: Not able to change password on secondary unit of 6850 stack
Explanation: Enabling the change in password on Primary to reflect on secondary CMM also

PR **165808** Build: 6.4.4.465.R01
Summary: IP Managed-Interface command being rejected by boot.cfg on switch reboot and boot.cfg.1.err file
Explanation: Corrected the interface name , when given within "" to avoid errors while processing

PR **165347** Build: 6.4.4.465.R01
Summary: Issue with Tunnel GRE setup and ACL.
Explanation: Qos policy should apply only on outer header of the packet, skipping QoS to apply policies in inner header.

PR **165666** Build: 6.4.4.466.R01
Summary: loopback0 interface in vrf cannot be advertised with bgp
Explanation: Loopback0 in non-default vrfs can also be used for advertisement

PR **166034** Build: 6.4.4.467.R01
Summary: 6to4 destination prefix 2002::/16 not added to the routing table with eui-64 addresses
Explanation: 2002::/16 destination prefix is automatically added to routing table for a eui-6to4 tunnel

PR **162043** Build: 6.4.4.468.R01
Summary: SFP on alcatel link down and other end link is half 1000Mbps
Explanation: Auto-Slave detection registers disabled for 1000-Fx(SX/LX/LH) for BCM 5482 phy chips.

PR **166423** Build: 6.4.4.468.R01
Summary: Flood rate limiting does not work and clear violation commands has no reaction in the test conducted.
Explanation: Reset Storm control violation condition on port reset

PR **165356** Build: 6.4.4.468.R01
Summary: DHCP relay to x.x.x.0 IP address not supported in AOS
Explanation: Configuration of IP-helper address is validated properly.

PR **165590** Build: 6.4.4.469.R01
Summary: bcmLINK.0 task high when "interfaces 1/8 tdr-test-start" command is executed
Explanation: This API will be introduced to set the interrupt configuration properly after the Tdr-Test Diagnostics is run. The interrupt will only be set if the port is using a PHY 5464SR or a PHY 54980

PR **166512** Build: 6.4.4.469.R01
Summary: OS6850 - LPS MAC learning issue
Explanation: Correcting flush logic on LPS port for permanent mac

PR **166831** Build: 6.4.4.471.R01
Summary: OS6850: RADIUS Cli (67e6f28) @ 100 SUSPEND
Explanation: Proper length handling in radius vendor specific fields

PR **166410** Build: 6.4.4.472.R01
Summary: Issue with Remote port mirroring related to QOS configuration.
Explanation: Have Cleared hardware register entry (EGR_RSPAN_VLAN_TAG) too , when remote port mirroring is un-configured.

PR **166713** Build: 6.4.4.472.R01
Summary: Double quotes on BFD interface is not getting saved in the boot.cfg
Explanation: Corrected the interface name , when given within "" to avoid errors while processing

PR	**165716**	Build:	6.4.4.473.R01
Summary:	Incorrect NAS Port value in Radius accounting request		
Explanation:	Introduced NASPortValueEnable flag to control NAS port value. Default value 0, NAS prt value will be 77. When set to 1, NAS Port will be the co-responding port number		

PR	**164856**	Build:	6.4.4.477.R01
Summary:	Stack of OS6850 crashed with taIpms and tCS_PRB task being suspended		
Explanation:	Added Debugs to dump required information from BCM Packet in PMD when data corruption in the packet occurs.		

PR	**167383**	Build:	6.4.4.478.R01
Summary:	PIM RP convergence problem.		
Explanation:	PIM RP hold time updated properly when multiple RPs listed in bootstrap message		

PR	**166435**	Build:	6.4.4.482.R01
Summary:	"interfaces crossover" - "mdi" and "mdix" parameters are accepted but don't work		
Explanation:	Added a error message for the interfaces crossover command when executed in cli.		

PR	**165198**	Build:	6.4.4.482.R01
Summary:	PVST+ is not converging for the default vlan with OAW		
Explanation:	VLAN 1 sends IEEE BPDU irrespective of PVST Mode set		

PR	**167100**	Build:	6.4.4.484.R01
Summary:	Show power x does not show the complete information till we reboot the switch.		
Explanation:	Corrected the EEPROM read to re-update the details of the power supply during Operational Status up/Down		

PR	**166417**	Build:	6.4.4.484.R01
Summary:	Switching boot up time increased after upgrade to 6.4.4.441		
Explanation:	Reduced the boot up time by removing delay in case EOIC is not received for VSTK module.		

PR	**164365**	Build:	6.4.4.484.R01
Summary:	Loopback0 if configured in same network as PIM interface is not sending RP & group info to neighbor		
Explanation:	PIM configured with loopback0 address as RP forwards multicast stream properly.		

PR	**166896**	Build:	6.4.4.484.R01
Summary:	A script is not executed if SW images are downloaded in Automatic Remote Config Download...		
Explanation:	Script is executed even after downloading new SW images and boot.cfg using Automatic Remote Config Download		

PR	**154357**	Build:	6.4.4.487.R01
Summary:	OS6850 - QoS user-port shutdown bpdu does not work properly		
Explanation:	Prevent lockup due to ESM reactor semaphore during port shutdown processing		

PR **167271** Build: 6.4.4.487.R01
Summary: IP multicast traffic drops when the primary switch in the stack is failed.
Explanation: Flushing of multicast source entries upon takeover was optimized

PR **165217** Build: 6.4.4.488.R01
Summary: On a Tunnel GRE setup, QoS DSCP priority is not shown in the packet
Explanation: When packet is forwarded to software due to tunnel environment stamp them in software.

PR **165647** Build: 6.4.4.488.R01
Summary: 6850: "bpdu shutdown" not get configured in actual NI
Explanation: 2 switches at Gwinnett county school has being in this NON FUNCTIONING "bpdu shut" state.Changes:-Prevent user-port getting reset for BPDU shutdown during periodic update.

PR **167148** Build: 6.4.4.492.R01
Summary: AOS Switch does not respond to MS Windows 7 ARP with APIPA source IP.
Explanation: Policy Switch Network group can be used from LDAP for QOS configuration

Problems Fixed Between Builds 503 and 508

PR **168666** Build: 6.4.4.503.R01
Summary: OS6850 crashes due to alias config.
Explanation: As per the implementation, Maximum 30 aliases can be configured, if more aliases are configured, appropriate error message is added for the same.

PR **167584** Build: 6.4.4.503.R01
Summary: DHCPACK packet being dropped by the DHCP snooping enabled switch
Explanation: Code changes done such that the packet is not dropped when Yiaddr is Zero only if Lease time is not updated by DHCP

PR **166712** Build: 6.4.4.503.R01
Summary: STR NON FATAL messages on log after the switch was upgraded
Explanation: case for mip_chassisSupervisionRfsDfSlot has been included in order to avoid error messages(No such instance: rcvd nominator 1invalid) in the log.

PR **165815** Build: 6.4.4.504.R01
Summary: 6855-14 crashes with no next hop self
Explanation: Semaphore protection for iprm routes

PR **168945** Build: 6.4.4.505.R01
Summary: OS6850-P48L switch crashed suspending the task 'onex'. (Switch-2)
Explanation: Receiving buffer has cleared after processing the session manager news message

PR **168517** Build: 6.4.4.507.R01
Summary: Broadcast and Multicast Frames sporadically delivered unidirectional only on VPLS service

Explanation:	Process VP_Update message only from the slot containing primary port.		

PR	**169172**	Build:	6.4.4.507.R01
Summary:	ERP issue		
Explanation:	Sent proper vlan parameters to dot1q NI on NI plug out and plugin scenarios		

PR	**168390**	Build:	6.4.4.507.R01
Summary:	802.1x supplicant bypass feature is not working after port admin down/up on OS68		
Explanation:	Fixed the 802.1x supplicant bypass feature on port down/up on OS68		

PR	**168443**	Build:	6.4.4.507.R01
Summary:	High CPU utilization on 6850		
Explanation:	High CPU utilization on IPMS is fixed		

PR	**168309**	Build:	6.4.4.508.R01
Summary:	Static route showing as 'inactive' even the routes are reachable and able to ping.		
Explanation:	Removed outgoing interface deletion code		

Problems Fixed Between Builds 509 and 530

PR	**168899**	Build:	6.4.4.510.R01
Summary:	WCCP stops forwarding traffic		
Explanation:	Send assignment weight in ISU message as it came in HIA of wccp packet exchange		

PR	**165232**	Build:	6.4.4.511.R01
Summary:	802.1x non supplicant device group mobility rule not applying correctly.		
Explanation:	Ignore ARP probe packet on AAA port		

PR	**162946**	Build:	6.4.4.512.R01
Summary:	Sending any packets with destination tunnel MAC (01:00:0c:cd:cd:d0) dropped at the UNI port.		
Explanation:	To disable layer 2 tunneling protocol using debug variable from AlcatelDebug.cfg[If noMacTunnelFeature =1, the layer 2 protocol tunneling is disabled, "debug set MacTunnelFeature 1"]		

PR	**168490**	Build:	6.4.4.513.R01
Summary:	DHCP offer/ack cannot be captured on mobile port when the mirror destination port is across the stack unit		
Explanation:	Fix done for stack of 8 to remotely send packet across units		

PR	**168864**	Build:	6.4.4.514.R01
Summary:	taQoS task suspended on 6.4.4.463.R01		
Explanation:	Debugs are added to report in pmd when number of hardware devices or slice goes out of range		

PR	**167483**	Build:	6.4.4.514.R01

Summary: Static ARP with "mac-address-table static-multicast" doesn't work on OS6850E-24X
Explanation: Static multicast support on standalone OS6850E introduced

PR **169989** Build: 6.4.4.514.R01
Summary: OS6400: link_oam_get_next_evt_log:8366
Explanation: Debugging Linkoam messages are masked to be non-default

PR **167589** Build: 6.4.4.516.R01
Summary: OS6850 - LPS issue in violation mode with dhcp-snooping enabled
Explanation: Corrected general DHCP handling on mobile and LPS ports

PR **167979** Build: 6.4.4.516.R01
Summary: Warning message to be displayed if an SNMP station is configured with a non-existent user
Explanation: A warning message displayed when SNMP station is configured with non-existent user

PR **167702** Build: 6.4.4.521.R01
Summary: Issue with BFD Static Routes remains down and doesn’t converge back even after the link up again
Explanation: Proper handling of BFD Sessions when L2-convergence happens over linkagg

Problems Fixed Between Builds 531 and 551

PR **169401** Build: 6.4.4.531.R01
Summary: Clients not getting the IP address when NAP is enabled
Explanation: Allowed Boot up length in Udp-Relay is 1464

PR **170073** Build: 6.4.4.531.R01
Summary: Switch is crashing when loopback detection configured on the OS685048L/OS6850U.
Explanation: Transmission Timer Cell during LBD packet transmission is set to NULL , after port is moved to blocking, to prevent Invalid memory access

PR **170717** Build: 6.4.4.531.R01
Summary: IP-Helper Mac Movement Errors in switch logs. These messages shouldn't be an error message and it sh
Explanation: Modified the IP-Helper MAC Movement Swlog Messages severity to "Warning"

PR **169759** Build: 6.4.4.531.R01
Summary: Ebgp multihop command does not changes the TTL value in a BGP neighbor packets
Explanation: Updated the TTL value in EBGP control packets

PR **170947** Build: 6.4.4.532.R01
Summary: ethernet-service svlan command issue
Explanation: Corrected the snapshot Issue to update the correct Vlan mapping after default assignment

PR **170650** Build: 6.4.4.532.R01
Summary: UNP-Allocation fails in case of bulk 802.1x-client-requests.
Explanation: Data Packets from Client before authentication is properly handled.

PR **170900** Build: 6.4.4.532.R01
Summary: ERROR: Alias name cannot be a keyword after upgrading from 6.4.3.R01 to 6.4.4.R01
Explanation: Aliases with same leading characters and substring's of existing Keywords are accepted.

PR **163667** Build: 6.4.4.533.R01
Summary: Query on trap OID "Trap OID: .1.3.6.1.4.1.6486.800.1.3.2.15.1.0.1" and packetDroptype 13
Explanation: Added Proper string while Query from NMS is sent for the following packet types dhcpserver, pim , dvmrp , isis , dns-reply

PR **165230** Build: 6.4.4.533.R01
Summary: OS9700 Switch crashed while executing the command rls cmm: b
Explanation: Corrected NULL Pointer access while executing rls command on Dual CMM

PR **171651** Build: 6.4.4.539.R01
Summary: stack crashed when the command policy port group test-qos mode split 1/15 is given.
Explanation: While configuring spilt mode for port group, validate the conditions with no destination port groups

PR **171051** Build: 6.4.4.539.R01
Summary: Issue with SOURCEPHOTONICS SFP (SFP-100-BX20LT) which are 100MB SFP are displayed as 1000 by default
Explanation: Support for 100-FX SOURCE PHOTONICS SFP

PR **159876** Build: 6.4.4.539.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 **161177** Build: 6.4.4.539.R01
Summary: Auto-negotiation not working properly on OS6400 only for 100Mbps patch cable.
Explanation: Ethernet@wirespeed feature has been enabled.

PR **171008** Build: 6.4.4.539.R01
Summary: OS6855-10: entityconfigchange message in OV if power supply is removed.
Explanation: Two traps entConfigChange and chassisTrapsAlert will be generated if we remove the power supply.

PR **158888** Build: 6.4.4.539.R01
Summary: The default (blt) network group Switch cannot be used via Omni Vista.
Explanation: Policy Switch Network group can be used from LDAP for QOS configuration

PR	**171193**	Build:	6.4.4.540.R01
Summary:	OS6250 crashed with taEthOAM_NI task suspended when tried to pull statistics from SAM.		
Explanation:	Optimize memory management on receiving CFMs over SAA configured		

PR	**172210**	Build:	6.4.4.545.R01
Summary:	Switch crashed due to suspension of bcmRX and tCsCSMtask2		
Explanation:	Added A Null check to Prevent the crash		

PR	**170039**	Build:	6.4.4.547.R01
Summary:	Stack split happened and unit remaining "down". LED is blinking as normal on that unit		
Explanation:	Stack Debug Log enhanced and stack split timeout increased to 60 seconds		

Problems Fixed Between Builds 552 and 559

PR	**171633**	Build:	6.4.4.554.R01
Summary:	Few SVLAN information missing from H/W table once transparent bridging config applied		
Explanation:	On SVLAN addition and deletion: Handle TB manipulations for SVLAN in NI		

PR	**172809**	Build:	6.4.4.554.R01
Summary:	Inconsistency between boot.cfg and "show configuration snapshot" after upgrade from AOS 6.3.4.R01		
Explanation:	VSTK MIP: Correcting aggregate port handling in show commands		

PR	**169391**	Build:	6.4.4.555.R01
Summary:	High Memory Utilization is OS6855		
Explanation:	Optimize memory management when traps are absorbed.		

PR	**172494**	Build:	6.4.4.555.R01
Summary:	Multicast prune is not forwarding within 2 seconds and it takes 2 1/2 min in pim dense		
Explanation:	Assert information is cleared when state moves to no-info and re-assertion is started		

PR	**171954**	Build:	6.4.4.556.R01
Summary:	OS_6850 crash with QOS task suspend		
Explanation:	Prevented Invalid FD access while accepting the sockets for HIC Re-Directed Packets and Introduced age out concept to Stale File Descriptors for connection which is opened more than 2 minutes, so that valid/further sessions can get accepted without any issues		

PR	**172211**	Build:	6.4.4.557.R01
Summary:	Intermittent BGP routes are missing in the routing Table		
Explanation:	Overlapping routes display issue in BGP is fixed		

PR **173649** Build: 6.4.4.558.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 **170080** Build: 6.4.4.558.R01
Summary: Issue with "show aaa-device all-users" output.
Explanation: Show aaa-device all-users will display all the clients in the switch.

Problems Fixed Between Builds 560 and 569

PR **172374** Build: 6.4.4.560.R01
Summary: Issue with QoS command "show policy classify l3" on OS6850.
Explanation: Added an option to view the pending policies in the show policy classify CLI command

PR **173195** Build: 6.4.4.560.R01
Summary: MAC OS does not gets the temporary Ip address on Captive portal setup
Explanation: Parameter Request List (option 55) is parsed and handled only for DHCP-Inform packet in case of both windows and mac operating system in Captive Portal State.

PR **173657** Build: 6.4.4.560.R01
Summary: "maximum bandwidth 0K" doesn't work immediately
Explanation: Configure 0 depths when bandwidth is 0. Hence not allocating any tokens for packet to go through.

PR **169877** Build: 6.4.4.564.R01
Summary: Attempt to copy working to cert w/flash synchronization failed
Explanation: Reset the flash synchro global flags in all units.

PR **174577** Build: 6.4.4.565.R01
Summary: "user password-policy cannot-contain-username" shown incorrectly under show configuration snapshot
Explanation: Changes done to update running configuration correctly

PR **174607** Build: 6.4.4.565.R01
Summary: CPLD version not updating correctly in swlogs
Explanation: Corrected the CPLD version number for 6850E in swlogs

PR **174818** Build: 6.4.4.566.R01
Summary: OS6850 stack split with dump files, keep crashing and taking over the primary role
Explanation: Validate bootp length for all incoming Bootp/Dhcp Packets

PR **175088** Build: 6.4.4.568.R01
Summary: OS9700E crashed with task tsMplsNi in suspended state.

Explanation: MPLS Reconnection mechanism is changed properly

Problems Fixed Between Builds 570 and 577

PR **174980** Build: 6.4.4.570.R01
Summary: dhcpd server crashes switch when Windows 7 computer with long name requests DHCP
Explanation: Coded to log host name separately, so it can get enough buffer size

PR **174849** Build: 6.4.4.570.R01
Summary: VRRP BFD session still UP after BFD process completely disabled
Explanation: Stamp 802.1q with priority 6 for BFD Control and Echo Packets
Handle Link-Agg and ARP Resolution Events for Sessions which are not in ADMIN_DOWN state only.

PR **174389** Build: 6.4.4.570.R01
Summary: Information on log message - debug1 : Sending Violation Shutdown Trap for IfIndex 13 with value 1600
Explanation: Correcting the debug message to include the correct parameters during display

PR **173643** Build: 6.4.4.570.R01
Summary: netJobRing overflow in 6850E and crash analysis required
Explanation: IPEDR will not use the global semaphore to lock the interface list

PR **175794** Build: 6.4.4.570.R01
Summary: Stack Split / Crash
Explanation: Validate malloc failure when switch is trying to synchronize dhcpBind.db

PR **173595** Build: 6.4.4.570.R01
Summary: BFD session DOWN on one side only
Explanation: Don t configure egress mask for Network ports in MPLS

PR **174753** Build: 6.4.4.570.R01
Summary: BFD tearing down OSPF sessions causing more than 30s failover time
Explanation: Stamp 802.1q with priority 6 for BFD Control and Echo Packets
Handle Link-Agg and ARP Resolution Events for Sessions which are not in ADMIN_DOWN state only.

PR **175082** Build: 6.4.4.571.R01
Summary: OS9700/9600 NI reset with PMDs when trying to test the hot swap.
Explanation: Fix done not to send ERP_CONFIG_NOT_CERTIFIED or any message to Ni while takeover is in progress.

PR **176137** Build: 6.4.4.574.R01
Summary: client cannot get DHCP IP-address behind the IP Phone on mobile port
Explanation: MAC addition into LPS RBT tree will be done properly for LPS enabled mobile ports

PR **172594** Build: 6.4.4.577.R01

Summary:	VIP ping losses received while CMM failover and Ip dos anti-spoof command enabled.		
Explanation:	Remove VRRP spoof entries from hardware on takeover		

Problems Fixed Between Builds 578 and 585

PR	**175249**	Build:	6.4.4.578.R01
Summary:	Auto-negotiation not working properly on 6850E only for 100Mbps patch cable.		
Explanation:	Auto-negotiation works properly on OS6850E when 100Mbps patch cables connected		

PR	**176082**	Build:	6.4.4.578.R01
Summary:	In "reload all at" command seconds difference seen		
Explanation:	"Reload all at" command shows exact seconds at which the reload has been planned.		

PR	**175703**	Build:	6.4.4.578.R01
Summary:	Remote host device shows as unknown for OS6450 on OS6850		
Explanation:	Code changes done to display correct name in Remote host device in "show amap" output for missed OS6450 products		

PR	**176573**	Build:	6.4.4.578.R01
Summary:	Remote command-log does not include IP address of session at the syslog		
Explanation:	Code changes done to send value 0 as argument for show Debug while sending command info to the session managerr for logging		

PR	**176593**	Build:	6.4.4.579.R01
Summary:	OS 9700E switch crashed with tSLNAdrLrn task suspension.		
Explanation:	Defensive fix have made so that it won’t call semTake if the sem id is zero.		

PR	**170703**	Build:	6.4.4.579.R01
Summary:	IP CAM not getting power when connected to OS6850E		
Explanation:	Code changes done to change the threshold of the fold back protection from a voltage drop of 10V down to a drop of 35V by setting the appropriate PoE register.		

PR	**174214**	Build:	6.4.4.579.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	**143591**	Build:	6.4.4.580.R01
Summary:	OS6850 - Flood rate limitation due to 224 bytes bcast packets sent by IP-based audio solution		
Explanation:	Disabling Storm Control when detected speed and configured flood limit are equal		

PR	**176341**	Build:	6.4.4.581.R01
Summary:	100% CPU utilization due to IPv6 Neighbor Solicitation packets copied to CPU by default		

Explanation: Debug cli to set or reset trapping of unknown ipv6 multicast, neighbor solicitation, and Martian packets to CPU is introduced. By default it is enabled.
To disable this feature following Command can be used
debug ipv6 set ipv6ControlProtocolDisable 0
NOTE: disabling this flag will modify switch behavior not to accept any multicast control packets, neighbor solicitation packets, and Martian packets. So protocols using this Multicast control packets (ff02 ::) will not work when disabling this feature.

PR **176617** Build: 6.4.4.582.R01
Summary: Qos user port configuration gets changed after a reload.
Explanation: qos user port filter and shutdown uses the single list for parsing the configurations, Need to reset the list once the parsing was done for the particular category.
Ensure the configuration applied for one category should not reflect in other.

Problems Fixed Between Builds 586 and 603

PR **177175** Build: 6.4.4.588.R01
Summary: 50Ms convergence not achieved on a ring of 7 switches with 1gig fiber ports
Explanation: Link Down detection for 1G port have been fasten up to achieve ERP convergences

PR **176699** Build: 6.4.4.589.R01
Summary: Some qos policies randomly applied to UNP profile are not working
Explanation: Policy list will be updated only for the clients (supplicant/non supplicant) who have been associated with the policy list.

PR **177223** Build: 6.4.4.589.R01
Summary: Duplicate line appear after upgrade from 6.3.4 to 6.4.4.559.R01
Explanation: Mip-Overflow for E-service NNI Link-Agg is handled properly

PR **177303** Build: 6.4.4.589.R01
Summary: Config for ethernet service svlan done but not shown on "show configuration snapshot".
Explanation: Mip-Overflow for E-service NNI Link-Agg is handled properly

PR **175805** Build: 6.4.4.589.R01
Summary: LLDP log messages does not have port information
Explanation: Added the port information for LLDP log messages in slot/port format.

PR **176940** Build: 6.4.4.590.R01
Summary: Reload command not working after upgrading the stack from 6.4.4.415 R01 to 6.4.4.577 R01.
Explanation: Exit from dshell as well when remote connection to the IDLE units ended

PR **177171** Build: 6.4.4.591.R01
Summary: IGMP General Queries are not forwarded when non-unicast hashing is enabled

Explanation: Software flooded multicast packets would be transmitted in intelligent mode if non-unicast hashing is enabled

---

PR **176455** Build: 6.4.4.591.R01
Summary: "IP-HELPER warning Corrupted UDP frame! bplen:303 efp->length:350" messages in the switch logs of OS
Explanation: Have done changes to allow packets when trailer byte is added at the end

---

PR **177453** Build: 6.4.4.592.R01
Summary: CTRL + keys trigger OS6850 reboot
Explanation: Bypass SIGQUIT signal processing on IDLE units CLI.

PR **177585** Build: 6.4.4.592.R01
Summary: dense mode multicast flows partially lose after several link/up/down on the Core
Explanation: Dense mode multicast flows partially lose after several link/up/down issue fixed

---

PR **177069** Build: 6.4.4.592.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 **176700** Build: 6.4.4.595.R01
Summary: Random 802.1x clients are not getting authenticated once we reboot 6850 and 9000
Explanation: The new CMM variable "onexCMMFirstRunup" introduced to differ the authentication process and set NI variable onexFirstRunup in all NIs via AlcatelDebug.cfg.

PR **177722** Build: 6.4.4.595.R01
Summary: IGMP General Queries are sent back on uplinks
Explanation: Issue with non-uc hash mode fixed.

PR **177682** Build: 6.4.4.595.R01
Summary: Switch crash with task taEthOAM_NI suspend
Explanation: Initialized the ethoam attribute variables during Init

---

PR **177971** Build: 6.4.4.595.R01
Summary: Corrupted UDP frame received in 6.4.4.585R01
Explanation: Since trailer byte is getting added at the end, message "corrupted UDP frame" is displayed. In order to find out the port no and mac address from where the packet is received, they are included in the warning message.

PR **177386** Build: 6.4.4.597.R01
Summary: DHL slow convergence time
Explanation: On DHL ports, flush mac based on protected and unprotected vlan bits

PR **177340** Build: 6.4.4.598.R01
Summary: Need to know the root cause for the OS6850 slot-1 crash.
Explanation: we introduce semaphore for the global structure with timeout value 2 , Ad8021xPort in order to avoid simultaneous read write

Problems Fixed Between Builds 604 and 623

PR **178444** Build: 6.4.4.605.R01
Summary: Please allow configuration of ipedrArpUnreachAge with millisecond granularity
Explanation: The delay between inter-ARP messages is implemented at millisecond level granularity. The value of ipedrArpUnreachAge can now be set at ms level.

PR **179245** Build: 6.4.4.606.R01
Summary: can display extended stats only for rule having split source port group!" even though all rules having
Explanation: Throw error only when the policy rule is in non-split mode

PR **178145** Build: 6.4.4.606.R01
Summary: Reference to the PR# 177283. I have opened new PR.
Explanation: Crash due to invalid payloadlen value fixed.

PR **176959** Build: 6.4.4.607.R01
Summary: ARP entry of print box aging out in combination with NAC setup on particular stack
Explanation: Proper handling of CCODE in case of ARP packets received on a .1x port

PR **178228** Build: 6.4.4.607.R01
Summary: "STR FATAL" error raised while checksum calculation
Explanation: Closed the unused file system fd before creating new fd

PR **178616** Build: 6.4.4.607.R01
Summary: 802.1x MAC in filtering when takeover of PRI unit while PC went to hibernating
Explanation: Hardware learning status for .1x Macs are properly updated in SLN database

PR **178863** Build: 6.4.4.607.R01
Summary: Unable to authenticate AVLAN after upgrading from 6.3.4.R01 to 6.4.4.585.R01 and Error message "qDis
Explanation: C code is not handling properly when avlan port-bound is enabled. Code changes are done to flush the c code entry when the process gets done.

PR **179287** Build: 6.4.4.608.R01
Summary: temperature sensor problem on some devices (i2cRandomRead ERROR)
Explanation: Swlog messages are added to display port number in which the sfp inserted that is responsible bus bus lock up

PR **179602** Build: 6.4.4.608.R01
Summary: Account terminates cause seen on the interim update.
Explanation: Code changes has been done to display the acct-terminate-cause only in the stop

packet

PR	**179722**	Build:	6.4.4.608.R01
Summary:	alaDoSTrap DoS Type: 14		
Explanation:	MIB is defined for anti-spoofing dos type		

PR	**178348**	Build:	6.4.4.608.R01
Summary:	"Read-only MIb are not accessible.		
Explanation:	Access permissions for some objects of alaDot1xDeviceStatusTable are changed to read-only.		

PR	**178227**	Build:	6.4.4.608.R01
Summary:	"Automatic Remote configuration download" does not work		
Explanation:	Timeout interval is 30s by default. Introduced a global variable "rmtCfgTimeoutInterval" to increase the timeout interval.		

PR	**179794**	Build:	6.4.4.609.R01
Summary:	"debug ip set ipedrArpUnreachControl 0" is present in running config by default		
Explanation:	When only icmp unreachable host-unreachable is configured, ICMP un-reachable message would be sent to only the source which has initiated the ARP in the switch. All other following source packets would not be responded by ICMP un-reachable message. After ARP entry is timed out, again if new source initiates the ARP entry in the switch a new ICMP un-reachable message would be generated to the new source. ======== NOTE: For complete (existing) functionality both icmp unreachable host-unreachable and debug set ipedrArpUnreachControl 0 should be configured. ========		

PR	**177918**	Build:	6.4.4.610.R01
Summary:	PoE devices are powered during boot up process then unpowered and powered back once again		
Explanation:	Fixed the issue of PoE devices powering up during boot-up in OS6400-P24. CPLD upgrade need for this from version 16 to version 17.		

PR	**179610**	Build:	6.4.4.611.R01
Summary:	Switch crashed due to data exception in IPMS-NI.		
Explanation:	Added debugs to dump the packet in pmd if there is a corruption of ethernet frame pointer and data portion of the packet		

PR	**179968**	Build:	6.4.4.612.R01
Summary:	ARP specific QoS rules cannot be logged		
Explanation:	ARP specific QoS rules can be logged		

PR	**178702**	Build:	6.4.4.613.R01
Summary:	DHCP release packets seen twice on NNI port.		
Explanation:	By disabling snooping in that vlan, two release packets are not seen and also client interface in that switch can get ip		

PR	**180283**	Build:	6.4.4.614.R01
Summary:	BFD session does not come up when slot 1 come up as secondary.		
Explanation:	While handling takeover send NBR DOWN message to static routes which have bfd enabled and has gone down due to takeover event		
PR	**180623**	Build:	6.4.4.614.R01
Summary:	In Omni Switch OS6400/OS6850RE,"Running configuration and saved configuration are different" is shown		
Explanation:	Modified the behavior of Show Configuration Status to sync with CMM Configuration Status		
PR	**179239**	Build:	6.4.4.614.R01
Summary:	OS9800 Ni 8,7,9,11 and 16 rebooted in the 2 core switch. ipcTech logs and NI.pmd and cmm.Ni.pmd file		
Explanation:	Third party fix to speed up flush API		
PR	**179971**	Build:	6.4.4.616.R01
Summary:	Stack of 6850 crashed due to the suspension of the task "taLnkAgg "		
Explanation:	As per the customer request defense check have been made not to access invalid memory pointer and also debugs has been added to track the task which corrupts the pointer		
PR	**177629**	Build:	6.4.4.617.R01
Summary:	CMM takeover happened and all NIs were RESET impacted the service.		
Explanation:	to introduce task delay between successive reads of the temperature sensor once the temperature goes beyond the danger threshold. This would enable the system to buy more time and ascertain if the temperature increase is genuine prolonged		
PR	**179629**	Build:	6.4.4.618.R01
Summary:	Swicth rebooted with the "tsStatistic (82fe080) @ 94 SUSPEND+I lckd=0 ME DS stk 82fe080-82fc140" tas		
Explanation:	Changes done to prevent i2c bus lock up if i2c errors are due to sfp devices. Only further i2c access to that particular sfp device will get blocked.		
PR	**181063**	Build:	6.4.4.620.R01
Summary:	ARP request packets are not flooded in a LAG in MPLS setup		
Explanation:	Non unicast Load Balancing over Linkagg is extended to VPLS Ports (Traffic)		
PR	**181230**	Build:	6.4.4.621.R01
Summary:	PXE clients unable to get DHCP IP addresses with UDP relay configured on OS9702(6.4.5.R01.445)		
Explanation:	Don t configures VPA for ports which are not part of the linkagg.		
PR	**181087**	Build:	6.4.4.621.R01
Summary:	CTRL+* during stack reload crashes stack units		
Explanation:	Code change done to avoid taking mutex In order to avoid incomplete pmd file generation		
PR	**176883**	Build:	6.4.4.622.R01

Summary:	OS9-GNI-C24E module crashed showing Hi gig link down messages in switch logs.		
Explanation:	Implementation of a trap to notify the user on NI reset due to fabric errors.		

Problems Fixed Between Builds 624 and 630

PR	**181615**	Build:	6.4.4.624.R01
Summary:	ICMP reply sent on Admin down port of Linkagg		
Explanation:	ICMP reply sent on Admin down port of Linkagg. Customer faces connectivity issues when 4 ports of a linkagg are down. The packets were trying to go through one of the ports which is already down.		

PR	**181474**	Build:	6.4.4.624.R01
Summary:	BFD session does not come up when slot 1 come up as secondary		
Explanation:	Proper source and destination is done while handling takeover functionality in BFD		

PR	**181386**	Build:	6.4.4.624.R01
Summary:	Unable to view configuration (show configuration snapshot), when ipv6 interface is up.		
Explanation:	NTP configuration was causing the problem.		

PR	**181245**	Build:	6.4.4.625.R01
Summary:	Issue#5: Switch crash when dhcp server config contains mac-address with ":" instead of a "-"		
Explanation:	code changes has been done to accept the mac address specified with both colon and hyphen while parsing the configuration file		

PR	**180822**	Build:	6.4.4.625.R01
Summary:	Query upgrading SSH Version to 5.2		
Explanation:	The order of selection of the ciphers is changed so that it will consider AES CTR mode and arc four ciphers are not vulnerable to this attack.		

PR	**181233**	Build:	6.4.4.625.R01
Summary:	OS 6850 Loopback-detection not working		
Explanation:	Reducing LBD Tx timer to 1 second		

PR	**180602**	Build:	6.4.4.625.R01
Summary:	High CPU issue on stack due to SrcLrn task hogging CPU.		
Explanation:	High CPU was observed due to read operation over the duplicate static MAC present on one port, root cause of the issue was , during boot up static MACs on LPS port were moving from their tagged vlan 1 to default vlan of the LPS port . This was the coroner case where MACs were configured in vlan 1 which was tagged vlan of LPS port .Check introduced to prevent the reconfiguration of the vlan 1 (tagged +static mac in boot.cfg at time of boot up .		

PR	**181187**	Build:	6.4.4.625.R01
Summary:	switch crash when BGP prefix list command with length		
Explanation:	Validation to check whether bgp policy prefixlist is created before configuring the conditions		

PR	**179967**	Build:	6.4.4.626.R01
Summary:	High CPU Noticed in stack of 6850		
Explanation:	debug cli to disable L3 slow path CPU is introduced. By default it is enabled. To disable the following Command can be used "debug ip set ipv4L3SlowPathToCpu 0"		

PR	**181919**	Build:	6.4.4.627.R01
Summary:	We lost some streams of mcast during some failover test cases.		
Explanation:	During clearing of hardware index for Multicast flows, proper cleaning up of hardware resources was carried out		

Problems Fixed Between Builds 631 and 645

PR	**182637**	Build:	6.4.4.633.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	**182391**	Build:	6.4.4.633.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	**181724**	Build:	6.4.4.633.R01
Summary:	SrcLrn, tOddJob, tSlcAgeTimer, tSlcHgTimer, la_cmm_tick, stpTick & tahw_l2		
Explanation:	As per our analysis the RCA of the issue is currently we have not validating the length of the buffer received for IPC transmission. This result in crash on the system whenever the buffer size is Zero. We have done code changes for validating the length of the buffer before sending to the destination Application.		

PR	**182836**	Build:	6.4.4.633.R01
Summary:	OSPF LSA type 5 never aged out and don't have a reason to exist in the OSPF DB at all		
Explanation:	There was a protocol value mismatch. We were using the protocol value of old route for new LSA entry. Have corrected this.		

PR	**182667**	Build:	6.4.4.633.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	**181179**	Build:	6.4.4.634.R01
Summary:	Reference PR# 173309: dhcpd server does not propagate global scope:		
Explanation:	DHCP options given in global scope will now be applied to local scope also.		

PR	**182765**	Build:	6.4.4.636.R01
Summary:	EXIT command issue with OmniSwitch.		

Explanation: Changes have been done to intimate accounting command information for exit command to tacacs server even there is no configuration

---

PR **182768** Build: 6.4.4.636.R01
Summary: Not all commands are sent to TACACS+ server to be authorized from the Omni Switch.
Explanation: We have done changes for whoami and history size. we have added these commands to session management families.

PR **182223** Build: 6.4.4.636.R01
Summary: OS6850 stack switch has been crashed "tCS_PRB & taIpni" task is suspended.
Explanation: changes done to drop the ARP packets received on hi gig port

---

PR **183031** Build: 6.4.4.636.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 **182918** Build: 6.4.4.637.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 **183211** Build: 6.4.4.638.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 **181917** Build: 6.4.4.639.R01
Summary: DS node failure: 100-105 sec convergence in Multicast
Explanation: Linkagg events in BFD is handled properly so that number of sessions in a slot is tracked properly

---

PR **169150** Build: 6.4.4.639.R01
Summary: OS6250 doesn't generate any trap when connectivity to a MEP is restored
Explanation: Trap will be generated when MEP connection is restored.

PR **182659** Build: 6.4.4.639.R01
Summary: Tacacs+ security issue with Omni Switch.
Explanation: Tacacs Authorization replies will be processed in order with the help of unique reference for each truncation which will avoid security issue due to stale replies.

PR **181508** Build: 6.4.4.642.R01
Summary: ntp server configuration does not store IP Address of NTP server, instead it

resolves NTP server to
Explanation: Controlling the snapshot of NTP configuration to store the IP address

---

PR **184068** Build: 6.4.4.642.R01
Summary: Stack got crashed while performing QOS changes
Explanation: As the crash is not re-creatable, provided defensive fix.

PR **183931** Build: 6.4.4.642.R01
Summary: Synchronization failed on 2*OS6850-P24X and 1*OS6850E-P48X stack when applying copy working certified
Explanation: Increased the maximum wait time for time zone update across cmm

---

PR **183531** Build: 6.4.4.642.R01
Summary: Swlog filled with error message "qosNiRDPbrUpdateNhipEntry: entry_reinstall returned -4"
Explanation: Error "qosNiRDPbrUpdateNhipEntry: entry reinstall returned -4" will not be thrown.

PR **183951** Build: 6.4.4.642.R01
Summary: Service sap-using sap gives error for a specific sap.
Explanation: Proper validation of linkagg ports in SAP configuration carried out

---

PR **185017** Build: 6.4.4.643.R01
Summary: Mac movement issue during DHL convergence when MAC flush mode is "RAW".
Explanation: Proper Gport validation while generating packets during DHL port change

---

PR **182585** Build: 6.4.4.643.R01
Summary: Issue with DHCP-snooping
Explanation: 1. When the NI is powered up, the Chassis supervision sends a NI_UP message to UDP relay application, after this, UDP relay initiates socket communication with the NI and, when this is successful we consider that the NI is ready.
2. For incorrect linkagg port entry, we have implemented a method to automatically scan all trusted ports using a timer (runs 240 secs after the application is initialized and during takeover) which are a part of a linkagg and update the linkagg port details in UDP relay CMM context if they are not updated correctly.

PR **184568** Build: 6.4.4.643.R01
Summary: MC Hashing Issue/ Load distribution af LAGs
Explanation: New CLI Implemented

PR **184689** Build: 6.4.4.643.R01
Summary: qos trust Port got shutdown with protocol dhcp-server or dns-reply
Explanation: While processing for QOS shutdown, process only first packet of fragmented packet and not all the fragmented packets

---

PR **185296** Build: 6.4.4.644.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.

Problems Fixed Between Builds 646 and 669

PR 185058 Build: 6.4.4.646.R01
Summary: tDvmrp0 ,tCsCSMtask2 and tCS_PRB. These are the tasks suspended and locked.
Explanation: Fix to avoid null pointer access

PR 183281 Build: 6.4.4.646.R01
Summary: Port status is showing as forwarding in spite there is no link connected on the interface.
Explanation: When the port physically goes down it should not be displayed in "show spantree active ports" output

PR 183948 Build: 6.4.4.646.R01
Summary: Stack crashed due to tCS_PRB and Qos task suspension when QOS is added or deleted.
Explanation: When qos is added or deleted switch wont crash.

PR 184016 Build: 6.4.4.646.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 183528 Build: 6.4.4.647.R01
Summary: SVCMGR error smgrMIPReactorReceive: MIP queue error! Line=2609
Explanation: Switch will not crash when SNMP Get operation is done with invalid index for object "alaServiceMgrPortMode".

PR 182755 Build: 6.4.4.647.R01
Summary: OV traps seen Vs switch logs events discrepancies.
Explanation: Rectifying discrepancy of timestamp between OV and the switch.

PR 180957 Build: 6.4.4.648.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 184739 Build: 6.4.4.648.R01
Summary: Change the frequency of swlog messages.
Explanation: Code changes have been done for changing the frequency of printing low flash messages in swlog.

PR 185304 Build: 6.4.4.648.R01
Summary: Switch loses its connection after issuing the command "no mac-address-table"
Explanation: Do not delete the mac-address if mac-port is cpu port

PR 185728 Build: 6.4.4.649.R01

Summary: OS9700 crashed with generating PMD files with "NISP" & "tSLNAdrLrn" task is suspended.

Explanation: Code changes have been done to pass the correct vlan information to the bcm .

PR **184858** Build: 6.4.4.649.R01

Summary: DDM threshold temperature alarm.

Explanation: Code changes done to prevent warning message until SFP reads the exact DDM values.

PR **184393** Build: 6.4.4.650.R01

Summary: After power cycle the snmp access is allow for few minutes without aaa authentication default l

Explanation: Fix done to disallow the access to the snmp server immediately after power cycle, when there is no aaa authentication snmp configuration.

PR **186908** Build: 6.4.4.650.R01

Summary: Switch crashing because of vlan name length.

Explanation: The size of the data structure that holds the VLAN name was increased to avoid overflow.

PR **186886** Build: 6.4.4.652.R01

Summary: How to delete a particular alias information in 6850 device

Explanation: Fix done to delete particular alias information using no alias command.

PR **185448** Build: 6.4.4.652.R01

Summary: ERP ring got blocked due to UDLD flood and switch got crashed with generating PMD file with suspended

Explanation: Prevent UDLD configuration for aggregate port or tagged aggregate port

---

PR **185999** Build: 6.4.4.654.R01

Summary: Issue with SFP-DUAL-SM10 with Omni switch with OS9-GNI-U24.

Explanation: Rectifying discrepancy in setting speed to 100 in a dual speed SFP

PR **187156** Build: 6.4.4.655.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 **186840** Build: 6.4.4.656.R01

Summary: Switches hang with error logs display and unable to console or SSH: memPartAlloc: block too big - 37

Explanation: Errors related to Memory leak in SAA module are corrected.

PR **187475** Build: 6.4.4.657.R01

Summary: Show interfaces link-monitoring statistics command not executing past interface 3/42

Explanation: Fix done to handle the proper mip overflow condition to execute the "Show interfaces link-monitoring statistics command" correctly.

PR **187081** Build: 6.4.4.657.R01
Summary: OS 6850 crashed with Stp task suspended.
Explanation: Defense validation while handling STP SNMP operations

PR **187641** Build: 6.4.4.657.R01
Summary: OS 6850 MAC authentication issue
Explanation: Ingress/ egress bandwidth parameters of UNP are initialized to proper default value; such UNP configurations through OV/Web view are correctly configured.

PR **188344** Build: 6.4.4.658.R01
Summary: DHCP relay and per VLAN IP helper information configured together on Omni Switch.
Explanation: Check agent information status before configuring dhcp-snooping

PR **188063** Build: 6.4.4.658.R01
Summary: A CLI debug command to control "bcmSwitchL3UcTtlErrToCpu"
Explanation: A new debug cli command bcmSwitchL3UcTtlErrToCpu introduced. bcmSwitchL3UcTtlErrToCpu = 0 means IP error packets will not be sent to CPU

PR **188695** Build: 6.4.4.659.R01
Summary: Issue with ip dos anti-spoofing clear command.
Explanation: statistics command will not change the configuration status of the switch

PR **187286** Build: 6.4.4.659.R01
Summary: With "show 802.1x non-supplicant users" command not showing the correct output.
Explanation: Fix done to handle the proper mip overflow condition to execute the "Show 802.1x non-supplicant" correctly.

PR **188374** Build: 6.4.4.661.R01
Summary: duplicate line appear in boot.cfg file
Explanation: Changes done to prevent MIP overflow in ethernet service and interfaces modules.

PR **185794** Build: 6.4.4.661.R01
Summary: OS 6400 crash issue
Explanation: Additional debug addition for crash issue.

PR **183025** Build: 6.4.4.664.R01
Summary: Unknown policy issue with 802.1x Authentication
Explanation: Changes done to resend the client MAC , if stuck in unknown policy during authentication process due to bulk authentication and IPC configuration.

PR **190230** Build: 6.4.4.668.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 **189787** Build: 6.4.4.669.R01

Summary: aaa ldap server configuration generating Command syntax error on OS6850 switch with 6.4.4 645 R01

Explanation: Fix done not to generate the syntax error for aaa ldap server configuration

Problems Fixed Between Builds 670 and 707

PR **190105** Build: 6.4.4.670.R01

Summary: Swlog were filled with the I2C error and bad SFP message and DSHELL got frozen after applying the co

Explanation: Changes done to isolate the i2c device which initially triggers i2c errors and to recover from i2cbuslock up by unlocking the bus after timeout

PR **190576** Build: 6.4.4.670.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 **190680** Build: 6.4.4.670.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 **189784** Build: 6.4.4.670.R01

Summary: Switch memory utilization increases and exceeds threshold.

Explanation: Code changes are done to prevent IPC congestion between STP CMM and STP NI

PR **191198** Build: 6.4.4.670.R01

Summary: Show stack status shows negative value for token used

Explanation: On reassignment of previous module IDs back to a re-joined stack element, the count of allocated module IDs is decremented from "available token count".

PR **191676** Build: 6.4.4.671.R01

Summary: OS6850 switch crashed with suspended tasks: tCS_PRB and taIpni

Explanation: Defensive check added.

PR **191795** Build: 6.4.4.671.R01

Summary: Static route not showing the snapshot but however throwing the message "Static route already exists"

Explanation: Including the entry causing mip_over flow in show configuration snapshot ip-routing.

PR **190971** Build: 6.4.4.671.R01

Summary: "zcSend" CODE 3997698 0x3d0002" error seen in logs and unable to save the configuration

Explanation: Merge done in 645R02 for to avoid the web view permanent stuck due to temporary socket errors and hence web view communication with the other tasks will not be affected.

PR **191769** Build: 6.4.4.671.R01

Summary:	ifConnectorPresent MIB (ifXTable) displays true value instead of False for LACP aggregate links.		
Explanation:	Condition introduced to check for the linkagg and update the value of if-connector present.		

PR	**191588**	Build:	6.4.4.672.R01
Summary:	BPDU Shutdown failure: qos user-port link-shutdown bpdu does not seem to shut down the ports		
Explanation:	With this change port shutdown properly.		

PR	**191740**	Build:	6.4.4.673.R01
Summary:	High Memory issue on OS6850.		
Explanation:	Code changes are done to free the allocated memory for HIC Svr monitoring packet.		

PR	**189881**	Build:	6.4.4.674.R01
Summary:	Issue with time synchronization with NTP on Layer 2 switch		
Explanation:	Changes have been made to set the dispersion value to the sample dispersion value in the case of global variable "ntpAccept" enabled.		

PR	**192263**	Build:	6.4.4.676.R01
Summary:	End user policy is violated when port-security is configured on all the ports.		
Explanation:	End-user profile check is added in LPS source learning.		

PR	**192654**	Build:	6.4.4.677.R01
Summary:	OS6850-802.1X users did not display in show command.		
Explanation:	Fix done to display all the onex clients’ information in global display when there are forced authorized ports present.		

PR	**191570**	Build:	6.4.4.678.R01
Summary:	L3 slow path CPU processed packets caused network instability (CPU running at 100% utilization)		
Explanation:	By default ip packets with options won't be trapped to CPU. Only when IPV6 interface is present or ipv6 multicast is enabled, ip packets with options will be trapped to CPU.		

PR	**193812**	Build:	6.4.4.684.R01
Summary:	Optical Port Physical Backup(OPPB) both ports are DOWN		
Explanation:	Fix done for the issues seen while handling timer expiration of OPPB backup Port		

PR	**193900**	Build:	6.4.4.686.R01
Summary:	LPS query on learn-trap-threshold in OS6850 and OS6400		
Explanation:	Fix done to display the trap-threshold configured value if it’s not 0.		

PR	**194004**	Build:	6.4.4.687.R01
Summary:	Ouput of show interface link-monitoring statistics missing few interfaces in all chassis after 3rd i		
Explanation:	Fix done to avoid MIP overflow		

PR	**193600**	Build:	6.4.4.689.R01
Summary:	Egress port sampling across routed traffic is not working in 6850 (non-E)		
Explanation:	Added CPU_PORT in port library for OS6850/OS6400/OS97E/OS6855.		

PR	**194868**	Build:	6.4.4.690.R01
Summary:	OS6400 : Lan power stops working, no logs reported. Available watts shows 0 in lpDumpData () output.		
Explanation:	Fix done to display the correct watts available in lpDumpData().		

PR	**194353**	Build:	6.4.4.691.R01
Summary:	OS6850E crashed with SNMPagt & tCS_PRB tasks		
Explanation:	Code changes done to ensure accessing valid varbind during bulk request		

PR	**194549**	Build:	6.4.4.693.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	**195374**	Build:	6.4.4.694.R01
Summary:	SNMP get gives back different descriptions for the same power supply.		
Explanation:	Fix done to display power supply details properly via SNMP.		

PR	**195589**	Build:	6.4.4.695.R01
Summary:	OS6850-U24X: Omni switch crash without any apparent reason.		
Explanation:	Fix done to check the SVLAN ID 0 for Ethernet service.		

PR	**195956**	Build:	6.4.4.700.R01
Summary:	LACP configuration lost instead of UDLD after software updating		
Explanation:	Now the configurations of LACP can be done prior to the UDLD configurations.		

Problems Fixed Between Builds 708 and 743

PR	**197237**	Build:	6.4.4.708.R01
Summary:	SFP MfgName not displayed in the correct OID and query regarding the model number in the power supply		
Explanation:	Code changes done to display manufacturer name in proper OID.		

PR	**197786**	Build:	6.4.4.709.R01
Summary:	OS6850: DHCPv6 does not work with DHCP Snooping		
Explanation:	DHCPV6 packets are getting dropped when ipv4 dhcp-snooping is enabled. So fix was made in such a way that if dhcpv6 packet is present and ipv4 dhcp snooping is enabled flood the dhcpv6 packets.		

PR	**197568**	Build:	6.4.4.710.R01
Summary:	Multicast rp-candidate issue with OS6850E.		
Explanation:	PIM-Bootstrap fragmentation issues fixed		

PR	**198586**	Build:	6.4.4.713.R01
Summary:	OpenSSH version upgrade query. OS6850E.		
Explanation:	CVE-2010-5107, CVE-2011-5000, CVE-2010-4755 : Vulnerabilities for OpenSSH 5.0		

PR	**197294**	Build:	6.4.4.714.R01
Summary:	OS6850 crashed with Memory dump file.		
Explanation:	Code change to avoid NULL pointer access		

PR	**199571**	Build:	6.4.4.715.R01
Summary:	error Csnmp(4418):Next for ring :1 does not exist		
Explanation:	Message is not thrown as an error and will be logged when debug2 level is enabled		

PR	**199981**	Build:	6.4.4.719.R01
Summary:	When "ethernet-service uni-profile ieee-fwd-all" is used frames with selected destination MAC addresses are dropped on UI and NNI		
Explanation:	Corrected hardware entries to handle iee-fwd-all		

PR	**199440**	Build:	6.4.4.721.R01
Summary:	Vulnerability in SSLv3 (POODLE / CVE -2014- 3566)		
Explanation:	Disable SSLv3 to mitigate POODLE attack		

PR	**198841**	Build:	6.4.4.722.R01
Summary:	BGP route for multi-hop neighbor learnt correctly but IPRM shows incorrect gateway for this route.		
Explanation:	In bgp, if insert event or update event triggered, do not update reachability info if the cached information is through a more specific route.		

PR	**199162**	Build:	6.4.4.722.R01
Summary:	DHCP NAK packet not sent by switch acting as DHCP server		
Explanation:	On NAKing the client do subnet broadcast, when there is no relay agent.		

PR	**201549**	Build:	6.4.4.724.R01
Summary:	High CPU seen on unit 1 due to task: VstkCmm on a stack of 2 OS6850 switches		
Explanation:	Fix done to avoid high CPU in vstkcmm task		

PR	**196450**	Build:	6.4.4.724.R01
Summary:	OS6850-U24X-Mac learning on port instead of Linkagg ID.		
Explanation:	made changes to avoid callback on ports part of linkagg		

PR	**198323**	Build:	6.4.4.724.R01
Summary:	OS6850: LACP problem with hub in between LACP peers		
Explanation:	Code changes done to attach the port properly when primary NI goes down (with hub in between links)		

PR	**202166**	Build:	6.4.4.726.R01
Summary:	Switch crashed with the suspended task "tCS_CCM " "tCS_PRB "		

Explanation:	Defensive fix to avoid crash		

PR	**202348**	Build:	6.4.4.727.R01
Summary:	Switch crashed with the suspended task "tCS_CCM " "tCS_PRB "		
Explanation:	Avoid stack overflow by increasing the stack size of Stack Log task.		

PR	**202326**	Build:	6.4.4.729.R01
Summary:	Multicast does not work after VRRP master is reloaded		
Explanation:	Multicast Flood Traffic loss during the STP convergence is fixed. Linkagg to Linkagg source move		

PR	**203334**	Build:	6.4.4.730.R01
Summary:	100% CPU with task vstkcmm after OS6850 NI takeover		
Explanation:	Fixed high CPU seen in vstk cmm on repeated takeovers		

PR	**202472**	Build:	6.4.4.731.R01
Summary:	Switch crash with the suspension of the task "tCsCSMtask2" "tCS_PRB"		
Explanation:	Restricted i2c bus lock logic to OS68 U24 models and corrected associated conflicts for other Omni switch variants		

PR	**205245**	Build:	6.4.4.736.R01
Summary:	OS6850-48: High memory utilization		
Explanation:	Code changes to free the memory allocated by the taUdldNi task properly.		

PR	**205190**	Build:	6.4.4.736.R01
Summary:	Output problem of 'show linkagg' command in version 6.4.4.731, the table are not aligned when there		
Explanation:	Alignment is done Properly		

PR	**201947**	Build:	6.4.4.737.R01
Summary:	MAC movement in one VLAN flushing MAC in all VLANs when using 802.1x		
Explanation:	Fix done to avoid the onex and SL table mismatch in case of client is getting moved from supplicant to non-supplicant and again non-supplicant with diff vlan on diff ports		

PR	**205223**	Build:	6.4.4.740.R01
Summary:	MAC address table and 802.1x table inconsistency issue		
Explanation:	Code changes done to update the SL CMM data base properly when LPS enabled.		

Under Verification:

PR	**155507**	Build:	6.4.4.264.R01
Summary:	DHCP discover packets drooped when discover has different client and source MAC addresses		
Explanation:	When the mac-address verification is disabled And if the source mac address and Hardware mac-address are different, Source mac is replaced with Hardware mac address in the software mac-address list available in udp-relay module.		

PR	**155285**	Build:	6.4.4.287.R01
Summary:	Issue in "auth-server-down" with the UNP profile.		

PR	**156542**	Build:	6.4.4.349.R01
Summary:	PCs are not able to get IP address until we disable the DHCP-snooping		
Explanation:	UDP-Relay Retry Mechanism introduced for Cfg Socket. Retry Mechanism is applicable only if Socket is in DISCONNECTED.		

PR	**160013**	Build:	6.4.4.365.R01
Summary:	Stacking LEDs are OFF in a stack environment		
Explanation:	Correcting the Stack LED settings to have the Initialization of LED in ESM context		

PR	**156059**	Build:	6.4.4.377.R01
Summary:	Stack of 7: "show spanning tree ports configured" command is not showing all 7ni ports.		
Explanation:	Handle the MIP overflow for STP show CLI		

PR	**158812**	Build:	6.4.4.378.R01
Summary:	IPv4 and IPv6 ACL is causing CPU to go to 100%		
Explanation:	Corrected configuring of QoS rule in hardware for IPV6 traffic.		

PR	**157814**	Build:	6.4.4.386.R01
Summary:	NI reset and PMD generated at 8:30hrs. Ni monitoring timeout seen in log		
Explanation:	Fix to Drop ND6 packets when there is no ipv6 interface configured on the router		

PR	**158781**	Build:	6.4.4.386.R01
Summary:	wrong message on swlog file regarding telnet and ssh session using IPv6 access		
Explanation:	Modified the swlog message with correct ipv6 address when any session is initiated		

PR	**162434**	Build:	6.4.4.403.R01
Summary:	OS6850L - Display issue for "show interfaces capability"		
Explanation:	Added proper check for Lite OS6850 48 port during port initialization		

PR	**161203**	Build:	6.4.4.404.R01
Summary:	Multicast traffic stopped for some streams after takeover		
Explanation:	Multicast forwarding problem on takeover resolved		

PR	**163205**	Build:	6.4.4.417.R01
Summary:	Frames coming out of UNI ports carrying SVLAN tag when transparent bridging is enabled.		
Explanation:	With transparent-bridging enabled we ensure the untag bitmap is clear.		

PR	**163121**	Build:	6.4.4.467.R01
Summary:	Qos port ingress-bandwidth is not working for TCP		
Explanation:	qosongaruda flag to be enabled on OS6400 to ensure proper setting of configurations		

PR	**166386**	Build:	6.4.4.496.R01
Summary:	SFP+ on XNI-U12E randomly displayed with "show module long" command		
Explanation:	Code changes are done to display properly for "show module long" for SFP+ on XNI-U12E.		

PR	**159062**	Build:	6.4.4.503.R01
Summary:	OS6855 - stack unit 3 or 4 is rebooting without any reason		
Explanation:	To assign previously allocated module ids for stack slots and it units.		

PR	**159692**	Build:	6.4.4.507.R01
Summary:	OS_9000 unexpected CMM take over		
Explanation:	Code changes done to add few more information in PMD.		

PR	**171280**	Build:	6.4.4.532.R01
Summary:	ASA command getting overwritten.		
Explanation:	aaa authentication console default will not be overwritten after reload		

PR	**171547**	Build:	6.4.4.539.R01
Summary:	Port-security issue.		
Explanation:	LPS: Correcting pseudo-static MAC transitions		

PR	**167481**	Build:	6.4.4.540.R01
Summary:	OS6850E : i2c_write failed @ boot up. Manual intervention required to reload.		
Explanation:	The updated fpga kit (CPLD) version 8 for OS6850E U24X has the fix for this issue. The software workaround fix for this has been reverted		

PR	**174272**	Build:	6.4.4.570.R01
Summary:	OS9000E 100% CPU due to pim3 task		
Explanation:	Fix done for PIM task crash due to route delete in IPRM context		

PR	**175179**	Build:	6.4.4.575.R01
Summary:	OS9700/9800 Telnet not working		
Explanation:	Added debug API's to recover the opened TELNET sessions and also to dump the state information of all opened sessions.		

PR	**176313**	Build:	6.4.4.575.R01
Summary:	Network related issue while adding a second link to a static LAG.		
Explanation:	Linkagg port status is properly updated		

PR	**177269**	Build:	6.4.4.586.R01
Summary:	"qos link-shutdown bpdu" command always keeps the admin state disable.		
Explanation:	Fix to enable recovery of port after STP-S violation		

PR	**174371**	Build:	6.4.4.594.R01
Summary:	VU-101208-2: Vulnerabilities in OpenSSL		
Explanation:	Work around for using older Netscape browser and servers is not available now		

PR **180268** Build: 6.4.4.614.R01
Summary: Reference to 178515: MIB not available for the "Number of Status Change" in the "show interfaces “
Explanation: "Number of Status Change" display is added in MIB

PR **181247** Build: 6.4.4.619.R01
Summary: PIM Issue
Explanation: PIM Protocol in Omni Switches will handle jumbo frame PIM Control Packets

PR **181089** Build: 6.4.4.619.R01
Summary: Issue with BFD session
Explanation: Additional Debugging Logs has been added in BFD to narrow down the

PR **181664** Build: 6.4.4.625.R01
Summary: Ref. to PR# 178515. Customer want to use the mac-flush debug command without the timer option.
Explanation: If the MAC count is increasing too fast and the flush is not successful due to port flaps or stp port change, then following solution could be used. Here we are forcing the flush to number of times with in the same day. Earlier, we had the force flush capability once every day. This was done using "Debug source-learning forced aging cycle time <HH:MM> threshold <mac countr>"This capability is enhanced to force flush the flush the MAC address more times in a day. After setting the force cycle flush, use macPerHourFlush in AlcatelDebug.cfg to trigger flush within the same day every few\ hour’s onceIn AlcatelDebug.cfg set the value of acPerHourFlush to 1 if an hourly check is required from above time. Debug set macPerHourFlush 1The value of macPerHourFlush will control the frequency of the flush within a day. If it is set to a value 2, then flush would be done every two hours from the set time and so on.

PR **181422** Build: 6.4.4.634.R01
Summary: After upgrade to 6.4.5.442.R02, with show microcode working the code uploaded code is not shown.
Explanation: Show microcode working will show proper code uploaded in working directory.

PR **183625** Build: 6.4.4.641.R01
Summary: LSA5 (default route) does not displayed on backbone router (CBB1 and CBB2) when we add new area on back bone
Explanation: Proper bitmask used for flags which denote ospf asbr-merge. So LSA5 will be displayed on backbone router.

PR **188541** Build: 6.4.4.662.R01
Summary: MED extended power over mdi TLV not advertised on OS6850E
Explanation: Fix done to retrieve correct port power and priority info for appropriate PoE controller for 6850E and 6855 switches to perform power negotiation over lldp.

PR **192072** Build: 6.4.4.686.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 **194186** Build: 6.4.4.687.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 enabled.

PR **195083** Build: 6.4.4.692.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 **198819** Build: 6.4.4.737.R01
Summary: MAC address learnt through 802.1x state is Captive-portal CP In-Progress.
Explanation: Fix done to synchronize the onex and mac table during mac move on different ports with different vlan.

PR **203807** Build: 6.4.4.742.R01
Summary: IGMP group messages dropped on mobile/802.1x ports
Explanation: After reload, IGMP report packet on mobile port will be learnt properly

---

PR **151944** Build: 6.4.4.385.R01
Summary: running and saved config status shown as identical for any Qos related configurations
Explanation: QOS mip handled properly

PR **153204** Build: 6.4.4.511.R01
Summary: Retry and session limit option missing in dot1x web view page.
Explanation: Added a retry count and session limit parameter in web view for 802.1x module configuration

---

PR **155932** Build: 6.4.4.264.R01
Summary: ACLMAN:+++ memPartAlloc: block too big - 67108864 in partition 0x4f3454.

PR **156572** Build: 6.4.4.352.R01
Summary: Too many port based ISF command will remove dhcp snooping trust port command
Explanation: Code changes to handle MIP overflow in UDP Relay

---

PR **156602** Build: 6.4.4.350.R01
Summary: Unit 2 in a stack of 6 crash with dump file.
Explanation: Code changes done to display the assembly instructions in pmd around both PC and Link Register

---

PR **157245** Build: 6.4.4.361.R01
Summary: OSPF neighbor goes down after changing system clock back by one hour or more
Explanation: OSPF MD5 Sequence Number is modified to a static counter initialized to system time during ospf restart

---

PR **157619** Build: 6.4.4.332.R01
Summary: 6850 crashed with STP data access exception

PR **158241** Build: 6.4.4.540.R01

Summary:	"show qos queue" showing wrong values		
Explanation:	Design change for resetting the qos hardware counters, No clear on read. show qos queue command showing wrong values corrected.		

PR	**158769**	Build:	6.4.4.377.R01
Summary:	Crash in Vstk after issuing few show commands		
Explanation:	Added defense check to prevent Crash in VSTK show commands		

PR	**160600**	Build:	6.4.4.375.R01
Summary:	DHCP_client not changing to discovery after link down/up.		
Explanation:	Discover process to be started, if any port of the dhcp-client interface vlan comes up		

PR	**161350**	Build:	6.4.4.422.R01
Summary:	OS6850E: Packet drops noticed when using 10 GIG modules instead of Stacking module.		
Explanation:	Keep Alive message not send on user ports on OS6850 6850E		

PR	**159655**	Build:	6.4.4.403.R01
Summary:	OS880 crashed after write memory command issued --Nxt2Clr = 2f, Nxt2wrt = 0, NxtNxt2wrt = 1		
Explanation:	Added validation check before processing invalid buffers in ZcBufDelete().		

PR	**166151**	Build:	6.4.4.496.R01
Summary:	When VRRP is enabled for NLB server vlan, client loses connectivity to VIP for NLB.		
Explanation:	Care taken to retain the Static Arp entries in both H/W and S/W when VRRP is enabled/disabled.		

PR	**180500**	Build:	6.4.4.614.R01
Summary:	Corrupted UDP frame! bplen:318 efp->length:68 port:15/2 smac:00:00:00:00:fe:01		
Explanation:	Corrupted UDP frame logs will be printed only once in swlog if multiple packets comes from the same source.		

PR	**183020**	Build:	6.4.4.658.R01
Summary:	OS 6850 uplink towards core switches going down frequently.		
Explanation:	In case of SVLAN flooding, the Qdriver Buffer was not released properly. We now keep track of all NULL entries for all SVLAN port bitmaps and release the buffers.		

PR	**158399**	Build:	6.4.4.503.R01
Summary:	OS6850 crashed:tUfiClnt (edd2560) @ 5 PEND lckd=0 ME DS stk edd2560-edcd740		
Explanation:	Debug added in PMD to dump Swlog and Console FD details		

PR	**171587**	Build:	6.4.4.585.R01
Summary:	Issue with bpdu shutdown on mobile ports.		
Explanation:	BPDU Link-Shutdown on 802.1x/mobile ports		

PR	**171983**	Build:	6.4.4.557.R01

Summary: QoS Policy PIM neighbor prevention problem
Explanation: Allow user policy precedence over system rules when "debug qos internal "slice 0/0 copytocpuflag 1"" is used

---

PR **174613** Build: 6.4.4.571.R01
Summary: Incorrect Mac addresses and vlans learnt through non tagged port
Explanation: Mac-address learnt on linkagg is displayed in proper vlans.

PR **172537** Build: 6.4.4.555.R01
Summary: Multicast forwarding entry missing due to RPF check failure - next hop router none
Explanation: Corrected the Multicast forwarding entry miss after reboot

---

PR **191587** Build: 6.4.4.717.R01
Summary: IGMP traffic not received, when port security is disabled.
Explanation: Receiving IGMP traffic with port-security disabled.

PR **194646** Build: 6.4.4.694.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 **184682** Build: 6.4.4.651.R01
Summary: Linkagg issue in a Vlan stacking configuration
Explanation: Packets with Double tags egressing out of uni port across Ni will not be losing inner tag.

PR **183594** Build: 6.4.4.642.R01
Summary: OoS display issue with Omni switch.
Explanation: Ensured the configurations applied for one category should not reflect in other.

PR **188774** Build: 6.4.4.682.R01
Summary: DHCP Discover and Offer are not forwarded between trusted ports
Explanation: When SRC mac and client mac of discover packet is different, update the client mac in the cmm context even though mac- verification disable command is configured.

PR **154067** Build: 6.4.4.361.R01
Summary: Power supply error coming for power supply which is not present
Explanation: Check for the presence bit whenever the operational bit of the power supply is changed.

PR **156356** Build: 6.4.4.356.R01
Summary: OS6850 gives internal error when trying to add same ip for snmp station as the loopback0
Explanation: SNMP Station address configuration restricted only to Pure Loopback0 address (not same as physical ip interface address)

PR	**156720**	Build:	6.4.4.379.R01
Summary:	qos policy condition is not displayed properly in config		
Explanation:	Display the default ether type in qos policy		

PR	**158169**	Build:	6.4.4.386.R01
Summary:	Port stuck in mirroring configuration. Unable to change the port configuration.		
Explanation:	Added check to throw error when remote port mirroring vlan enabled on default mirroring session		

PR	**157953**	Build:	6.4.4.379.R01
Summary:	Need to redefine the MAC range in alaPhones mac group		
Explanation:	Addition of mac range to the existing alaPhones mac group		

PR	**157990**	Build:	6.4.4.350.R01
Summary:	LPS configuration is removed when upgrading from 6.4.3 to 6.4.4.		
Explanation:	boot.cfg is taken care so that no boot up errors occur during upgradation from 643R01 to 644 R01 related to Port-security.		

PR	**159302**	Build:	6.4.4.383.R01
Summary:	OS6400 crash when creating banner from CLI		
Explanation:	Memory allocated for the SLOP value (which is used for indentation purpose) needs to be memset with NUL.		

PR	**160528**	Build:	6.4.4.508.R01
Summary:	OS6850 is duplicating 802.1x commands line under show configuration snapshot output.		
Explanation:	Handle MIP overflow errors in aaa snapshot		

PR	**161054**	Build:	6.4.4.392.R01
Summary:	Axis camera is not put in the correct vlan based on ip rule configured.		
Explanation:	Ignore IPv4 based rules for IPv6 packets on mobile ports		

PR	**162676**	Build:	6.4.4.512.R01
Summary:	Interface speed display errors. In ifHighSpeed on AOS 6.4.3.R01 we reply always 0 instead of 1000		
Explanation:	Code changes done to display correct interface speed		

PR	**163003**	Build:	6.4.4.511.R01
Summary:	Radius cli task suspended on OS9800 running 6.4.3.717.R01		
Explanation:	Radius cli task suspension issue is fixed		

PR	**167944**	Build:	6.4.4.538.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	**170018**	Build:	6.4.4.531.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 **179308** Build: 6.4.4.613.R01
Summary: High CPU due to task bcmLink.0
Ref PR#176562
Explanation: Number of interrupts exceeds the threshold of ~150(?) interrupts per second, disable the interrupts to the system, which would prevent interrupt based link scanning to be done. System perform Polling based link scanning and send a traps to SNMP

PR **178087** Build: 6.4.4.611.R01
Summary: OS6450 tftp incorrect behavior
Explanation: Clearing the buffer to prevent taking previous file name from the buffer

---

PR **182219** Build: 6.4.4.638.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 **180342** Build: 6.4.4.612.R01
Summary: Bootp request packet dropped while snooping is activated.
Explanation: BOOTP packets are not dropped even when DHCP snooping is enabled by enabling the variable udpFloodDirBcat to 1.

PR **180835** Build: 6.4.4.617.R01
Summary: SSL related Vulnerabilities in OS6850E Switches.
Explanation: For web view Authentication ssl certificate is integrated in code under path /sw/management/switch_management/emweb/html/avlan/custom. These certificates were incorporated in secu.img and get extracted to the switch

---

PR **181842** Build: 6.4.4.625.R01
Summary: PIM boot up delay issue.
Explanation: PIM Interfaces will not be enabled till PIM

PR **182910** Build: 6.4.4.642.R01
Summary: Switch reboots when IP phone is connected.
Explanation: Array is handled properly to prevent memory corruption.

PR **170828** Build: 6.4.4.530.R01
Summary: Incorrect PIM DR
Explanation: Fix done to shows correct DR values in "show ip pim interface" command.

PR **173598** Build: 6.4.4.570.R01
Summary: Issue with a special character and ssh session
Explanation: While parse the tty modes to the terminal fd, set all of the option bits and disable the special ROM monitor trap character CTRL+X and CTRL+C

PR	**174567**	Build:	6.4.4.594.R01
Summary:	VU-091113-1: Vulnerability in the SSL/TLS protocol.		
Explanation:	Disabling Renegotiation in open SSL		

PR	**174370**	Build:	6.4.4.594.R01
Summary:	VU-110617-3: Vulnerability in OpenSSL		
Explanation:	Add protection against ECDSA timing attacks		

PR	**194561**	Build:	6.4.4.737.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	**200710**	Build:	6.4.4.733.R01
Summary:	OS6850 stack Low Flash issue		
Explanation:	Value of minFlashRequired debug variable set in AlcatelDebug.cfg is updated to all units of stack.		

PR	**201216**	Build:	6.4.4.738.R01
Summary:	802.1x having issues with Random clients		
Explanation:	Fix done to avoid the onex and SL table mismatch in case of client is getting moved from supplicant to non-supplicant and vice versa with the same vlan.		

PR	**154465**	Build:	6.4.4.198.R01
Summary:	wrong message display when you use "port-security X/Y enable/disable" in 6850 with 6.4.4.141 build		

PR	**158983**	Build:	6.4.4.361.R01
Summary:	EntConfigChange trap does not seem to get generated.		
Explanation:	EntConfigChange trap is implemented properly in OV and Web view.		

PR	**159223**	Build:	6.4.4.377.R01
Summary:	"ALL NIs (License expired, CMM Config OUT-OF-SYNC)" Seen in "show running directory output.		
Explanation:	Don't check for MPLS license while executing 'show running-directory'		

PR	**159585**	Build:	6.4.4.407.R01
Summary:	"Show power supply" show type AC instead of DC.		
Explanation:	PoE register values has updated based on the type of board		

PR	**160578**	Build:	6.4.4.477.R01
Summary:	OS6855-14 - LANPOWER error 181 Invalid Slot		
Explanation:	The severity level of error messages when validating a lan-power slot which is not present is reduced to Debug1		

PR	**161130**	Build:	6.4.4.393.R01
Summary:	Adding OAM configuration to a 6850E seemed to cause a crash.		

Explanation: Avoid double free of qDriver packet buffer originating from ethoamNi

---

PR **163046** Build: 6.4.4.420.R01
Summary: Error Message on OS6850. svlan 0 message
Explanation: Deleting a ethernet service with wrong svlan id should not impact any show commands.

PR **175910** Build: 6.4.4.578.R01
Summary: Show spantree command doesn’t show PVST+ enable.
Explanation: By default PVST + will be disable. Whenever pcst+ mode is enable it will be get displayed in the following command show spantree" and " show spantree < num>"

PR **178945** Build: 6.4.4.609.R01
Summary: 6450/6250 standalone switches always not shown as mono switch while doing a mib walk
Explanation: Check has been added to set the synchronization status as CS_SYNCHROSTATUS_MONOCMM if it is a standalone unit

---

PR **177150** Build: 6.4.4.589.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 **181090** Build: 6.4.4.621.R01
Summary: L2-VPLS - frames not forwarded properly
Explanation: Number of VPLS (DSP) Services that could be handled has been increased to 2K

PR **171702** Build: 6.4.4.538.R01
Summary: ERP Connectivity issue - We noticed that a linkagg port was incorrectly programmed as STP status bl
Explanation: Change STP state to forwarding as soon as lag join is received by directly verifying if link state is up instead of checking local variable

---

PR **166634** Build: 6.4.4.501.R01
Summary: OS6850E: Issue with bandwidth rate-limiting
Explanation: Code changes done to configure default depth to 4M

PR **172190** Build: 6.4.4.557.R01
Summary: Blocking Multicast traffic on interface connecting to third party router.
Explanation: Mroute-Boundary check condition is modified to accommodate all the multicast data ranges

---

PR **173651** Build: 6.4.4.577.R01
Summary: SAA statistics are not consistent
Explanation: Corrected the SAA Statistics with Proper timestamp in Packets

---

PR **193612** Build: 6.4.4.688.R01

Summary: Write memory flash synchronization and show configuraiton snapshot command output issue with OS9700
Explanation: Sflow Display Commands will not increase memory utilization

---

PR **193617** Build: 6.4.4.718.R01
Summary: OSPF routes are installed with delay into the routing table
Explanation: first packet LSA handling and OSPF LSA length overflow handling

---

PR **197425** Build: 6.4.4.720.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 **184085** Build: 6.4.4.648.R01
Summary: OS6580 at Alcova ES crashed.
Explanation: defense fix to avoid invalid memory access

PR **198917** Build: 6.4.4.716.R01
Summary: high cpu noticed when we poll the device from OV
Explanation: Introduction of debug variable to control the healthMonDeviceTrap generated from switch when CPU crosses threshold limits.

PR **156360** Build: 6.4.4.356.R01
Summary: OS6400 doesn t forward option-82 information to another switch (Telco) when DHCP snooping is enabled
Explanation: The DHCP packet will be forwarded without stripping opt82 format from the packet if POLICY_KEEP is enabled.

PR **156204** Build: 6.4.4.287.R01
Summary: OS6850 - 802.1x EAP Failure after switch reboot
Explanation: Fix done to handle supplicant authentication on boot up

---

PR **157326** Build: 6.4.4.459.R01
Summary: show temperature , Upper threshold and Temperature status
Explanation: Temperature status will update based on threshold change.

PR **159704** Build: 6.4.4.466.R01
Summary: OS6850: nisup_sounderHealthMonitor +1cc: nisup_sounderSendTaskSuspendedTrouble()
Explanation: Code changes done for preventing memory leak in wrong LDAP configuration in switch.

PR **159978** Build: 6.4.4.368.R01
Summary: With aaa hic enabled, the IGMP member report/join from first client is also seen by second client.
Explanation: IGMP Behavior will not be affected when HIC is Enabled

---

PR **161255** Build: 6.4.4.429.R01
Summary: OS6400-24 Reboot Suddenly

Explanation: Added Validation checks in LinkAgg task

PR **161099** Build: 6.4.4.391.R01
Summary: On web gui view the system uptime is showing 000 after 365 days.
Explanation: Display year field in system up time for web view display

PR **163332** Build: 6.4.4.458.R01
Summary: If 802.1x and LPS are enabled then a MAC address of a supplicant is not learned
Explanation: Search and delete LPS table as per vlan specified

PR **163735** Build: 6.4.4.418.R01
Summary: crash caused by "sflow receiver 0" command
Explanation: Null pointer check handled for SFLOW Receiver command

PR **163784** Build: 6.4.4.432.R01
Summary: DHCP offer forwarded back to WAN link from 6850E if a route entry to local subnet in routing table
Explanation: Sending DHCP offer based on client information. Kindly set relayUcastReply as 1 in AlcatelDebug.cfg to enable the fix.

PR **167885** Build: 6.4.4.588.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 **167128** Build: 6.4.4.493.R01
Summary: Radius authentication failure with OS6850 and third party ACS.
Explanation: Have corrected defense check to check whether v_len value is less than 6 of overall length and added correct authentication debug in systrace logs.

PR **168357** Build: 6.4.4.495.R01
Summary: Running the "aaa test-radius-server ..." command is crashing the switch.
Explanation: Fixed the crash issue on running "aaa test-radius-server ..." command.

PR **177570** Build: 6.4.4.593.R01
Summary: Buffer issue in OS6850.
Explanation: Buffer is properly released, in case the software generated packets is tried to be flooded over SVLAN on a dual omni products

PR **181549** Build: 6.4.4.648.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 **182292** Build: 6.4.4.636.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	**179716**	Build:	6.4.4.661.R01
Summary:	Third party GBPT Control 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 treatment 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 CDPVTP DTP PVST VLAN UPLINK		

PR	**182646**	Build:	6.4.4.639.R01
Summary:	PIM task got stuck in a wrong state		
Explanation:	Send Join (non-periodic) only if the upstream state is not in joined state		

PR	**181175**	Build:	6.4.4.617.R01
Summary:	Gratuitous ARP is sometimes send with the physical MAC		
Explanation:	During refreshing of ARP timers, make sure to send VRRP MAC for VRRP IP always		

PR	**174571**	Build:	6.4.4.590.R01
Summary:	VU-080718-1: Vulnerability in various IPv6 protocol implementations.		
Explanation:	Vulnerability Fix based on the open bsd patch		

PR	**172495**	Build:	6.4.4.557.R01
Summary:	AOS 6850 is dropping PIM DM State Refresh Message when running with 2000 S,G routes and 4 PIM DM Nei		
Explanation:	Flush old proxy arp for SLB cluster ip after takeover		

PR	**195257**	Build:	6.4.4.697.R01
Summary:	DHCP offer packet is not forwarded by OS6450 udp relay		
Explanation:	Per vlan rtr mac destined changes		

PR	**185527**	Build:	6.4.4.654.R01
Summary:	IGMP general query packet creating loop.		
Explanation:	Fixed the issue with IGMP query getting loop backed when hash-control non-unicast is enabled.		

PR	**189124**	Build:	6.4.4.666.R01
Summary:	Permanent MAC cannot be changed from one vlan to another VLAN in the LPS port		
Explanation:	Fix done to allow changing permanent MAC address from one vlan to another VLAN on the LPS port. And do not change tagged vlan of the LPS port during boot up.		

PR	**149980**	Build:	6.4.4.361.R01
Summary:	OS 9800E linkagg port join leave message on swlog.		
Explanation:	Added a LACP Debug code changes for the various reasons of linkagg port leave		

	failure		
PR	**153855**	Build:	6.4.4.488.R01
Summary:	OS9702E crashed: P1:Startup default Secondary value: 0x100		
Explanation:	Removing invalid "sflow receiver” command which causes a crash.		
PR	**156618**	Build:	6.4.4.359.R01
Summary:	"ethernet-service uni-profile l2-protocol stp peer" is not applied on UNI port		
Explanation:	Added a check not to allow peer option support in ethernet-services l2-protocol		
PR	**159035**	Build:	6.4.4.344.R01
Summary:	OS6850 switch crashes continuously after a code upgrade to 644 GA.		
Explanation:	Correcting the length of the PCI address in the sysMem table to prevent invalid data access during boot up		
PR	**159459**	Build:	6.4.4.401.R01
Summary:	Wrong Length calculation of tagged Rapid PVST+ frame with extra byte "00" padded at the end		
Explanation:	Ethernet Frame Length calculation has been corrected for pvst+tagged case and total frame length corrected to remove extra padding byte.		
PR	**160786**	Build:	6.4.4.388.R01
Summary:	taIPni and bcmRx high on OS6850 running 6.4.3.779.R01		
Explanation:	Inform SFLOW NI when SFLOW receiver is removed, hence respective hardware entries will be removed.		
PR	**161041**	Build:	6.4.4.411.R01
Summary:	Slow RSTP Convergence time in OS6850E-24X		
Explanation:	Link Interrupt enabled for 10G SFP+ ports		
PR	**162121**	Build:	6.4.4.544.R01
Summary:	100% CPU hike in 6400 unit 1 due to taIpni		
Explanation:	Semaphore lock in 802.1x to prevent task lockup		
PR	**163005**	Build:	6.4.4.462.R01
Summary:	MAC address is learned but no connectivity		
Explanation:	Correcting dot1x message and callback handling		
PR	**166827**	Build:	6.4.4.474.R01
Summary:	Wrong value in the length field of AMAP packets		
Explanation:	Corrected length field value in amap frame		
PR	**167344**	Build:	6.4.4.478.R01
Summary:	DHLAA forwarding loop when the primary unit reloaded and came back as idle or secondary unit		
Explanation:	Fix provided to avoid simultaneous connection between DHLAA across NIs by checking if socket connection already exists before retrying.		

PR	**168834**	Build:	6.4.4.538.R01
Summary:	OS 9700 BGP configured with AS-prepend issues.		
Explanation:	Update the queued attribute structure to 0 if an attribute already exists and peer's send policy is sent for re-evaluation		

PR	**176730**	Build:	6.4.4.589.R01
Summary:	tCS_PRB (d780fe8) & WebView (81bdb88) suspended on OS6850 Stack.		
Explanation:	Check has made to verify username and password for captive portal login page		

PR	**177517**	Build:	6.4.4.604.R01
Summary:	NI2 on nw-dsb-fwo crashed with PMD		
Explanation:	With this fix the reported crash won't occur.		

PR	**183170**	Build:	6.4.4.638.R01
Summary:	Password command on secondary management module should not be allowed		
Explanation:	Password command is not allowed in secondary CMM		

PR	**155200**	Build:	6.4.4.540.R01
Summary:	need to preserve TCAM space by using software rules (no-cache option)		
Explanation:	Display issue with "show qos statistics" for no-cache option has been fixed		

PR	**171349**	Build:	6.4.4.562.R01
Summary:	OS6250M - Need explanation for ETHOAM log "error 2018:handle_dmr_info:Timer expired at CMM."		
Explanation:	Changed severity of the ethoam log message "handle_dmr_info:Timer expired at CMM"		

PR	**192200**	Build:	6.4.4.712.R01
Summary:	When we do flash synchro we notice error message in swlog "CCM_CSM_FLASH_SYNCHRO_RS-appError 24"		
Explanation:	Fix to avoid internal ftp hung issue during flash-synchro causing CVM timeout		

PR	**193117**	Build:	6.4.4.681.R01
Summary:	768 VPA limit is not enforced in CLI		
Explanation:	Code changes done to log message while creating more than 768 VPA.		

PR	**190788**	Build:	6.4.4.728.R01
Summary:	Particular port of OS9-XNI-U12E module on OS9702E down		
Explanation:	Code changes done to allow UDLD in static linkagg ports.		

PR	**189848**	Build:	6.4.4.670.R01
Summary:	SFP showing incorrect DDM value.		
Explanation:	Fix done to show proper DDM value		

PR	**201948**	Build:	6.4.4.737.R01
Summary:	MAC address learnt through 802.1x state is Captive-portal CP In-Progress.		
Explanation:	Fix the mac-address table inconsistency after continuous mac move		

PR **204971** Build: 6.4.4.741.R01
Summary: 6850 - I2c Bus Locked + LACP flapping
Explanation: Reduces i2c read attempts (in case of failure to a maximum of 2) and allows more time (15 ticks) between the attempts.

PR **152163** Build: 6.4.4.407.R01
Summary: Issue in accessing switch using SSH client running OpenSSH 3.9p1
Explanation: Changed the socket Level MTU in SSH to reflect the Client MTU configuration
The Fix is controlled using an Global Variable tcpMSSLimit .
We need to set this value with the same as specified in the Interface MTU for the SSH client. The Same MTU will remain valid for any other SSH session established on the DUT.

PR **156049** Build: 6.4.4.378.R01
Summary: OS9 - Subnet broadcast in Bootp Packets are not relayed to the relay address configured.
Explanation: Bootp buffer handling size increased from 1024 to 1400 to handle pxe discover packets NOTE: BOOTP Packets of Max Size 1400 Bytes only will be handled by AOS 64x Devices

---

PR **156609** Build: 6.4.4.361.R01
Summary: info === HSM === Power Supply 1 has been REMOVED message coming frequently on os6855
Explanation: Changes to hold the power supply down message on 6855 C14

PR **157697** Build: 6.4.4.423.R01
Summary: OS6850 Sensitive delay in TV zapping
Explanation: Code changes to handle when static querier ports enabled in multicasting

---

PR **157541** Build: 6.4.4.392.R01
Summary: inserted new CMM B and switch crashed on CMM A
Explanation: Handle the improper insertion of CMM-B into the chassis graciously.

PR **158692** Build: 6.4.4.391.R01
Summary: OS 6850 stack crash with error "== CSM == Excep in task: LnkAgg PC : 0x19a78b4
Explanation: Added defense fix as port index pointer validation check

---

PR **160586** Build: 6.4.4.503.R01
Summary: Jumbo MTU size setting loss on 10MB port setting when port bounces
Explanation: Code fix done to retain the max frame size configured when port bounces

---

PR **160807** Build: 6.4.4.503.R01
Summary: topology view issue between in OV for fiber links between 9800 switches
Explanation: Added needed validation to the PortID ifIndex of LLDP

PR **161689** Build: 6.4.4.408.R01
Summary: Lost management access to OS6400 - qdriver buffer depletion.
Explanation: Fixed buffer depletion at qdriver because of ethoam packets

PR	**161186**	Build:	6.4.4.399.R01
Summary:	OS6850 does not pass traffic through ports where transparent-bridging is enabled.		
Explanation:	Sending the Vlan Info before enabling the Trans-Bridging, rather than sending the msg to NI for every Vlan Event.		

PR	**163121**	Build:	6.4.4.441.R01
Summary:	Qos port ingress-bandwidth is not working for TCP		
Explanation:	qosongaruda flag to be enabled on OS6400 to ensure proper setting of configurations		

PR	**165308**	Build:	6.4.4.447.R01
Summary:	Redirection to HIC remediation server sometimes takes more than 30 seconds.		
Explanation:	Destination IP is also checked for caching the Host Information for HIC remediation Server		

PR	**167955**	Build:	6.4.4.545.R01
Summary:	6850E: PoE: i2cReadOnBoardTemp, PD640xx and pd69_lp write error at boot up		
Explanation:	CPLD changes for proper detection of OS6850E PoE units		

PR	**167745**	Build:	6.4.4.488.R01
Summary:	Show system does not display the model name for some OS6850.		
Explanation:	Corrected the buffer to include product name.		

PR	**175734**	Build:	6.4.4.577.R01
Summary:	OS6850E set DEI bit for qos rule hit packets over 10/s when log is enable on the rule		
Explanation:	Don t set CFI bit for packets that are switched/routed when qos-logging is enabled		

PR	**178660**	Build:	6.4.4.602.R01
Summary:	HIC https redirection fix for PER# 177375 does not work when Switch is not configured with IP Interface.		
Explanation:	Fix provided to allow HTTP packets to be processed by IPNI even if it is not destined to our switch. When the port is .1x and hic is configured.		

PR	**182718**	Build:	6.4.4.637.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	**170503**	Build:	6.4.4.659.R01
Summary:	dshell is currently in use, try again later; CHASSIS warning unable to post semaphore, 6250 over memo		
Explanation:	Recover dshell for debug purpose		

PR	**172644**	Build:	6.4.4.558.R01
Summary:	taIPMS stucked at 100% due to hardware write failure		
Explanation:	Fix done for CPU 100% when hardware write failed in bcm_freeze function.		

Known Issues:

PR	**164017**
Summary:	[DHL] Convergence is relay slow when losing the unit supporting the active link in a stack

PR	**156045**
Summary:	Mac not displayed in mac-address table if set as permanent on another port

PR	**160107**
Summary:	NTP updates time but not date
Explanation:	NTP date does not get updated if the discrepancy is high.

PR	**160684**
Summary:	having the Copper SFP in hybrid port disable the copper port link in 6850-U24x
Explanation:	"SFP-GIG-T is not support on combo ports". On a hybrid port at any time there is only one physical medium active copper or fiber. If we insert copper sfp in fiber port we are changing physical medium from fiber to copper and the actual copper link is brought down as copper as a medium cannot be active on fiber and copper both at same time. There is no reason behind having copper sfp readily inserted on fiber port and on failure physically move the copper onto hybrid fiber.

PR	**156967**
Summary:	VRF specific IP address information, not displayed in AOS
Workaround:	This can be done using an SNMPv3 user in the following manner: Read the contents of alaVirtualRouterNameTable. The value in each row for alaVirtualRouterNameIndex specifies the VRFId and corresponding alaVirtualRouterName provides you the SNMPv3ContextName for the VRF. If SNMPv3 requests are made for each contextId in this table then you will get all entries for the table across all VRF Id's.

PR	**145589**
Summary:	Auto-neg configuration needs to be replicated in both fiber and copper mediums for combo ports.
Explanation:	On an OS6850 auto-negotiation configuration needs to be replicated on both fiber and copper mediums for combo ports.
Workaround:	Use the following commands to duplicate the auto-negotiation configuration: -> interfaces <slot/port> hybrid fiber autoneg {enable | disable} -> interfaces <slot/port> hybrid copper autoneg {enable | disable}

PR	**159999**
Summary:	after a arp probe: gratuitous arp are not used to move vlan in 802.1x port mobility.
Explanation:	onex configuration, first packet will not process if it is non ip packet or source ip is 0.0.0.0.
Workaround:	Use MAC rule rather than IP rule

PR	**170822**
Summary:	Vendor specific dhcp option#43 is not passed correctly.

New Software Features:

1. Loopback Detection

Introduction:
LBD can detect and prevent L2 forwarding loops on port either in the absence of other loop-detection mechanisms like STP/RSTP/MSTP or when the mechanism can't detected it. Sometimes the STP/RSTP/MSTP based loop detection can't be used due to the following Facts

- There is a client's equipment that drops or cuts the BPDUs.
- The STP protocol is restricted on edge Network

The LBD feature detects that a port has been looped back or looped. If a loop-back/loop is detected, the port is disabled (forced down) and the appropriate Error Log is issued.

Ethernet switch periodically sends out L2 Ethernet frame (LBD frame) from all loop-back detection enabled ports. The LBD frame is not a BPDU frame. In normal state of the access line this frame is removed from the network segment by the subscriber equipment. In case of failure (cable fault, NIC incorrect work, etc) switch receives back the control frame on the port. After receiving the frame switch should force the access port down and issues a SNMP trap. In addition the port also can be re-enabled by user by cli commands.

Platforms Supported:
6400, 6850, 6850E, 6855, 6855-U24X, 9000E

CLI Commands:
New Cli command has been introduced for this feature

1.Loopback detection is Enabled/Disabled Globally using the below Command

loopback-detection [DISABLE ENABLE]

2. Loopback detection is enabled/disabled for the Port level using the below command

loopback-detection port [<num/num>] [DISABLE ENABLE]

3. To Change the auto-recovery timer for Loopback detection the below command is used

interfaces <num/num-num> violation-recovery-time [30 sec to 600sec]

This is the existing command which will work along with Loopback detection by default 300 sec is the violation recovery timer.

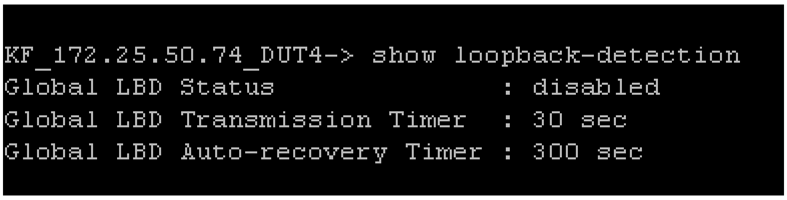
4.To Change the transmission timer for Loopback detection the below command is used

loopback-detection transmission-timer <range> [5 sec to 600sec]

By default 5 sec is the transmission timer for Loopback detection

5. To Verify the Loopback detection globally the below command is used

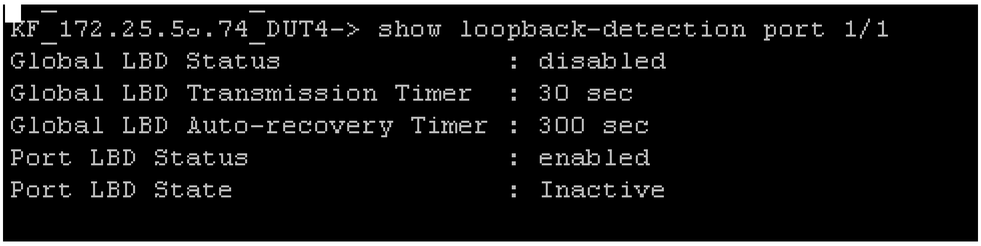
show loopback-detection



```
KF_172.25.50.74_DUT4-> show loopback-detection
Global LBD Status                : disabled
Global LBD Transmission Timer    : 30 sec
Global LBD Auto-recovery Timer : 300 sec
```

6. To Verify the Loopback Detection on a Port basis the below command is used .

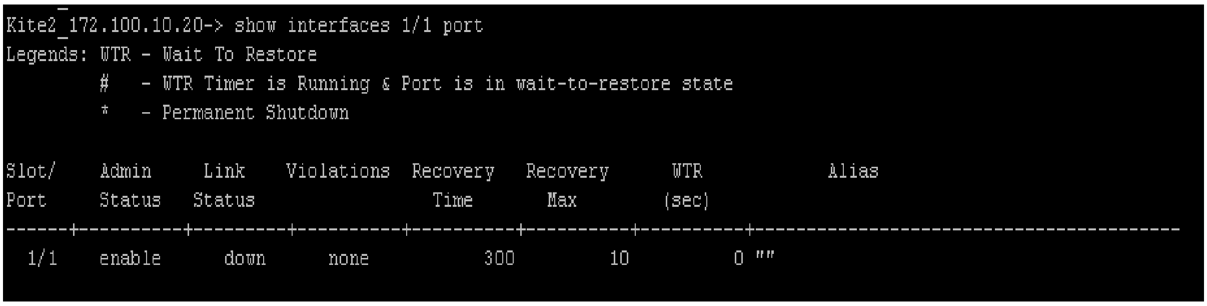
show loopback-detection port <num/num>



```
KF_172.25.50.74_DUT4-> show loopback-detection port 1/1
Global LBD Status                : disabled
Global LBD Transmission Timer    : 30 sec
Global LBD Auto-recovery Timer : 300 sec
Port LBD Status                  : enabled
Port LBD State                   : Inactive
```

7. To Verify the Violation recovery timer for the Port the below command is used along with Loopback detection .

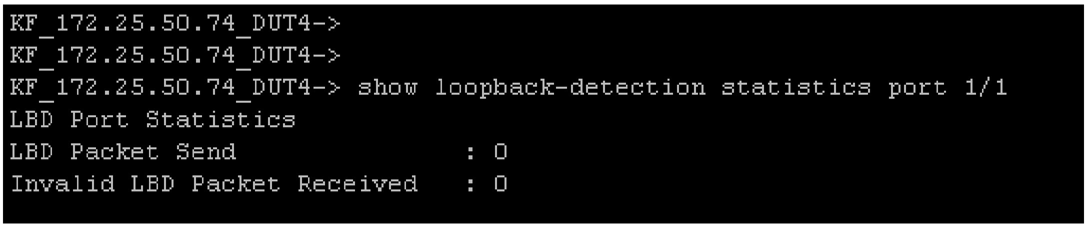
show interfaces <num/num> port



```
Kite2_172.100.10.20-> show interfaces 1/1 port
Legends: WTR - Wait To Restore
        #   - WTR Timer is Running & Port is in wait-to-restore state
        *   - Permanent Shutdown

Slot/    Admin     Link    Violations  Recovery   Recovery      WTR           Alias
Port     Status   Status                 Time       Max        (sec)
------+----------+---------+----------+----------+----------+----------+----------------------------------------
  1/1    enable      down      none           300        10         0 ""
```

8. To Verify the LBD Packets sent out of the Specific ports and LBD Packets Received on the Port the below command is used

show loopback-detection statistics port <num/num>



```
KF_172.25.50.74_DUT4->
KF_172.25.50.74_DUT4->
KF_172.25.50.74_DUT4-> show loopback-detection statistics port 1/1
LBD Port Statistics
LBD Packet Send               : 0
Invalid LBD Packet Received   : 0
```

Software Limitations: None

2. Additional Storm Control Options

Introduction:
This feature enhances the current rate limiting feature to configure actions if broadcast and multicast traffic reaches upper threshold and also provide the ability to recover automatically from the actions if lower threshold is configured and if the traffic level drops from upper threshold to lower threshold.

When traffic (Broadcast or Multicast) flows on a port for 5 seconds at an average speed above the configured upper threshold value, then the port is considered to be in storm state and actions would be taken as any one of the below .

- Default – The traffic gets rate limited to the upper threshold value and user will not get any indication. This is pre-existing behavior
- Trap – The traffic gets rate limited to the upper threshold value and also user will be notified by a trap message.
- Shutdown – The corresponding port will go down and also a trap will be generated to alert the user.

The storm state of the port can be recovered by both manually and automatically. The below procedure is to recover the port manually.

- Interfaces slot/port admin down/up
- Port plug out/ plug in
- Interface clear all violations (Only applicable for Shutdown action)

Also the port can be automatically recovered form storm state if the port is configured with lower threshold value and if the traffic on the port, where storm occurs, reaches below that lower threshold value.

Platforms Supported:

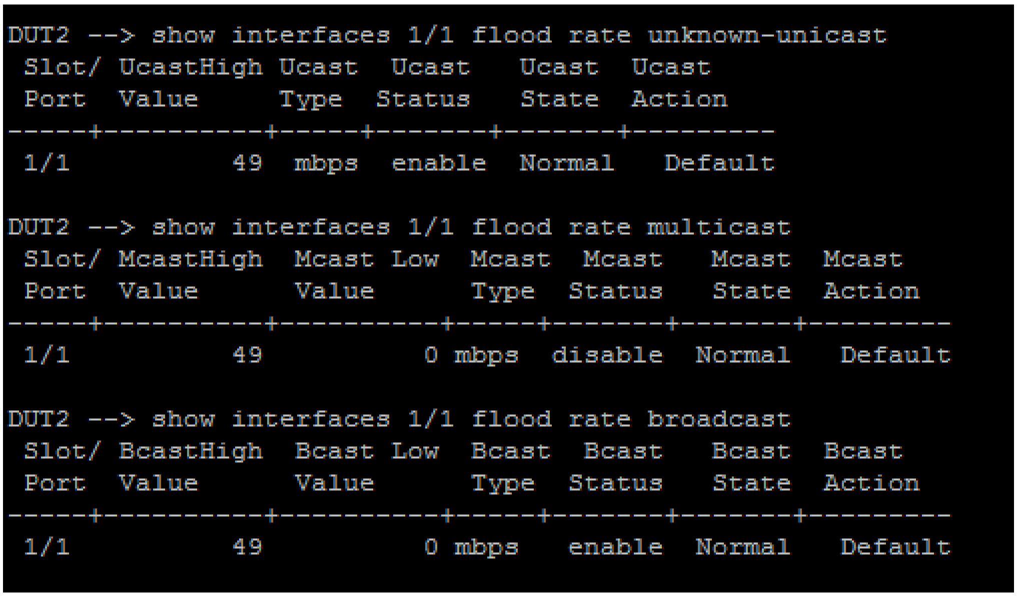
OmniSwitch 6400, 6850, 6850E, 6855, 9000E

Commands:

1. Command to configure upper threshold and lower threshold for multicast and broadcast:
interfaces [*slot/port* | *slot/port1-port2* | *slot*] **flood** [**broadcast** | **multicast** | **all**] **rate** [**mbps** *num* | **pps** *num* | **percentage** *num*] [**low-threshold** *num***]**

2. Command to configure action for storm state:
interfaces [*slot/port* | *slot/port1-port2* | *slot*] **flood [broadcast | multicast] [action [shutdown| trap | default**]]

3. Command to verify the configuration, action and status of the port:
show interfaces [*slot/port* | *slot/port1-port2* | *slot*] **flood rate [unknown-unicast | multicast | broadcast]**



```
DUT2 --> show interfaces 1/1 flood rate unknown-unicast
 Slot/ UcastHigh Ucast  Ucast   Ucast  Ucast
 Port  Value     Type  Status   State  Action
-----+----------+-----+-------+-------+---------
 1/1          49  mbps  enable  Normal   Default

DUT2 --> show interfaces 1/1 flood rate multicast
 Slot/ McastHigh  Mcast Low  Mcast  Mcast   Mcast  Mcast
 Port  Value      Value      Type  Status   State  Action
-----+----------+----------+-----+-------+-------+---------
 1/1          49          0 mbps  disable  Normal   Default

DUT2 --> show interfaces 1/1 flood rate broadcast
 Slot/ BcastHigh  Bcast Low  Bcast  Bcast   Bcast  Bcast
 Port  Value      Value      Type  Status   State  Action
-----+----------+----------+-----+-------+-------+---------
 1/1          49          0 mbps   enable  Normal   Default
```

Limitations:

1. The rate limiting is accurate only for 512 byte packets since the calculation for threshold is based on packet of size 512 bytes.
2. The threshold value at any given point is the average value of the traffic rate for 5 seconds.

3. ASA Re-Authentication/Refresh Authentication per service

Introduction:

This feature Enhancement provides the facility to configure the re-authentication or refresh time for various services offered by Switch like Console, Telnet, FTP, SSH, HTTP and HTTPS when using the authenticating server as LDAP or TACACS or while doing local authentication.

Earlier each user session is refreshed for every 5 minutes. User credentials provided during initial authentication request are forwarded to the server for re-authenticating the user. This refresh time was not configurable and it happens for every 5 minutes. This feature is enhanced to change the refresh timer or disable the refresh process by the user.

Platforms Supported:

OmniSwitch 6400, 6850, 6850E, 6855, 9000E

Commands usage:

1. **session reauth-interval {console |telnet |ssh |ftp |http |https |all} {** *<number>* **|default}**

   Syntax Definitions

number   re-auth timer Value. The Range is 0 – 60 Minutes

Defaults

Parameter	Default
number	5

Usage Guidelines

- The Refresh mechanism can be disabled by configuring the timer as 0.
- The re-authentication timer can be restored to 5 minutes using “default” for timer value

Examples

```
-> session reauth-interval all default
```

2. **Show session config**

Displays information about the sessions configuration

Examples

```
-> show session config
Cli Default Prompt                = 172.25.50.61->,
Cli Banner File Name              = ,
Cli Inactivity Timer in minutes  = 555555,
Ftp Banner File Name              = ,
Ftp Inactivity Timer in minutes  = 4,
Http Inactivity Timer in minutes = 4,
Http Banner File Name             = ,
Login Timer in seconds            = 55,
Maximum number of Login Attempts = 3,
Default Reauth Interval           = 5,
Console Reauth-Interval           = 6,
Telnet Reauth-Interval            = 6,
SSH Reauth-Interval               = 6,
FTP Reauth-Interval               = 6,
HTTP Reauth-Interval              = 6,
HTTPS Reauth-Interval             = 6

-> show session config
Cli Default Prompt                = 172.25.50.61->,
Cli Banner File Name              = ,
Cli Inactivity Timer in minutes  = 555555,
Ftp Banner File Name              = ,
Ftp Inactivity Timer in minutes  = 4,
Http Inactivity Timer in minutes = 4,
Http Banner File Name             = ,
Login Timer in seconds            = 55,
Maximum number of Login Attempts = 3,
Default Reauth Interval           = 5,
Console Reauth-Interval           = Default,
Telnet Reauth-Interval          = Default,
SSH Reauth-Interval             = Default,
FTP Reauth-Interval             = Default,
HTTP Reauth-Interval            = Default,
HTTPS Reauth-Interval           = Default
```

3. show configuration snapshot session

```
-> session reauth-interval telnet 3
-> session reauth-interval http 2
-> show configuration snapshot session
! Session manager :
session timeout cli 555555
session prompt default "172.25.50.11->"
session reauth-interval telnet 3
session reauth-interval HTTP 2
```

Limitations: None

4. TPCE Error Counter correction

Introduction:

This feature avoids incrementing TPCE Errors for Multicast Routing traffic in XNI-U12E Card when it is working fine

Earlier in Multicast Routing Environment TPCE Errors were incremented on egress ports of XNI-U12E card when multicast replication happens for only one vlan on that port. This is now changed to avoid the TPCE error counters getting incremented during successful transmission of multicast packet when ports of XNI-U12E acts as egress port or ports of XNI-U12E replicates the traffic.

Platforms Supported:

OmniSwitch 9000E (XNI-U12E card only)

Commands usage:

No new commands introduced as part of this enhancement

Limitations:

None

5. TACACS Command 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:

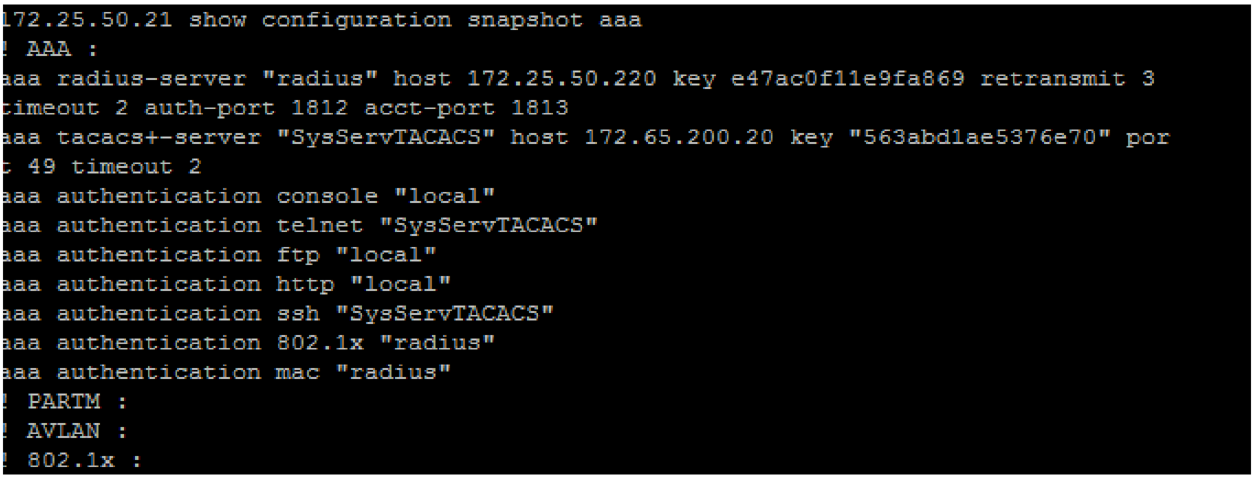
Omni Switch 6400, 6850, 6850E, 6855, 9000E

Commands usage:

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

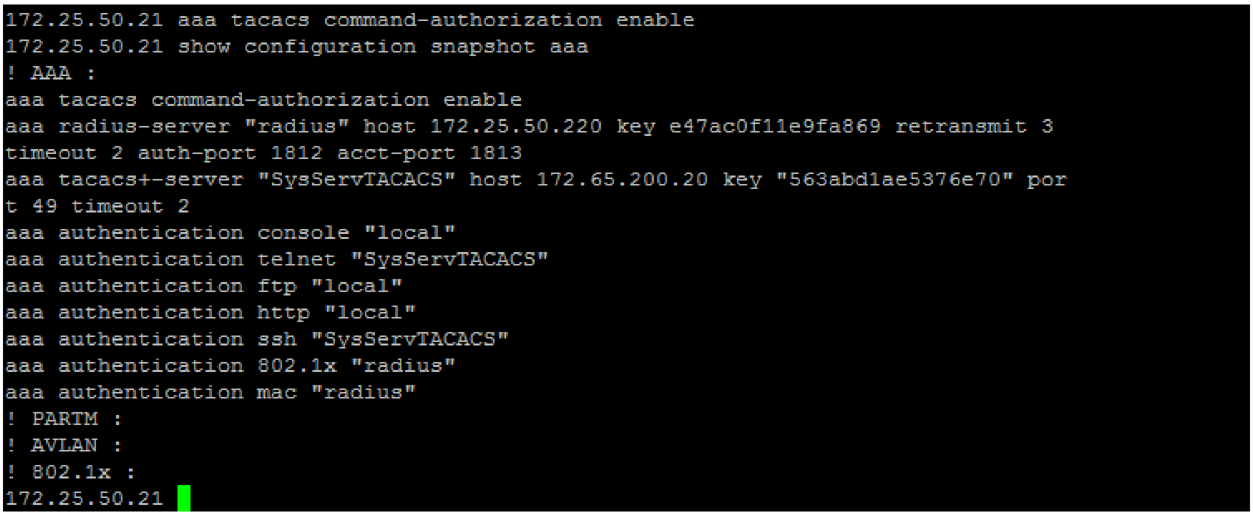
Configuration snapshot:

1. Snapshot of : aaa tacacs command-authorisation 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. Snapshot of : aaa tacacs command-authorisation 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

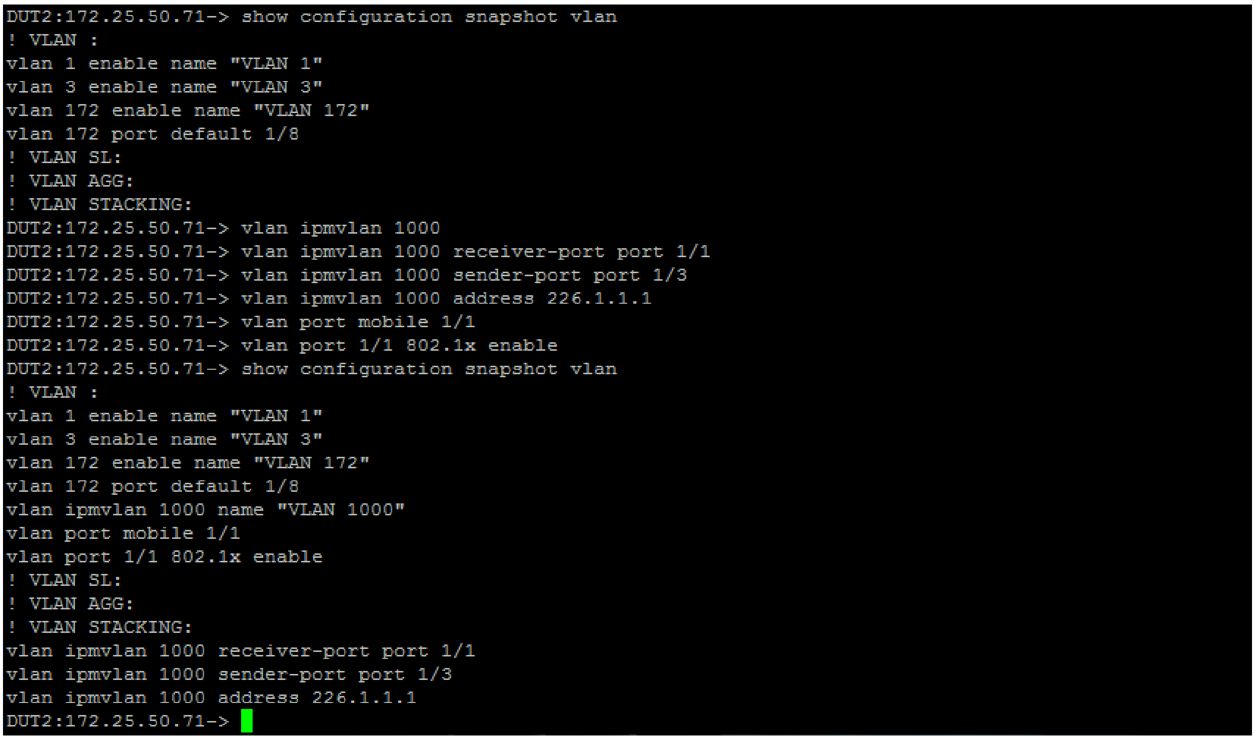
6. 802.1X ON IPMVLAN PORT

Introduction:
IPMVLAN is mainly developed to cater the networks where one end of provider is Ethernet service based (metro edges) and remote end is connected to routers with 802.1Q capability. IPMVLAN will be used to classify the multicast streaming requests into a different VLAN (other than service VLAN). So that Edge devices ‘bridge’ the multicast traffic even though the customers and content providers are in different VLAN/subnet. In this enhancement, 802.1x support is provided on IPMVLAN Receiver port in Enterprise Model.

Platforms Supported:
Omni Switch 6400, 6850, 6850E, 6855, 9000E, 6250, 6250M

Commands usage:
No new commands were introduced.

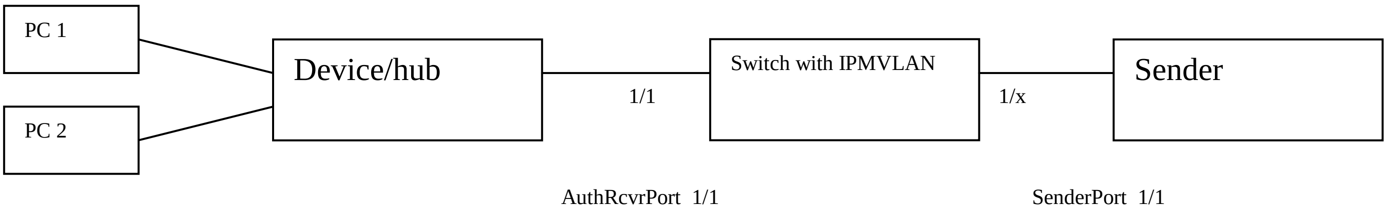
Configuration Snapshot:



```
DUT2:172.25.50.71-> show configuration snapshot vlan
! VLAN :
vlan 1 enable name "VLAN 1"
vlan 3 enable name "VLAN 3"
vlan 172 enable name "VLAN 172"
vlan 172 port default 1/8
! VLAN SL:
! VLAN AGG:
! VLAN STACKING:
DUT2:172.25.50.71-> vlan ipmvlan 1000
DUT2:172.25.50.71-> vlan ipmvlan 1000 receiver-port port 1/1
DUT2:172.25.50.71-> vlan ipmvlan 1000 sender-port port 1/3
DUT2:172.25.50.71-> vlan ipmvlan 1000 address 226.1.1.1
DUT2:172.25.50.71-> vlan port mobile 1/1
DUT2:172.25.50.71-> vlan port 1/1 802.1x enable
DUT2:172.25.50.71-> show configuration snapshot vlan
! VLAN :
vlan 1 enable name "VLAN 1"
vlan 3 enable name "VLAN 3"
vlan 172 enable name "VLAN 172"
vlan 172 port default 1/8
vlan ipmvlan 1000 name "VLAN 1000"
vlan port mobile 1/1
vlan port 1/1 802.1x enable
! VLAN SL:
! VLAN AGG:
! VLAN STACKING:
vlan ipmvlan 1000 receiver-port port 1/1
vlan ipmvlan 1000 sender-port port 1/3
vlan ipmvlan 1000 address 226.1.1.1
DUT2:172.25.50.71->
```

Limitations:
802.1x cannot be enabled on Linkagg receiver ports and ERP receiver ports.
Mobile-tag cannot be enabled on IPMVLAN .

Hypothetical scenarios like the below are not allowed: Reason being if PC 1 is authenticated, 1/1 is open for IPMVLAN traffic. But PC 2 is not authenticated, still it can receive UDP sender traffic as the sender traffic is always a UDP multicast traffic.



Another scenario which is not supported is as follows: Mac/User is authenticated. IPMVLAN group and forward entry is formed. But later if at all the mac/user moves to un-authenticated state and the policy is block, though the ingress IPMS traffic will be blocked, the IPMS group/forward entry will remain until the IPMS entry ages out. The same hold for bypass feature.

7. RADIUS TEST TOOL

Introduction:

The RADIUS test tool provides the administrator with the utility to test the reach ability of RADIUS server from the Network Access Server (AOS Switch) itself. This test tool will be useful in validating the RADIUS server configuration such as server-name, IP address, UDP authentication-port/accounting-port, secret key.

This tool will allow the administrator to validate authentication of the given username and password. Only MD5 and PAP method will be used for sending the password over the network. The CLI session will display the result of the Radius authentication along with the round trip time of sending the request to the RADIUS server and receiving the response from the RADIUS server. The returned RADIUS attributes will be displayed on the CLI of the user session (console/telnet/ssh).

Similarly user can verify the accounting for a particular username

Thus this tool will help in simulating the RADIUS client on the AOS Switch, providing the network administrator with a utility to verify the authentication/accounting of a client with a RADIUS server.

This tool can be used simultaneously from different sessions (console/ssh/telnet) for verifying same or different RADIUS server.

Platforms Supported:

Omni Switch 6250

Commands usage:

aaa test-radius-server *server* type {authentication user *username* password *password* [method {MD5 | PAP}] | accounting user *username*}

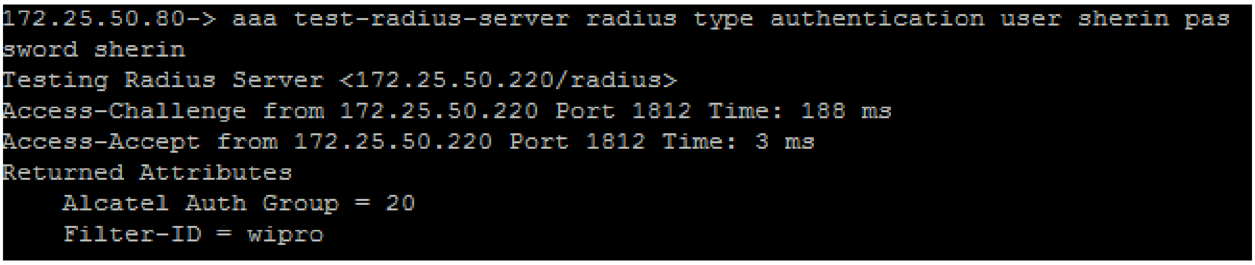
Syntax Definitions

server	Server name for which test has been configured
authentication | accounting	Type of test to be configured.
username	User name for which test has been configured
password	Password for the given user name
MD5 | PAP	Password encryption method for the test

Usage Guidelines

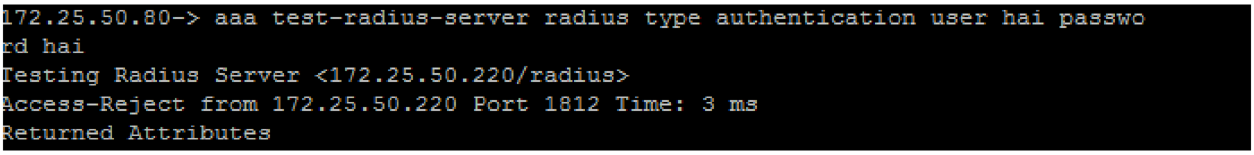
- By default, authentication method is MD5
- RADIUS server configurations like RADIUS server name, acct-port, auth-port, secret key, Retransmit Count, Timeout shall be done on the AOS switch before starting the test tool.
- IP managed interface shall be configured for Radius application or either Loopback0 interface should be configured for Radius Test Tool to work
- Maximum length of the user name shall not exceed 63 characters.
- The length of password should not exceed 128 characters.

Configuration snapshot:
In Case of Success authentication:



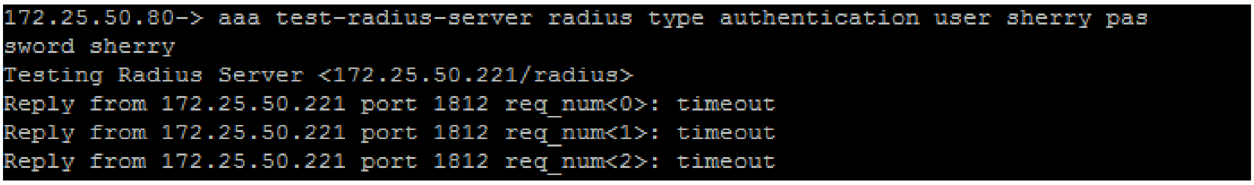
```
172.25.50.80-> aaa test-radius-server radius type authentication user sherin pas
sword sherin
Testing Radius Server <172.25.50.220/radius>
Access-Challenge from 172.25.50.220 Port 1812 Time: 188 ms
Access-Accept from 172.25.50.220 Port 1812 Time: 3 ms
Returned Attributes
    Alcatel Auth Group = 20
    Filter-ID = wipro
```

In case of Failure authentication:



```
172.25.50.80-> aaa test-radius-server radius type authentication user hai passwo
rd hai
Testing Radius Server <172.25.50.220/radius>
Access-Reject from 172.25.50.220 Port 1812 Time: 3 ms
Returned Attributes
```

In case of Server not reachable:



```
172.25.50.80-> aaa test-radius-server radius type authentication user sherry pas
sword sherry
Testing Radius Server <172.25.50.221/radius>
Reply from 172.25.50.221 port 1812 req_num<0>: timeout
Reply from 172.25.50.221 port 1812 req_num<1>: timeout
Reply from 172.25.50.221 port 1812 req_num<2>: timeout
```

Limitations:

When Radius test tool is running, the CLI of that session is blocked until the test gets over or until (ctrl+c) is issued. This test tool is not supported from Webview and SNMP

8. POLICY PORT GROUP ENHANCEMENT

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 6400, 6850, 6850E, 6855, 9000E

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

Syntax Definitions

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

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.

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.

Examples

```
policy port group pg1 mode split 1/3 2/1
policy port group pg1 mode non-split 1/3 2/1
```

show active policy rule r1 extended

```
Policy              Port                Matches
r1                  1/3                 6008280
                          2/1                 6738088
```

show active policy rule r1 meter-statistics extended

```
 Policy:r1,  Port:1/3 Counter Color Mode:RED_YELLOW
 Green    :                     -,      Non-Green:                -,
  Red      :                     0,     Non-Red  :                 -,
 Yellow   :                     0

Policy:r1,  Port:2/1 Counter Color Mode:RED_YELLOW
Green    :                     -,     Non-Green:                  -,
 Red      :                    0,     Non-Red  :                   -,
        Yellow   :                              0
```

show policy port group

```
Group Name            From   Entries         Mode
 Slot01                 blt     1/1-26        non-split

Slot02                  blt      2/1-24        non-split

 Slot03                 blt    3/1-24         non-split

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

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

9. PPPoE Intermediate Agent

Introduction:

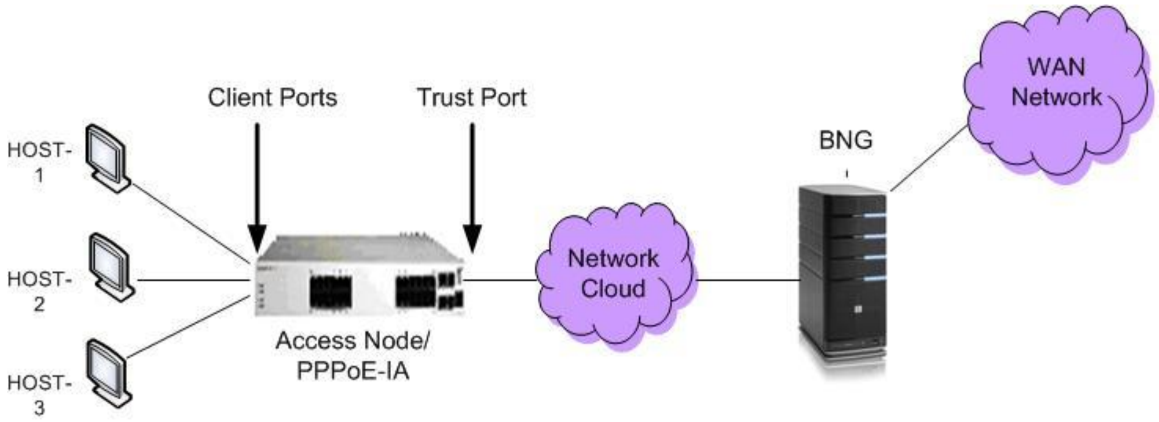
This enhancement provides the ability to connect network of hosts to remote access concentrator (e.g., Broadband network gateway) over a bridging device. In this model, each user host utilizes its own ppp stack and every user is presented with a familiar user interface. Access control billing and type of service can be done per user basis rather than per site basis.
This has been developed as a new feature. To provide a point-to-point connection over Ethernet, each PPP session must learn the Ethernet address of the remote peer, as well as establish a unique session identifier. PPPoE includes a discovery protocol that provides this.
There are four steps in discovery phase to establish session with remote peer and one step in terminating the session.

Discovery phase:

PADI, PADO, PADR, PADS

Termination Phase:

PADT



PPPoE-IA:

PPPoE Intermediate Agent (PPPoE-IA) is placed between a subscriber and Broadband Network Gateway to help the service provider distinguish between end hosts connected over Ethernet to an access switch.

BROADBAND NETWORK GATEWAY:

Broadband Network Gateway is the aggregation point for the user traffic. It provides aggregation capabilities for different kind of traffic (e.g. IP, PPP, and Ethernet) between the access network and the ISP network.

ACCESS NODE:

An access node is a node that provides connectivity between the user and the network cloud. It aggregates the traffic coming from a user and routes it to the network.

ACCESS LOOP:

Access loop signifies the physical connectivity between the Network Interface Device at the customer premises and the Access Node.

Platforms Supported:
Omni Switch 6400, 6850, 6850E, 6855, 9000E.

Commands usage:

1. pppoe-ia {enable | disable}
Globally enables or disables the PPPoE intermediate agent.

Syntax Definitions

enable|*disable*   Enables/disables the PPPoE intermediate agent globally

Usage Guidelines

By default, pppoe intermediate agent is globally disabled.
All PPPoE-IA parameters are configurable irrespective of the global status of PPPoE-IA

Example
pppoe-ia enable
pppoe-ia disable

2. pppoe-ia { port <slot/port [-port2]> | linkagg <num> } {enable | disable}
Enables or disables the PPPoE-IA on port(s) or a linkagg.

Syntax Definitions

slot/port[-port2] The slot number for the module and the physical port number(s) on that module (e.g., 3/1 specifies port 1 on slot 3). Port2 refers to the last port in the range of ports.

enable|disable Enables/ disables the PPPoE-IA on port(s)

num Linkagg Id

Usage Guidelines
By default, PPPoE-IA is disabled on all ports.
All PPPoE-IA parameters are configurable irrespective of the per port status (enable/disable) of PPPoE-IA.
For PPPoE-IA to work, it should be enabled globally as well as on the port.
PPPoE-IA is not supported on port mirroring destination ports, but configuration shall be allowed.
PPPoE-IA is not supported on aggregable ports.

Example
pppoe-ia port 1/1 enable
pppoe-ia port 2/1-12 enable
pppoe-ia port 2/4 disable
pppoe-ia port 2/2-10 disable
pppoe-ia linkagg 1 enable
pppoe-ia linkagg 0 disable

3. pppoe-ia { port <slot/port [-port2]> | linkagg <num>} {trust | client}
Configures a port(s)/linkagg as a trusted or client port(s)/linkagg, for PPPoE intermediate agent. A trust port is a port that is connected to the Broadband Network Gateway whereas a client port is connected to the host.

Syntax Definitions

slot/port[-port2] The slot number for the module and the physical port number(s) on that module (e.g., 3/1 specifies port 1 on slot 3). Port2 refers to the last port in the range of ports.

trust|client Mode of the port as trust or client.

Num Linkagg Id

Usage Guidelines
By default, all ports are client ports.
All PPPoE-IA parameters are configurable irrespective of the per port status of PPPoE-IA.

For PPPoE-IA to work, it should be enabled globally as well as on the particular port.
For PPPoE-IA to work, it should be enabled on a client port as well as a trusted port.
In case of configuration of a client or trust port as a client or trust port respectively again, no action will be taken.
PPPoE-IA is not supported on aggregable ports.

Example

```
pppoe-ia port 1/1 trust
pppoe-ia port 2/3-12 trust
pppoe-ia port 2/3 client
pppoe-ia port 1/2-6 client
pppoe-ia linkagg 7 trust
pppoe-ia linkagg 0 client
```

4. pppoe-ia access-node-id { base-mac | system-name | mgnt-address | user- string   <string> }

Globally configures a format to form an identifier that uniquely identifies an access node.

Syntax Definitions

base-mac	The base mac-address of the switch.
system-name	The configured name of the switch.
mgnt-address	The management IP address of the switch.
user-string	A configurable user string.
<string>	The value of user configured string.

Usage Guidelines

By default, base-mac is used as a format for access-node-identifier.
The access-node-identifier can have a maximum of 32 characters. The access-node-identifier longer than 32 characters will be truncated to 32 characters.
In case of mgnt-address format, the mgnt-address used is Loopback0 address if configured and active or the first active IP interface address otherwise 0.0.0.0 is used.
The access-node-id must not contain spaces.
If any format other than user-string is specified, the setting of string value will not be allowed through SNMP and WEB.
If the format type is user-string, it will be mandatory to provide the string value through SNMP using Multi-varbind.

Example

```
pppoe-ia access-node-id base-mac
pppoe-ia access-node-id system-name
pppoe-ia access-node-id mgnt-address
pppoe-ia access-node-id user-string acessnode1
```

5. pppoe-ia circuit-id { default | ascii [base-mac system-name interface vlan cvlan interface-alias user-string <string> delimiter <char>]}

Globally configures a circuit-id format that forms an identifier which uniquely identifies an access node and access loop on which PADI/PADR/PADT is received.

Syntax Definitions

default The default value of circuit-id is used.

ascii The circuit-id format is an ascii string formed using the following formats fields and a delimiter

base-mac The base mac-address of the switch.

system-name The configured name of the switch.

interface The slot/port on which the PPPoE message is received.

vlan The vlan on which the PPPoE message is received.

cvlan The inner-vlan or customer vlan of the PPPoE message.

Interface-alias The configured alias of the interface on which PPPoE message is received.

user-string A configurable user string.

<string> The value of user configured string

delimiter A user configurable delimiter used to separate the fields of an ascii string forming the circuit-id.

char The value (a character) of user configurable delimiter.

Usage Guidelines

By default, the value of circuit-id is “access-node-id eth slot/port[:vlan-id]”. For e.g. if the value of access-node-id is “vxTarget”, the default value of Circuit ID will be “vxTarget eth 1/1:10” if packet is received on interface 1/1 in vlan 10.

By default, the delimiter used is ‘:’.

The available delimiters are: ‘:’, ‘|’, ‘/’, ‘\’, ‘-‘, ‘_’, ‘ ‘, ‘#’, ‘.’, ‘,’ and ‘;’ and ‘:’

The circuit-id can have a maximum of 63 characters. The circuit-Id longer than 63 characters will be truncated to 63 characters.

At most 5 fields out of the available 7 will be encoded for the Circuit ID in the order specified by the user.

If any format other than user-string is specified, the setting of string value will not be allowed through SNMP and WEB.

If the format type is user-string, it will be mandatory to provide the string value through SNMP using Multi-varbind.

Same format can be configured multiple number of times.

Example

```
pppoe-ia circuit-id default
pppoe-ia circuit-id ascii base-mac vlan
pppoe-ia circuit-id ascii system-name interface user-string cid1
pppoe-ia circuit-id ascii cvlan interface-alias base-mac user-string cid1 delimiter –
pppoe-ia circuit-id ascii system-name delimiter #
```

6. pppoe-ia remote-id { base-mac | system-name | mgnt-address | user- string <string> }

Globally configures a format to form an identifier that uniquely identifies the user attached to the access loop.

Syntax Definitions

base-mac The base mac-address of the switch.

system-name The configured name of the switch.

mgnt-address The management IP address of the switch.

user-string A configurable user string.

<string> The value of user configured string.

Usage Guidelines

By default, base-mac is used as the format for remote-id.
The remote-id can have a maximum of 63 characters. The remote-id longer than 63 characters will be truncated to 63 characters.
In case of mgnt-address format, the mgnt-address used is Loopback0 address if configured and active or the first active IP interface address otherwise 0.0.0.0 is used.
If any format other than user-string is specified, the setting of string value will not be allowed through SNMP and WEB.
If the format type is user-string, it will be mandatory to provide the string value through SNMP using Multi-varbind.

Example

```
pppoe-ia remote-id base-mac
pppoe-ia remote-id system-name
pppoe-ia remote-id mgnt-address
pppoe-ia remote-id user-string remoteuser1
```

7. clear pppoe-ia statistics [port { <slot/port[-port2]> } | linkagg <num>]

Clears the statistics for all the ports, a single port /linkagg or a range of ports for PPPoE Intermediate Agent.

Syntax Definitions

slot/port[-port2] The slot number for the module and the physical port number(s) on that module (e.g., 3/1 specifies port 1 on slot 3). Port2 refers to the last port in the range of ports.

num Linkagg id

Usage Guidelines

None

Example

```
clear pppoe-ia statistics
clear pppoe-ia statistics port 1/1
clear pppoe-ia statistics port 1/1-6
clear pppoe-ia statistics linkagg 0
```

clear pppoe-ia statistics linkagg 13

8. show pppoe-ia configuration
Displays the global configuration for PPPoE Intermediate Agent

Syntax Definitions
None

Usage Guidelines
None

Example

Default Configuration
show pppoe-ia configuration

```
Status                    : disabled,
Access Node Identifier
  Acess-node-id Format     : base-mac,
  Acess-node-id String     : 00:d0:95:ee:fb:02,
Circuit Identifier
  Circuit-Id Format        : default,
  Circuit-id Field1        : none,
  Circuit-id Field1 String : ,
  Circuit-id Field2        : none,
  Circuit-id Field2 String : ,
  Circuit-id Field3        : none,
  Circuit-id Field3 String : ,
  Circuit-id Field4        : none,
  Circuit-id Field4 String : ,
  Circuit-id Field5        : none,
  Circuit-id Field5 String : ,
  Circuit-id Delimiter     : “:”,
Remote Identifier
  Remote-id Format         : base-mac,
  Remote-id String         : 00:d0:95:ee:fb:02
```

pppoe-ia enabled
pppoe-ia access-node-id user-string “accessNode1”
pppoe-ia circuit-id ascii sytem-name base-mac interface delimiter “|”
pppoe-ia remote-id mngt-address
show pppoe-ia configuration

```
Status                    : enabled,
Access Node Identifier
  Acess-node-id Format     : system-name,
  Acess-node-id String     : vxTarget,
Circuit Identifier
  Circuit-Id Format        : ascii,
  Circuit-id Field1        : system-name,
  Circuit-id Field1 String : vxTarget,
  Circuit-id Field2        : base-mac,
  Circuit-id Field2 String : 00:d0:95:ee:fb:02,
  Circuit-id Field3        : interface,
  Circuit-id Field3 String : ,
  Circuit-id Field4        : none,
  Circuit-id Field4 String : ,
  Circuit-id Field5        : none,
  Circuit-id Field5 String : ,
  Circuit-id Delimiter     : “|”,
Remote Identifier
  Remote-id Format         : mgnt-address,
  Remote-id String         : 172.21.161.106
```

pppoe-ia access-node-id user-string “accessNode1”
pppoe-ia circuit-id ascii interface-alias cvlan system-name user-string “Circuit1” vlan delimiter “#”
show pppoe-ia configuration

```
Status                    : disabled,
Access Node Identifier
  Acess-node-id Format     : user-string,
  Acess-node-id String     : Node1,
Circuit Identifier
  Circuit-Id Format        : ascii,
  Circuit-id Field1        : interface-alias,
  Circuit-id Field1 String : ,
  Circuit-id Field2        : cvlan,
  Circuit-id Field2 String : ,
  Circuit-id Field3        : system-name,
  Circuit-id Field3 String : vxTarget,
  Circuit-id Field4        : user-string,
  Circuit-id Field4 String : Circuit1,
  Circuit-id Field5        : vlan,
  Circuit-id Field5 String : ,
  Circuit-id Delimiter     : “#”,
Remote Identifier
  Remote-id Format         : base-mac,
  Remote-id String         : 00:d0:95:ee:fb:02
```

9. show pppoe-ia {port [<slot/port[-port2]>] | linkagg <num>} [enabled | disabled | trusted | client]

Displays the PPPoE Intermediate Agent configuration for a port, port range or all the ports. Also displays the port or port range configuration for ports with PPPoE-IA enabled or disabled or ports that are trusted or client.

Syntax Definitions

slot/port[-port2] The slot number for the module and the physical port number(s) on that module (e.g., 3/1 specifies port 1 on slot 3). Port2 refers to the last port in the range of ports.

num Linkagg Id

Usage Guidelines
None

Example
show pppoe-ia port

```
Slot/Port    Status      Mode
```

```
----------+----------+------------
1/1       enabled     client
1/2       disabled    trusted
1/3       disabled    client
1/4       enabled     trusted
.
1/24       enabled     client
0/0        enabled     client
0/1        disabled    trusted
```

show pppoe-ia port 1/1

```
Slot/Port    Status      Mode
----------+----------+------------
1/1       enabled     client
```

show pppoe-ia port 1/3-5

```
Slot/Port    Status      Mode
----------+----------+------------
1/3       enabled     client
1/4       disabled    trusted
1/5       disabled    client
```

10. show pppoe-ia [port { <slot/port[-port2]> } | linkagg <num>] statistics

Displays the PPPoE-IA statistics for a port/linkagg, port range or all the ports.

Syntax Definitions

slot/port[-port2] The slot number for the module and the physical port number(s) on that module (e.g., 3/1 specifies port 1 on slot 3). Port2 refers to the last port in the range of ports.

num Linkagg Id

Usage Guidelines

None

Example

show pppoe-ia statistics

```
Slot/  PADI   PADR   PADT    PADI     PADR    PADT    PADO    PADS
Port    Rx     Rx     Rx    Discard  Discard Discard Discard Discard
------+------+------+------+--------+-------+-------+-------+--------
1/1     2      2      0      1       0       0       2       3
1/2     2      1      0      1       0       0       2       0
1/3     3      2      2      2       1       2       2       3
.
1/24    2      2      0      1       0       0       2       3
0/0     2      2      0      1       0       0       2       3
0/1     2      2      0      1       0       0       2       3
```

show pppoe-ia port 1/1 statistics

```
Slot/  PADI   PADR   PADT    PADI     PADR    PADT    PADO    PADS
```

```
Port    Rx     Rx     Rx    Dropped  Dropped Dropped Dropped Dropped
------+------+------+------+--------+-------+-------+-------+--------
1/1     2      2      0      1       0       0       2       3
```

show pppoe-ia linkagg 1 statistics

```
Slot/  PADI   PADR   PADT    PADI     PADR    PADT    PADO    PADS
Port    Rx     Rx     Rx    Discard  Discard Discard Discard Discard
------+------+------+------+--------+-------+-------+-------+--------
0/1     2      2      0      1       0       0       2       3
```

show pppoe-ia port 1/1-10 statistics

```
Slot/  PADI   PADR   PADT    PADI     PADR    PADT    PADO    PADS
Port    Rx     Rx     Rx    Discard  Discard Discard Discard Discard
------+------+------+------+--------+-------+-------+-------+--------
1/1     2      2      0      1       0       0       2       3
1/2     2      1      0      1       0       0       2       0
1/3     3      2      2      2       1       2       2       3
.
1/10    2      2      0      1       0       0       2       3
```

Limitations:

None

10. DHL Active-Standby Increased Size

Introduction:
The Dual-Home Link (DHL) Active-Standby feature is already supported. It is limited to Linkagg of size 2. We are extending DHL to support Linkagg of size 4 such that 2 active links and 1 standby link can be configured. For detailed feature configuration and usage guidelines please refer network configuration guide.

Platforms Supported:

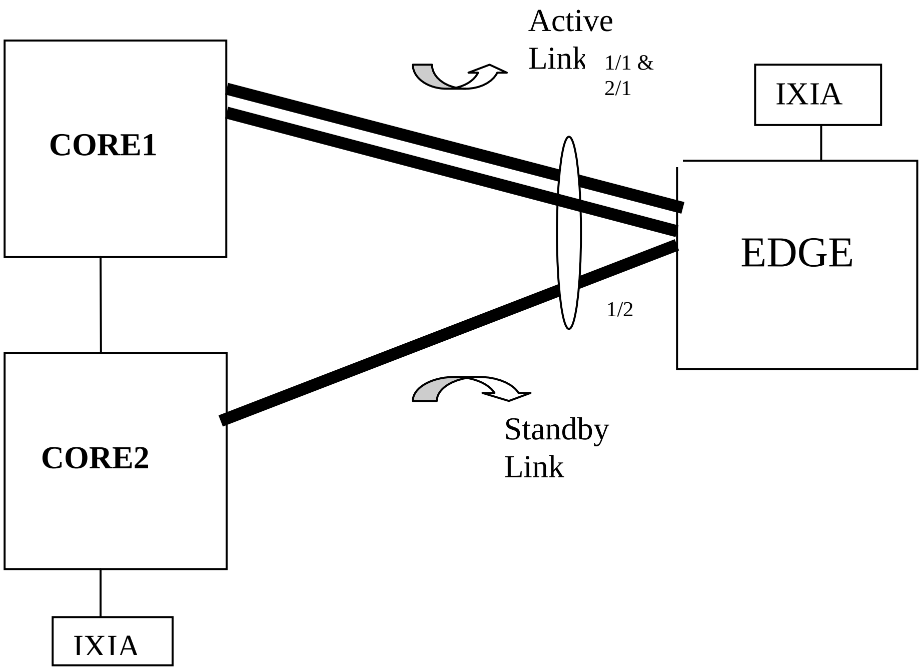
Omni Switch 6850, 6850E

Commands usage:

No new commands introduced.

Topology :

On EDGE device create the LACP linkagg group of size 4 and set port 1/2 in STANDBY mode:



```
-> lacp linkagg 1 size 4 admin state enable
-> lacp linkagg 1 actor admin key 1
-> lacp agg 1/2 standby enable
-> lacp agg 1/1 actor admin key 1
-> lacp agg 1/2 actor admin key 1
-> lacp agg 2/1 actor admin key 1
```

11. Telnet Port

Introduction:
This feature will allow the AOS switch to act as a telnet client and connect to external telnet servers running on non-default TCP port (i.e other than port 23). This feature will support telnet over both IPv4 and IPv6. This is only applicable when the switch is acting as a Telnet Client. The Telnet Server running on the AOS will still be listening on TCP port 23

Platforms Supported:
OS6850, OS6850E, OS6855, OS6400, OS9000E

CLI Commands:
telnet {host_name | host_ip_address} port [dest_port]
telnet6 {host_name | host_ip_address} port [dest_port] [ifname]
Port Number Range should be between 1024 and 65535

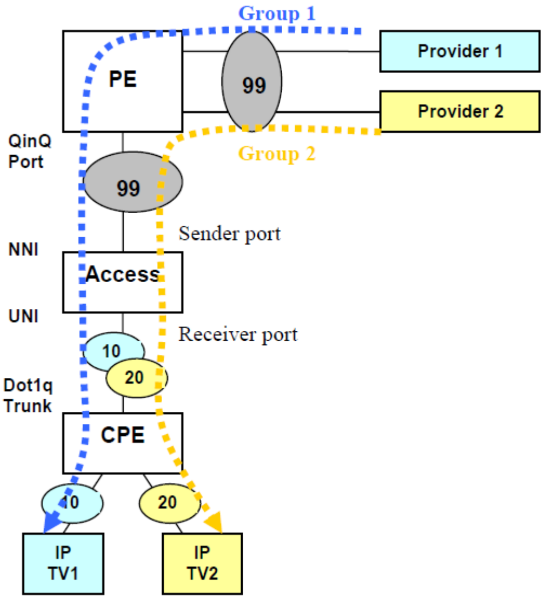
Examples:
telnet6 3ffe:0501:0008:0000:0260:97ff:fe40:efab port 1122
telnet 1.1.1.1 port 1122

Limitation:
None

12. IPMVLAN Replication

Introduction:
IPMVLAN Replication feature is to allow several subscribers from different VLANs on a trunk interface to subscribe and unsubscribe to a single IPMVLAN. This feature is supported on Ethernet-Service mode and Enterprise mode. QinQ service is provided using E-Service mode. Pure dot1q service is provided by Enterprise mode.

E-Service



Service Details

Internet service is provided using QinQ.
Multicast service is provided using dot1q.

Setup Details

2 providers share the same IPMVLAN 99.
The PE is connected to the Access switch on QinQ port.
The PE acts as the querier.
Ethernet-Service is configured in the Access switch. The Access switch is connected to the PE on NNI and connected to the CPE on UNI.

In Access switch, CVLAN 10 and 20 configured on the UNI.
In Access switch, Sender port and Receiver port is configured. Receiver VLANs (RVLANs) 10 and 20 are configured on the Receiver port.
The CPE is connected to the Access switch on a qtagged trunk.
Each provider deploy their own STB in customer premises.
Each STB uses its own VLAN. In this case, VLAN 10 and VLAN 20.

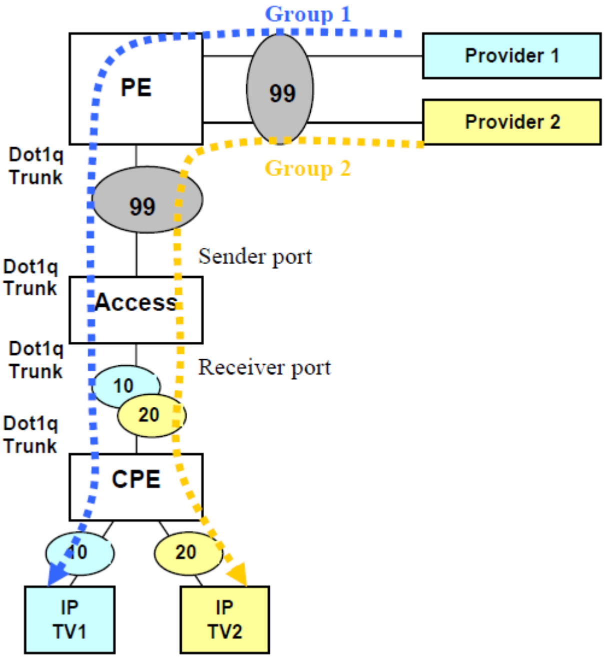
Working

The Access switch snoops the IGMP membership messages from the STB and maintains the membership on multicast VLAN 99 for Receiver VLANs 10 and 20.
Multicast source traffic is forwarded from sender port to group members on the receiver port tagged with RVLANs.

Configuration in Access switch

```
 ! IPMS :
ip multicast status enable
! VLAN :
 vlan 1 enable name "VLAN 1"
ethernet-service ipmvlan 99 name "VLAN 99"
ethernet-service svlan 1000 name "VLAN 1000"
! VLAN STACKING:
 ethernet-service svlan 1000 nni 1/1
ethernet-service service-name "customer1" svlan 1000
ethernet-service sap 10 service-name "customer1"
 ethernet-service sap 10 uni 1/2
ethernet-service sap 10 cvlan 10
ethernet-service sap 10 cvlan 20
vlan ipmvlan 99 sender-port port 1/1
 vlan ipmvlan 99 receiver-port port 1/2 receiver-vlan 10
vlan ipmvlan 99 receiver-port port 1/2 receiver-vlan 20
vlan ipmvlan 99 address 227.0.0.7
```

Enterprise



Service Details
Internet service is provided using dot1q.
Multicast service is provided using dot1q.

Setup Details
2 providers share the same IPMVLAN 99.
The PE is connected to the Access switch on a qtagged trunk.
The PE acts as the querier.
In Access switch, VLAN 10 and 20 are created as regular tagged VLANs.
In Access switch, Sender port and Receiver port is configured. Receiver VLANs (RVLANs) 10 and 20 are configured on the Receiver port.
The CPE is connected to the Access switch on a qtagged trunk.
Each provider deploy their own STB in customer premises.
Each STB uses its own VLAN. In this case, VLAN 10 and VLAN 20.

Working
The Access switch snoops the IGMP membership messages from the STB and maintains the membership on multicast VLAN 99 for Receiver VLANs 10 and 20.
Multicast source traffic is forwarded from sender port to group members on the receiver port tagged with RVLANs.

Configuration in Access switch

```
! IPMS :
 ip multicast status enable
 ! 802.1Q :
vlan 10 802.1q 1/2 "TAG PORT 1/2 VLAN 10"
vlan 20 802.1q 1/2 "TAG PORT 1/2 VLAN 20"
```

```
! VLAN :
vlan 1 enable name "VLAN 1"
vlan ipmvlan 99 name "VLAN 99"
! VLAN STACKING:
vlan ipmvlan 99 sender-port port 1/1
vlan ipmvlan 99 receiver-port port 1/2 receiver-vlan 10
vlan ipmvlan 99 receiver-port port 1/2 receiver-vlan 20
vlan ipmvlan 99 address 227.0.0.7
vlan ipmvlan 99 address 227.0.0.7
```

Platforms Supported:
OS6850, OS6850E, OS6855, OS6400, OS9000E

Commands:

[no] vlan ipmvlan <num> receiver-port {port <slot/port> | port <slot/port1-port2>| linkagg <aggregate_num>| linkagg <aggregate_num1-aggregate_num2>} [receiver-vlan <num>]

This command is used to configure the port (or a range of ports) as receiver port for the IPMVLAN and associate RVLAN to receiver port (or a range of receiver ports).

Syntax Definitions

ipmvlan *An existing VLAN ID number (1–4094) of the IPMVLAN to which the port is to be attached as the receiver port*

slot/port *The slot number for the module and the physical port number on that module (e.g. 3/1 specifies port 1 on slot 3). If port range specified, then all ports should be on the same slot. Port range across multiple slots not accepted*

aggregate_num *The link aggregate ID number (0–31) to assign as the receiver port to the specified IPMVLAN*

receiver-vlan *Receiver vlan to be associated with the receiver port(s)*

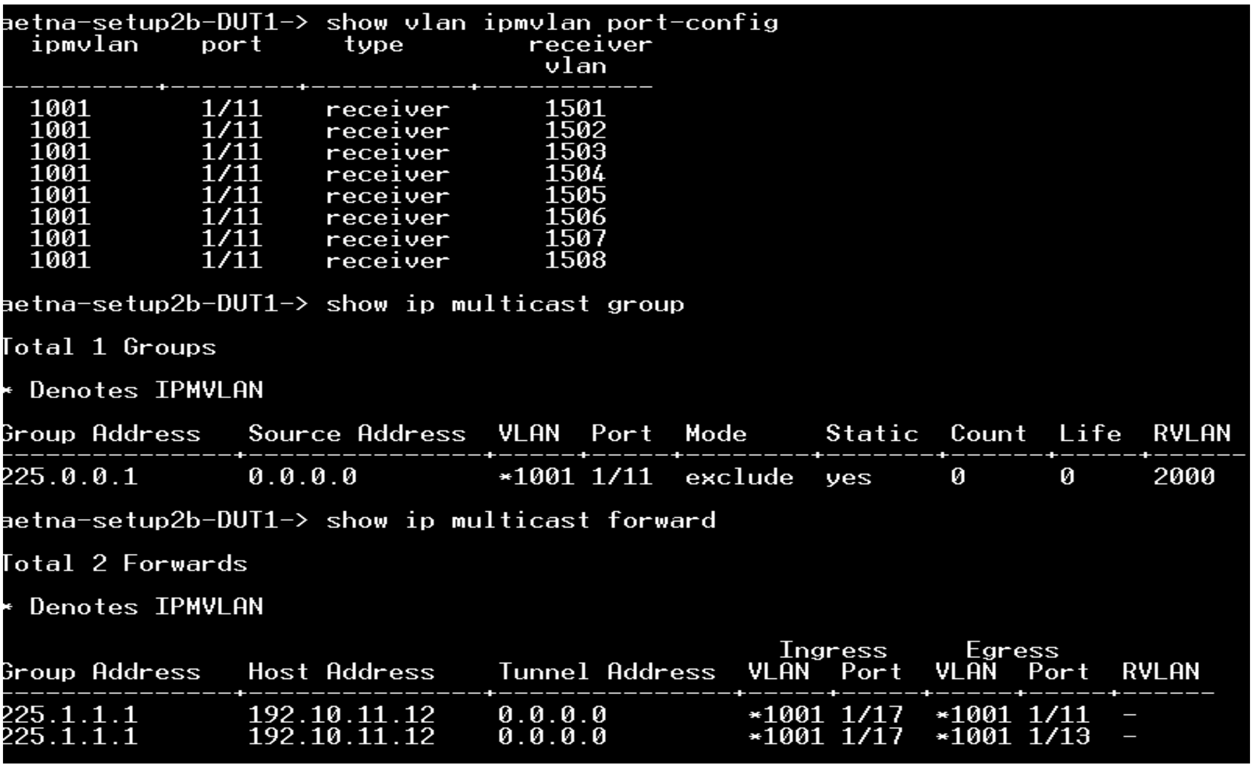
[no] ip multicast static-group <address> vlan <num> port <num | slot/port> [receiver-vlan <num>]
This command is used to create/delete a static IGMP group entry on a specified VLAN, port and on a specified receiver vlan.

Syntax Definitions
addressThe IP address of the multicast group

vlan <num> *Vlan to include as a static IGMP Group. In this case, user should provide the IPMVLAN.*

num | slot/port *The port number or the linkagg ID on which the user wants to configure a static IGMP group. In this case, user should provide the receiver port.*

receiver-vlan *VLAN ID number (2–4094).*

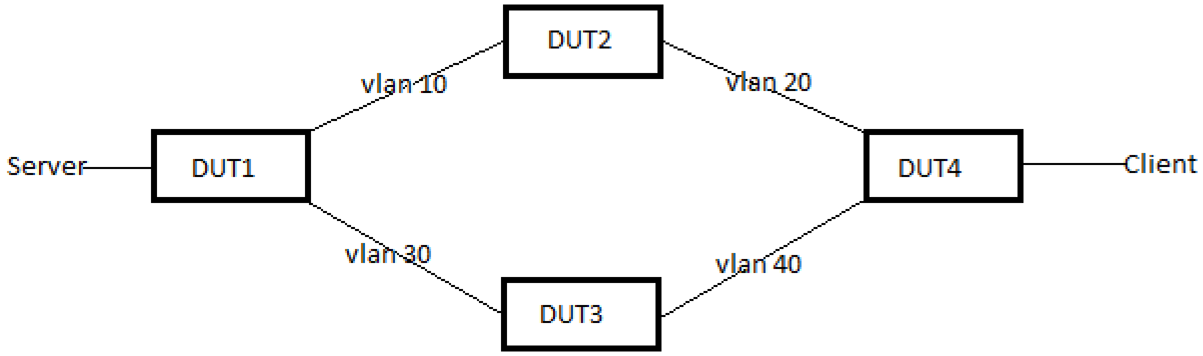


```
aetna-setup2b-DUT1-> show vlan ipmvlan port-config
  ipmvlan     port      type         receiver
                                       vlan
----------+--------+----------+-----------
  1001       1/11    receiver      1501
  1001       1/11    receiver      1502
  1001       1/11    receiver      1503
  1001       1/11    receiver      1504
  1001       1/11    receiver      1505
  1001       1/11    receiver      1506
  1001       1/11    receiver      1507
  1001       1/11    receiver      1508

aetna-setup2b-DUT1-> show ip multicast group

Total 1 Groups

* Denotes IPMVLAN

Group Address    Source Address   VLAN  Port  Mode      Static  Count  Life  RVLAN
---------------+----------------+-----+-----+---------+--------+-------+-----+------
225.0.0.1        0.0.0.0          *1001 1/11  exclude   yes     0      0     2000

aetna-setup2b-DUT1-> show ip multicast forward

Total 2 Forwards

* Denotes IPMVLAN

                                                 Ingress      Egress
Group Address    Host Address     Tunnel Address   VLAN  Port   VLAN  Port   RVLAN
---------------+----------------+----------------+-----+------+-----+-----+------
225.1.1.1        192.10.11.12     0.0.0.0          *1001 1/17   *1001 1/11   -
225.1.1.1        192.10.11.12     0.0.0.0          *1001 1/17   *1001 1/13   -
```

13. PIM Sub-second Convergence

Introduction:

This feature is to minimize the delay at the time of failure in the primary path forwarding multicast data packets by deploying BFD in Multicast Routing Protocols – in both PIM DM and PIM SM. On intimation from BFD about the primary link (neighbor) failure, sub second convergence could be achieved by a redundant path to carry forward the source traffic immediately. And also to minimize the delay in resuming the data packet flow in the alternate path by deploying the redundant path functionality.



Platforms Supported:
OS6850, OS6850E, OS6855, OS9000E

Commands Usage:
The below commands were introduced for this feature

ip pim interface <interface> bfd-std {enable | disable }
This enables bfd for the pim interface

ip pim sparse bfd-std status {enable | disable}
This enables BFD for PIMSM protocol

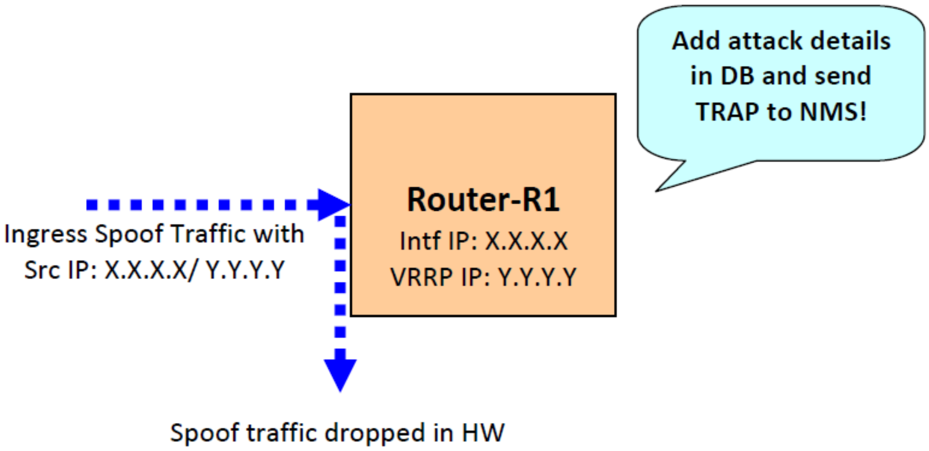
ip pim dense bfd-std status {enable | disable}
This enables BFD for PIMDM protocol

14. IP and ARP Spoof Protection

Introduction:

IP and ARP spoof detection feature will allow the network administrator to block and know the originator of spoof traffic coming from front panel ports with Source IP as IP-addresses configured internal to the router. Once IP spoof-detection is enabled, all data and control packets ingress on the switch with Vlan and internal IP-address of that Vlan as source information will be dropped. The details of dropped spoof packets will be maintained in the attack database. For any new attack event (source ip, source mac, source vlan) combination, a TRAP will be generated to NMS station if configured. The router will send gratuitous ARP request for each and every attack attempt. CLI options provided to enable IP and ARP Spoof detection at the Global level, per IP interface level and per VRRP IP address level

Sl. No.	Global Status	Per Interface IP Anti-Spoof Status	Per IP Interface Arp-Only Spoof Status	Per Virtual Router IP Anti-Spoof Status	Per Virtual Router IP Arp-Only Spoof Status
1.	Anti-Spoof Enabled	Enabled	Enabled	Enabled	Enabled
2	Anti-Spoof Disabled	Disabled	Disabled	Disabled	Disabled
3	Arp-Only Spoof Enabled	Disabled	Enabled	Disabled	Enabled
4.	Arp-only Spoof Disabled	Enabled	Enabled	Enabled	Enabled


Add attack details in DB and send TRAP to NMS!
Router-R1
Intf IP: X.X.X.X
VRRP IP: Y.Y.Y.Y
Ingress Spoof Traffic with Src IP: X.X.X.X/ Y.Y.Y.Y
Spoof traffic dropped in HW

Platforms Supported:
OS6850, OS6855, OS6400, OS6850E, OS9000E.

CLI commands:
ip dos anti-spoofing {enable | disable}
This command configures ip anti-spoofing at global level.

ip dos anti-spoofing arp-only {enable | disable}
This command configures arp-only spoof detection at Global level

ip dos anti-spoofing address <ip-address> {enable | disable}
This command configures IP Spoof at Per Interface

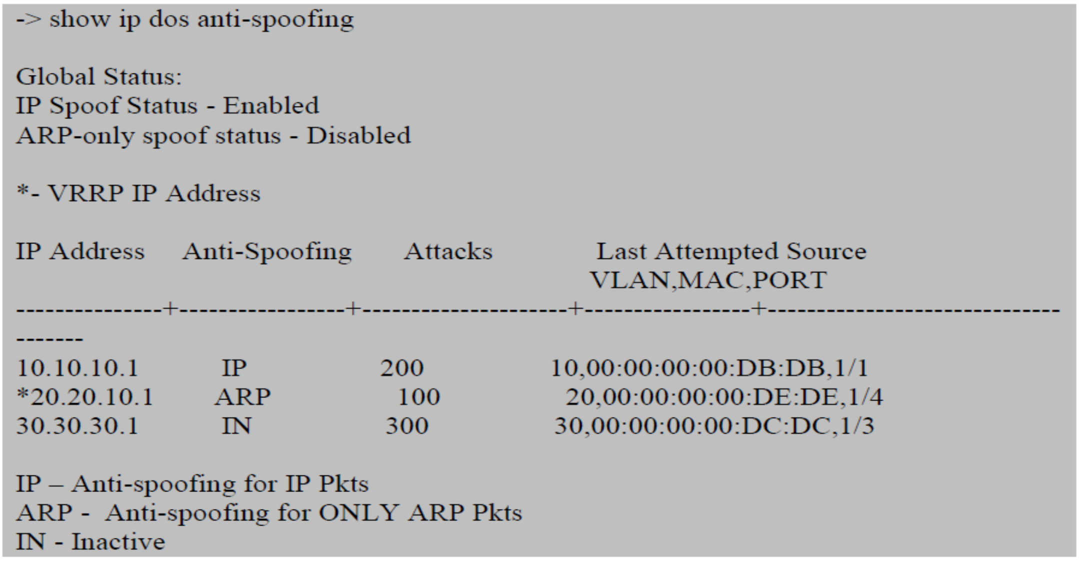
ip dos anti-spoofing address <ip-address> arp-only {enable | disable}
This command configures arp-only Spoof configuration Per IP Interface.
ip dos anti-spoofing clear stats
This command clears the Anti-Spoofing Attack Information Globally.

ip dos anti-spoofing address <ip-address> clear stats

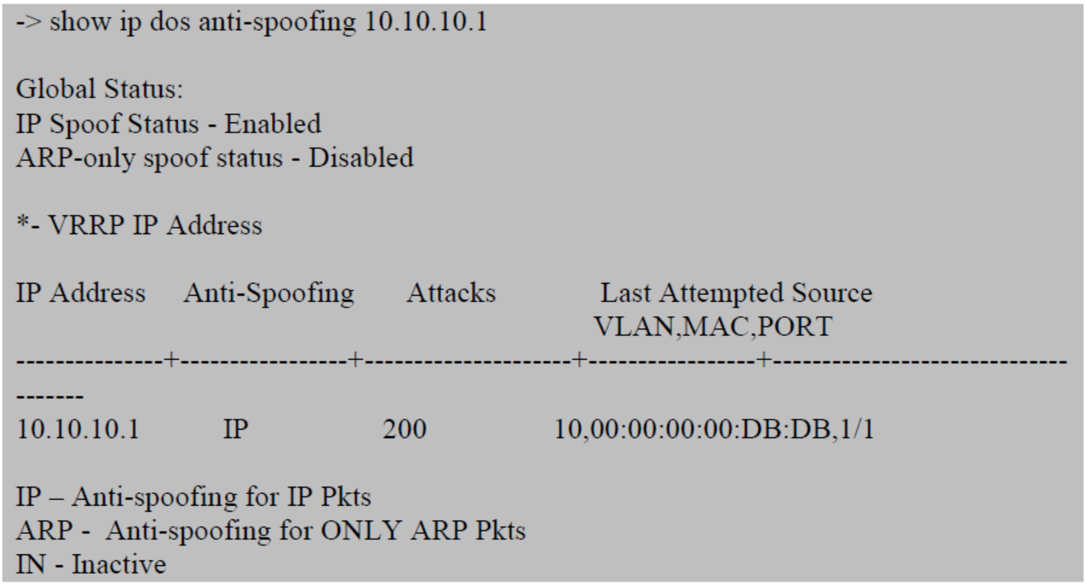
This command clears the Anti-Spoofing Attack Information at Per Interface

show ip dos anti-spoofing
This cli displays all the attack information

show ip dos anti-spoofing <ip-address>
This cli displays all the attack information particular interface



```
-> show ip dos anti-spoofing

Global Status:
IP Spoof Status - Enabled
ARP-only spoof status - Disabled

*- VRRP IP Address

IP Address     Anti-Spoofing      Attacks           Last Attempted Source
                                                   VLAN,MAC,PORT
---------------+-----------------+---------------------+-----------------+------------------------------
-------
10.10.10.1          IP              200             10,00:00:00:00:DB:DB,1/1
*20.20.10.1        ARP               100              20,00:00:00:00:DE:DE,1/4
30.30.30.1          IN               300             30,00:00:00:00:DC:DC,1/3

IP – Anti-spoofing for IP Pkts
ARP -  Anti-spoofing for ONLY ARP Pkts
IN - Inactive
```



```
-> show ip dos anti-spoofing 10.10.10.1

Global Status:
IP Spoof Status - Enabled
ARP-only spoof status - Disabled

*- VRRP IP Address

IP Address     Anti-Spoofing      Attacks           Last Attempted Source
                                                   VLAN,MAC,PORT
---------------+-----------------+---------------------+-----------------+------------------------------
-------
10.10.10.1          IP              200             10,00:00:00:00:DB:DB,1/1

IP – Anti-spoofing for IP Pkts
ARP -  Anti-spoofing for ONLY ARP Pkts
IN - Inactive
```

15. Routed IP Port

Introduction:

AOS currently supports addition of an IP interface on a particular VLAN. The device type is set to VLAN and the physical ports are attached to the particular VLAN. The current IP interface is not directly associated with the physical port and the underlying VLAN can support a host of L2 protocols and also VLAN switching. A routed port is a physical port on which we supporting L3 functionality. To achieve this we also support an IP interface of new device type “RTR-PORT” and specify the rtr-vlan, rtr-port and the type (tagged/ untagged VLAN frames) in one go. The user shall not be able to modify any of these 3 parameters once specified, but will have to delete and recreate the IP interface to change the association. The user will however be allowed to administratively disable the IP interface. The underlying rtr-vlan will not switch in L2 as there is only one port associated with the VLAN.

Platforms supported:

OS6850, OS6855, OS6400, OS6850E, OS9000E.

CLI commands:

[no] ip interface <name> {vlan <num> | { rtr-port [<agg_num>| <slot/port>] rtr-vlan <num> [type {tagged | untagged}]} }

rtr-port: The physical port associated with the IP interface (device type “RTR-PORT”). This can be the “slot/ port” to identify the port or the “agg-num” in the case of a link aggregation port. This parameter is mandatory for a RTR-PORT IP interface.

rtr-vlan: An unused vlan on the system to be associated with this IP interface. This parameter is mandatory for a RTR-PORT IP interface.

type: Tagged or untagged specifying whether to handle 802.1q frames or untagged frames on the specified port. This parameter is optional and defaults to type “untagged” if not specified.

Examples :-

```
ip interface IP1 rtr-port 1/2 rtr-vlan 20 type untagged
ip interface IP2 rtr-port 3 rtr-vlan 40 type tagged
```

The IP interface needs to be associated with the rtr-port, rtr-vlan (an unused vlan) and the type (tagged for handling 802.1q frames on the port or untagged to handle untagged frames) for setting this to be a RTR-PORT IP interface. The options vlan / rtr-port are mutually exclusive - the device type will be set to VLAN or RTR-PORT accordingly. Note that the other existing parameters like address/ mask for an IP interface remain as they are as for a VLAN IP interface.

16. UDP Relay to a specific IP address

Introduction:

This enhancement feature helps AOS switches for relaying UDP packets to an ip address (destination ip). Earlier, the existing AOS implementation redirects the broadcasted UDP packets to a destination VLAN (Server's VLAN). This enhancement provides an additional feature of relaying all custom serviced UDP packets to the configured ip address (Server's IP) as unicast packet.

Platforms Supported:

OS6400, OS6855, OS6850E,OS6850, OS9000E.

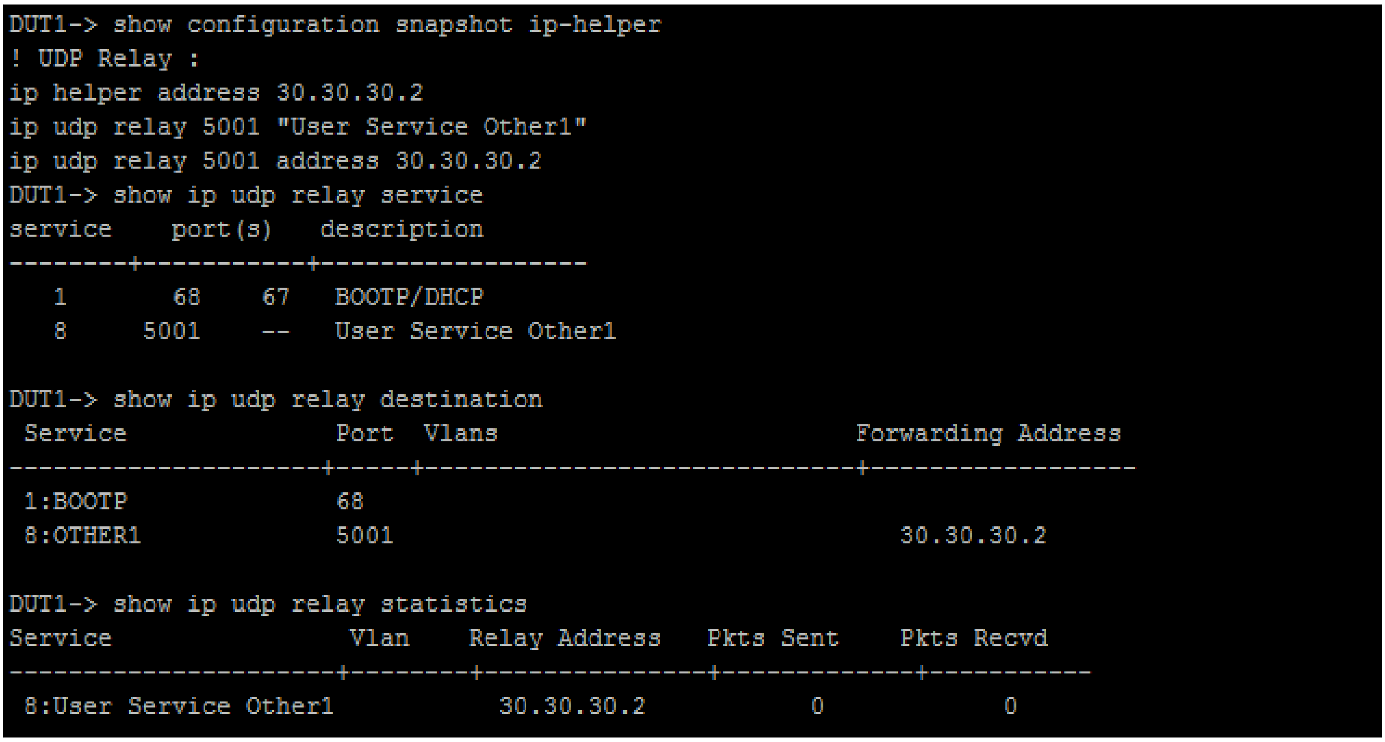
Commands Usage:

ip udp relay <*port No*> address <*ipv4 address*>

Syntax Definitions

Port no A user specified port that is not a well-known port
IPv4 address UDP server address to which the UDP packets are destined.

Configuration snapshot:



```
DUT1-> show configuration snapshot ip-helper
! UDP Relay :
ip helper address 30.30.30.2
ip udp relay 5001 "User Service Other1"
ip udp relay 5001 address 30.30.30.2
DUT1-> show ip udp relay service
service    port(s)   description
--------+-----------+------------------
   1       68    67   BOOTP/DHCP
   8     5001    --   User Service Other1

DUT1-> show ip udp relay destination
 Service              Port  Vlans                        Forwarding Address
---------------------+-----+-----------------------------+------------------
 1:BOOTP              68
 8:OTHER1             5001                                  30.30.30.2

DUT1-> show ip udp relay statistics
Service                Vlan    Relay Address   Pkts Sent    Pkts Recvd
----------------------+--------+---------------+-------------+-----------
 8:User Service Other1           30.30.30.2           0            0
```

Limitations:

This service is unidirectional only. The response from UDP server must be sent directly to the UDP client and software will not process those packets.
If the configured UDP server and UDP client located on the same VLAN, then the server receives duplicate packets as the switch will perform native broadcast and relaying also.
One relay IP per UDP port is supported.
UDP packets will be routed only between same VRF

17. MAX BFD-512

Introduction
This feature enhancement facilitates to configure 64 BFD sessions per NI and 512 BFD sessions (8 NI's *64) per switch. Before this, only 16 BFD sessions per NI and 128 BFD sessions (8NI's * 16) per switch can be configured. Hence this feature has been scaled up so that more number of BFD sessions can be established per NI and switch. If BFD sessions are to be configured using multiple protocols in the switch, please refer the section 4(Information).

Platforms Supported
OS9000E

Commands Usage
Not Applicable

Information

While configuring BFD session using multiple protocols like OSPF, BGP,PIM, MULTI-HOP BGP, VRRP and Static route, Then Maximum 448 BFD sessions can be configured with 56 BFD sessions Per NI.

Below is the distribution of 448 BFD sessions of various protocols slot wise:

		BFD SESSIONS						
SWITCH	OSPF neighbours	OSPF	PIM	BGP	EBGP MULTI HOP	STATIC	VRRP	TOTAL BFD SESSIONS/NI
SLOT 1	24	12	12	2	4	22	4	56
SLOT 2	23	12	11	2	4	27	0	56
SLOT 3	24	12	12	2	4	26	0	56
SLOT 4	23	12	11	4	4	21	4	56
SLOT 5	23	12	11	2	0	31	0	56
SLOT 6	24	12	12	4	0	28	0	56
SLOT 7	23	12	11	0	0	31	2	56
SLOT 8	24	12	12	0	0	32	0	56
	TOTAL BFD SESSIONS/ SWITCH							448

Limitations:

EBGP multi hop BFD sessions cannot be established with OSPF as an IGP because of ECMP routes, alternatively static routes can be used.
While configuring BFD session using multiple protocols like OSPF, BGP,PIM, MULTI-HOP BGP, VRRP and Static route, CPU may spike when BFD sessions are configured beyond 448 sessions(56 BFD sessions/NI).

18. Captive-portal Performance Improvements

Introduction:

Captive-Portal Enhancement Phase 2 deals with the overhauling of EmWeb Server so as to improve the performance of Captive-portal . As per the current implementation, the serving of Captive-portal web-pages is slow when multiple users try to access the login page at the same time. This slow performance is not only due to the design of EmWeb Server but also due to the current Captive-portal traffic rate limiting implemented. This enhanced feature will improve the performance of captive-portal to accommodate even if an average of 20 users requested the page at a time.

Captive-portal Enhancement phase 2 also provides Auto-proxy support to the users that enable them to automatically obtain their proxy settings, without taking the effort of manually configuring them in their browser or internet application settings.

Platforms Supported:

OS6850, OS9000E, OS6850E, OS6400 and OS6855

Commands Usage:

No new commands introduced as part of this feature

19. HIC on OS 9000E

Introduction:

This Enhancement extends the “Host Integrity Check” feature to OS 9000E. It was already supported in OS 6850, 6850E, 6400 and 6855. Host Integrity Check (HIC) is a mechanism for verifying the compliance of an end user device when it connects to the switch. Configurable HIC policies are used to specify, evaluate, and enforce network access requirements for the host. For example, is the host running a required version of a specific operating system or anti-virus software up to date.

Platforms Supported:

OmniSwitch 9000E

Commands usage:

All existing HIC commands will be supported in OS9000E

Limitations:

None

20. Increase in number of OSPF interface per Area

Introduction:

This enhancement feature helps AOS switches for creating more than 100 OSPF interface per Area. By default, we can create only 100 OSPF interfaces per area. In this enhancement, “gOspfAreaMaxIntfs” variable is set to the required number of OSPF interfaces. This variable should be declared in the config file “AlcatelDebug.cfg”. An Optimization has also been introduced with this enhancement.

Before this enhancement, a passive OSPF interface was created with 4 lines of configuration in boot.cfg. This would be a tedious one when there is more number of passive OSPF interfaces created in an Area. To optimize this difficulty, route map is used. A route map with set action of route-type internal needs to be created for the local interface (routes) on which passive OSPF interface needs to be created. Using this route-map in redistribution of local into OSPF, the passive OSPF interfaces will be learned as intra routes. Thus those interfaces will act as passive OSPF interfaces. The OSPF interfaces created by the route-map command can be accessed in all the OSPF display commands. This passive OSPF interface will not be written into boot.cfg and will not be visible in snapshot.

Eg:
Include all IP interfaces which need to be configured as passive ospf interface, in a route map and then use the below commands to have them as passive ospf interface without configuring those IP interfaces as ospf interface.

```
ip route-map "R1" sequence-number 50 action permit
ip route-map "R1" sequence-number 50 set metric-type internal
ip redist local into ospf route-map R1 status enable
```

Platforms Supported:

OS6855, OS6855-U24X, OS6850E,OS6850, OS9000E.

Commands usage:

No new commands introduced

Limitations:

If there is local to OSPF redistribution route-map along with passive interface creation route map, administrator has to take care that the match criteria is clearly defined

If there are multiple areas configured in the OSPF domain. The OSPF interface would be created in backbone area

21. Multicast Boundary Range Expansion

Till this 6.4.4 release users have the ability to stop multicast traffic being forwarded out from an ip interface by using the "ip mroute boundary" command:
ip mroute-boundary *if_name scoped_address mask*

However, the scoped address range is limited to 239.0.0.0 – 239.255.255.255. There can be multicast addresses that are used for a group outside of this range as well. This enhancement allows the mroute boundary scope address to be expanded to all multicast group range. 225.0.0.0 through 239.255.255.255.

22. Acct-Input-Gigawords & Acct-Output-Gigawords

Introduction:
This enhancement feature provides the facility to identify how many times the Acct-Input-Octets(type-42), Acct-Output-Octets(Type-43) counter has wrapped around 2^32 it will calculate the value in multiples of 4GB and send using the attributes Acct-Input-Gigawords (type 52) & Acct-Output-Gigawords (type 53).Earlier, size of Acct-Input-Octets & Acct-Output-Octets with which we can only represent maximum 4GB(2^32) of Octets. In this enhancement Acct-Input-Gigawords, Acct-Output-Gigawords will be sent in Interim-Update, Periodic-Interim-Update & Stop Messages. Acct-Input-Gigawords, Acct-Output-Gigawords that are sent in accounting packets for both supplicant and non-supplicant users.

Platforms Supported:
OS6850,OS6855,OS6855-U24X, OS6850E, OS6400, OS9000E.

Commands usage:
Commands are same as in previous feature.

Information:

Whenever the input octets and output octets exceeds 2^32-1 bytes i.e. before sending accounting packet to the Radius Server these octets were converted into multiples of 4GB and will be sent in attributes Acct-Input-Gigawords(Type-52) Acct-Output-Words(Type =53).

```
Ex 1:     if input octets              =        5368711570
              Acct-Input-Gigawords          =        5368711570/(2^32-1) = 1(4GB)
              Acct-Input-Octets             =        5368711570/(2^32-1) = 1073744274.
```

Ex2: If output Octets = 13958643712
Acct-Output-Gigawords = 13958643712/(2^32-1)= 3(12GB)
Acct-Output-Octets = 13958643712/(2^32-1)= 1073741824

Limitations:
None

23. Automatic OSPF static neighbor in point-to-point

Introduction:
This feature is enhanced to detect the OSPF neighbors dynamically on P2P interface. Earlier, we have to configure the neighbors statically for P2P Interface in-order to establish neighbor ship /adjacencies between two peers.

According to the new implementation, the OSPF router dynamically detects neighbor routers by using the Hello packets in that P2P interface. So, we don’t need to configure the neighbors statically

Platforms Supported:
OS6855-U24X, OS6850E,OS6850,OS6855, OS9000E.

Commands usage:
There is no new Command introduced for this feature. We can check the neighbor ship establishment by using below commands

24. Calling Station-ID

Introduction:
This enhancement feature provides the facility to identify the ip-address of the supplicant, non-supplicant and ASA (telnet, console, ftp, ssh, http, https) clients via the attribute called Calling-station-Id in accounting request packet.

Earlier calling-station-id attribute was not filled for supplicant, non-supplicant or ASA (telnet, console, ftp, ssh, http, https) clients. This Feature is enhanced so that the ip-address of the Clients (Supplicant, non-supplicant and ASA (telnet, console, ftp, ssh, http, https)) is filled in calling-station-id attribute corresponding to the accounting session. Calling-station-id attribute will be present if the client receives the ip address. Calling-station-id attribute will be present only in the Interim-Update and Accounting Stop packet. For supplicant/non-supplicant clients Calling Station-ID is filled in the interim update accounting packet that is sent from the switch. This is applicable only when client is enabled to fetch IP dynamically and DHCP snooping is enabled on the switch.

Platforms Supported:
OS6850, OS6855, OS6855-U24X, OS6850E, OS6400, OS9000E

Commands usage:
Commands are same as in previous feature.

Limitations: None

25. LPS Sticky mode

Introduction:

This feature Enhancement provides the facility to configure the learning window to learn all mac as static and to allow the mac- movement within it.
Earlier, The LPS feature limits the number of MACs that can be learned, up to a pre-determined number, plus supports a learning time window, and provides logging and notification if a rule violation occurs. This feature is enhanced to support the static learning, mac-move(within the learning window) and infinite learning window.

Platforms Supported:
OS6850, OS6855, OS6855-U24X, OS6850E, OS6400, OS9000E

Commands usage:
port-security shutdown <num> [no-aging {enable|disable}] [convert-to-static {enable|disable}] [boot-up {enable|disable}] [learn-as-static {enable|disable]

Syntax Definitions

Learn-as-static : this option is used for learning a MAC as static during learning window.

Enable : Enables LAS functionality on this port.

Disable : Disables LAS feature on this port without removing LPS configuration.
Learning is unrestricted.

Usage Guidelines

By default, LAS admin-status is N/A.

When disabled, all filtered MAC addresses on the port are removed and all bridged and static MAC addresses stay “forwarding”. The LPS static mac configuration is preserved. The source learning mode is set the hardware mode for the port and all new MAC addresses are learnt and not visible in the LPS context. The port-security configuration is still allowed but not applied, but configuration of LPS static mac is refused. Reducing the “maximum” to a lower value than the number of static mac is also refused.

.

port-security shutdown <num> [no-aging {enable|disable}] [convert-to-static {enable|disable}] [boot-up {enable|disable}] [mac-move {enable|disable}]

Syntax Definitions

Mac-move : Allows the movement of pseudo static/static mac when enabled.

Usage Guidelines

By default, the option is N/A.

port-security shutdown <0> [{ no-aging <enable|disable>} |{convert-to-static <enable | disable>} | {boot-up <enable|disable>} | {learn-as-static <enable|disable>} | {mac-move <enable|disable>}]
Configuration will enable user to use all the options for learning window, when shut down time is zero.

Syntax Definitions:
Num : Learning window time in minutes (Max value ->65535)

No-aging : When enabled, MAC learnt during learning window will not be flushed.

Convert-to-static : When enabled, MAC learnt during learning window are converted into static MAC.

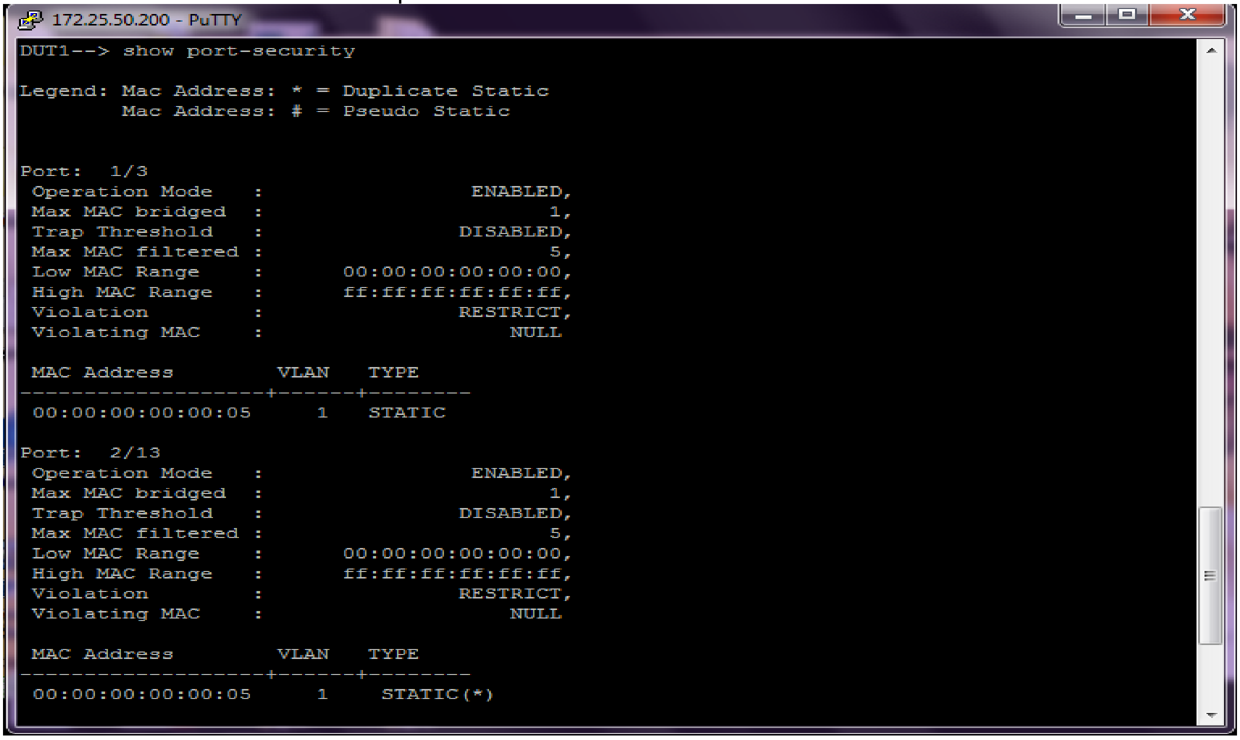
Boot-up : When enabled, Learning window should occur at boot-up time when box restarts.

Mac-move : Allows the movement of pseudo static/static mac when enabled.

Learn-as-static : this option is used for learning a MAC as static during learning window.

Usage Guidelines:
User can use all, any or none of flags with “port-security shutdown 0 command now .

Show commands are same as in previous feature.



172.25.50.200 - PuTTY

```
DUT1--> show port-security

Legend: Mac Address: * = Duplicate Static
        Mac Address: # = Pseudo Static


Port:  1/3
 Operation Mode    :                  ENABLED,
 Max MAC bridged   :                        1,
 Trap Threshold    :                 DISABLED,
 Max MAC filtered  :                        5,
 Low MAC Range     :        00:00:00:00:00:00,
 High MAC Range    :        ff:ff:ff:ff:ff:ff,
 Violation         :                 RESTRICT,
 Violating MAC     :                     NULL

 MAC Address         VLAN    TYPE
-------------------+------+--------
 00:00:00:00:00:05      1    STATIC

Port:  2/13
 Operation Mode    :                  ENABLED,
 Max MAC bridged   :                        1,
 Trap Threshold    :                 DISABLED,
 Max MAC filtered  :                        5,
 Low MAC Range     :        00:00:00:00:00:00,
 High MAC Range    :        ff:ff:ff:ff:ff:ff,
 Violation         :                 RESTRICT,
 Violating MAC     :                     NULL

 MAC Address         VLAN    TYPE
-------------------+------+--------
 00:00:00:00:00:05      1     STATIC(*)
```

Limitations:
None

26. Case Sensitive Mac-Address Authentication

Introduction:
This enhancement feature enables the AOS switches to send MAC address of the non-supplicant client in lower case as username and password for authentication to the authentication server. During non-supplicant authentication the client MAC address is sent as username and password. Earlier, for non-supplicant authentication the client MAC address is sent as username and password .This MAC address is sent in Uppercase for username and password. This enhancement enables to the send the MAC address of client as username and password in lower case.

Platforms Supported:
OS6850, OS6855, OS6855-U24X, OS6850E, OS6400, OS9000E

Commands usage:
Commands are same as in previous feature.

Information:

In order to facilitate this global variable “onexMacAuthLowerCase” is introduced setting which the MAC of the client is sent in lower case as username and password for authentication to the authentication server.
“onexMacAuthLowerCase” variable by default is set to 0.
“onexMacAuthLowerCase” can be set through Alcateldebug.cfg.
If onexMacAuthLowerCase =0 Username and password is sent in Uppercase .Hence for successful authentication the Mac address should be configured in Uppercase in authentication server.
If onexMacAuthLowerCase =1 Username and password is sent in Lowercase. Hence for successful authentication the Mac address should be configured in Lowercase in authentication server.

Limitations:
None

27. Support for 16 BFD sessions per slot

Introduction
This feature enhancement facilitates to configure 16 BFD sessions per NI and 64 BFD sessions (8 NI’s *16) per switch. Before this, only 8 BFD sessions per NI and 32 BFD sessions per switch can be configured. Hence this feature has been scaled up so that more number of BFD sessions can be established per NI and switch. If BFD sessions are to be configured using multiple protocols in the switch, please refer the section 4(Information).

Platforms Supported
OS6850 & OS6850E.

Commands usage
Not Applicable

Limitations:
BFD sessions are showing down while moving the BFD sessions from one Slot to another Slot

28. RADIUS-UNIQUE SESSION ID

Introduction:
This feature Enhancement provides the facility to differentiate the accounting packet received from users logging in supplicant, non-supplicant and ASA(telnet,console,ftp,ssh,http,https) clients by incorporating timestamp along with the mac-address of the clients in the Session-Id attribute of the accounting request packet. If the client is supplicant or non-supplicant then client's mac-address along with timestamp will be passed as session-id and for ASA clients(telnet,console,ftp,ssh,http,https) virtual mac-address along with timestamp will be passed as session-id.

Earlier session-id attribute used to be filled as mac-address of the supplicant/non-supplicant client and virtual mac-address for ASA (telnet, console, ftp, ssh, http, https) clients. Hence, it was difficult to differentiate the accounting sessions for users logging in and logging out from the clients. This Feature is enhanced so that accounting session-id can be enabled to differentiate the accounting sessions.

Platforms Supported:
OS6850, OS6855, OS6855-U24X, OS6850E, OS6400, OS9000E

Commands usage:

aaa accounting session-id <enable/disable>

Syntax Definitions

enable timestamp will be included along with mac-address in the session-id attribute in accounting request packet.

disable session-id attribute will contain only mac-address.

Defaults

By default accounting session-id will be disabled.

Limitations:
None

29. UNP BANDWIDTH RATE LIMITING

Introduction:
This feature Enhancement provides the facility to apply ingress and egress bandwidth limitations on a port on basis of UNP classification locally or remotely through radius-server return attribute. A UNP profile will be associated with maximum ingress and egress bandwidth, whenever authenticates under UNP policy either through radius returned UNP attribute or through local policy, associated bandwidth limitations are applied on port.
When Qos port with ingress or egress bandwidth specified will override bandwidth associated due to UNP. If ingress/egress bandwidth is set through qos port command then any change in qos port parameter will over ride bandwidth set due to UNP.

When multiple users authenticate under same port latest bandwidth limitation will overwrite the previous limitation existing on the port.

Earlier there was no option to associate bandwidth parameters with UNP. Hence No bandwidth limitation can be applied to the port on basis of UNP classification.

Platforms Supported:
OS6850, OS6855, OS6855-U24X, OS6850E, OS6400, OS9000E

Commands usage:
aaa user-network-profile name <profile-name> vlan <vlan> [maximum-ingress-bandwidth <num> maximum-egress-bandwidth <num> maximum-default-depth <num>]

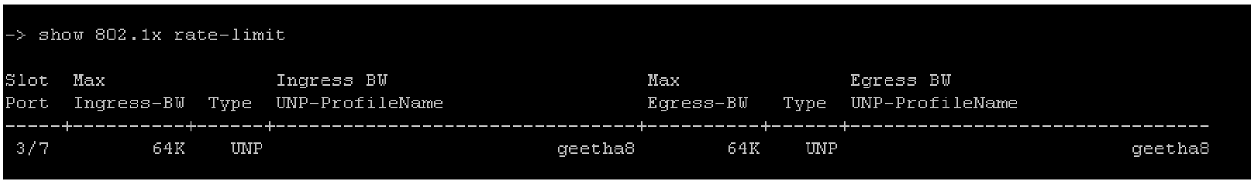
Syntax Definitions

Maximum-ingress-bandwitdh	Ingress bandwidth to be applied on the port
Maximum-egress-bandwitdh	egress bandwidth to be applied on the port
Maximum-default-depth	depth to be applied on the port

Defaults

Maximum-ingress-bandwitdh	-1 (no rate-limit)
Maximum-egress-bandwitdh	-1 (no rate-limit)
Maximum-default-depth	-1 (1 Mbps)

show 802.1X rate-limit



```
-> show 802.1x rate-limit

Slot  Max               Ingress BW                       Max               Egress BW
Port  Ingress-BW  Type  UNP-ProfileName                  Egress-BW   Type  UNP-ProfileName
-----+----------+------+---------------------------------+----------+------+--------------------------------
 3/7         64K    UNP                          geetha8        64K    UNP                          geetha8
```

Limitations:
None

30. PIM START-UP DELAY

Introduction:

This feature Enhancement provides the facility to configure the startup delay for PIM neighbourship, So that the PIM neighbourship will be formed after the delay value configured .This delay is applicable only when the switch boots up.
The delay can be configured in the range of 0 to 120. The default value for delay is 0.

In certain networks, when PIM become active before the unicast applications like OSPF and BGP, multicast packet loss will be observed until the unicast routing information gets manipulated. To overcome such packet loss due to startup latency between the PIM and unicast routing applications, a user-define startup delay has been introduced in PIM.

Platforms Supported:

OmniSwitch 6850/ 6855/ 6850E/ 9000E

Commands usage:

ip pim startup-delay <seconds>

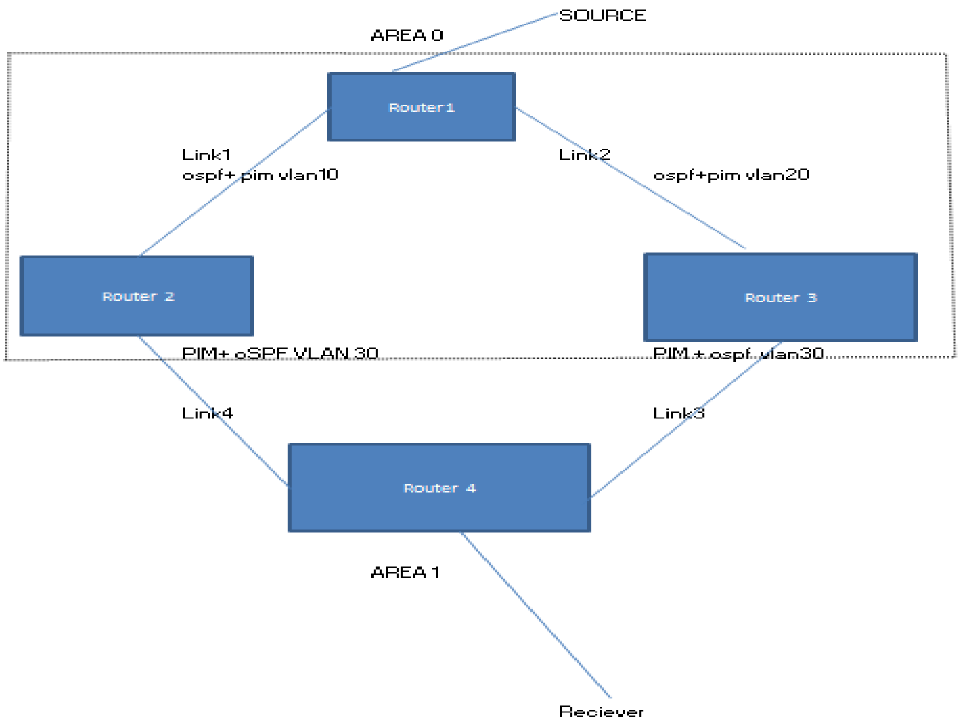
Syntax Definitions

Input Range	0 to 120 Seconds
Default value	0 Seconds

ILLUSTRATION

The input value of PIM start-up delay depends upon the packet loss occurring in the particular topology. For Example, in the below mentioned topology, The multicast traffic is flowing via Link1-link4 since it is best path via OSPF .when Router 2 is reloaded then traffic flows via Link2-Link3 and when Router 2 comes up, the PIM neighbourship in Link1-Link4 is established earlier than OSPF neighbourship, hence the multicast traffic switches to Link1-Link4 but because of lack of OSPF routing information, there will be time loss of 10 seconds.

Now if PIM start-up delay is configured as 30 seconds in Router 2, and when Router2 boots up, the PIM nieghbourship establishes after 30 seconds since boot up, so that in the meantime OSPF convergence is ensured, hence reducing the time loss to 2-3 seconds.



SETUP DESCRIPTION:

Router 1, Router 2 and Router 3 are in OSPF area 0.
Multicast source is connected to Router 1.
Multicast Client is connected to Router 4.

Router 4 is in LAN. Link1 is configured as OSPF best path.
Router 2 is DR and Router 4 is BDR.

CONFIGURATION:

Router1

```
IPMS :
ip multicast status enable
! OSPF :
ip load ospf
ip ospf area 0.0.0.0
ip ospf area 1.1.1.1
ip ospf interface "vlan10"
ip ospf interface "vlan10" area 1.1.1.1
ip ospf interface "vlan10" status enable
ip ospf interface "vlan20"
ip ospf interface "vlan20" area 0.0.0.0
ip ospf interface "vlan20" status enable
ip ospf interface "vlan40"
ip ospf interface "vlan40" area 0.0.0.0
ip ospf interface "vlan40" cost 400
ip ospf interface "vlan40" status enable
ip ospf status enable
! IP multicast :
ip load pim
ip pim interface "vlan20"
ip pim interface "vlan10"
ip pim interface "vlan40"
ip pim cbsr 10.10.10.1
ip pim candidate-rp 10.10.10.1 225.1.1.1/32
ip pim sparse status enable
ip pim dense status disable
ipv6 pim sparse status disable
ipv6 pim dense status disable
```

Router2

```
IPMS :
ip multicast status enable
! OSPF :
ip load ospf
ip ospf area 0.0.0.0
ip ospf interface "vlan20"
ip ospf interface "vlan20" area 0.0.0.0
ip ospf interface "vlan20" status enable
ip ospf status enable
! IP multicast :
```

```
ip load pim
ip pim interface "vlan20"
ip pim interface "vlan30" bfd-std enable
ip pim sparse bfd-std status enable
ip pim sparse status enable
ip pim dense status disable
ipv6 pim sparse status disable
ipv6 pim dense status disable
```

Router3

```
IPMS :
ip multicast status enable
! OSPF :
ip load ospf
ip ospf area 0.0.0.0
ip ospf interface "vlan40"
ip ospf interface "vlan40" area 0.0.0.0
ip ospf interface "vlan40" cost 400
ip ospf interface "vlan40" status enable
ip ospf status enable
! IP multicast :
ip load pim
ip pim interface "vlan40"
ip pim interface "vlan30" bfd-std enable
ip pim sparse bfd-std status enable
ip pim sparse status enable
ip pim dense status disable
ipv6 pim sparse status disable
ipv6 pim dense status disable
```

Limitations:

When OSPF best path is given as the path where BDR resides, (i.e.) the path Link2-Link4 as mentioned in topology in section 4, the traffic will flow via Link2-Link4. When Router3 is reloaded the traffic shifts to Link1-Link3, and when Router3 comes up the traffic shifts to Link2-Link4 causing a time loss of 10 seconds. In the above scenario if Pim delay is configured as 30 seconds in Router3, the 10 seconds time loss is not getting reduced. When The BDR(Router3 as mentioned in topology in section 4) is reloaded consecutively, then multicast traffic gets stuck-up without getting forwarded for around 5-10 minutes

31. Cisco Protocol Hardware Tunneling

Introduction:

This feature Enhancement provides the facility to tunnel all the Cisco control frames through Hardware. This prevents all the cisco control protocol packets being sent to CPU, thus avoiding the packet drop due to rate limit. Earlier, The Cisco Control Protocols were always handled in software regardless of their configured action in the UNI profile. Since it is handled in software, the packets are rate limited to 512 pps. Hence cisco control packets are dropped and CPU spike is seen.

Platforms Supported:

OmniSwitch 6850, 6850E, 6855, 6855U24X, 6400, 9000E

Commands usage:

Ethernet-service uni <slot/port> uni-profile ieee-fwd-all
This command associates the uni port to a profile "IEEE-FWD-ALL" in which all the packets with mac 01:80:C2:00:00:XX will be forwarded.

Ethernet-service uni <slot/port> uni-profile ieee-drop-all
This command associates the uni port to a profile "IEEE-DROP-ALL" in which all the packets with mac 01:80:C2:00:00:XX will be dropped.

All other commands are same as in previous.

Limitations:

Sending the control packets with its own destination mac, when NoMac-tunnel feature is set via AlcatelDebug.cfg

Sending Traffic with 0180c2000002-0180c200000f with unknown ether type using IEEE-FWD-ALL as uni-profile

32. First Multicast Packet Forwarding

Introduction:

AOS multicast architecture is centralized and all forwarding decision are taken from a dedicated control plane module. Due to this architecture, initial multicast packets are lost in routing environment until the flow is learnt.

In railways oriented networks, multicast is used for signaling applications where first packet is at most important for transitioning to next available source.

This Feature helps in preventing the First Multicast packet loss in Routing environment. As soon as the initial Multicast packet received, software will hold the initial packets in the buffer untill the routing flow is learnt. User may see subsequent packets lost which normally happens in the initial processing of the New Multicast stream.

Platforms Supported:

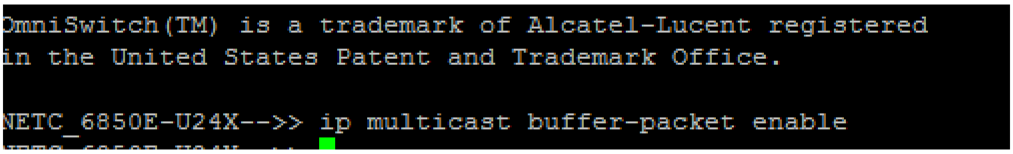
OmniSwitch 6850, 6850E, 6855, 6855U24X, 6400, 9000E

Commands usage:

ip multicast buffer-packet <enable/disable>

Syntax Definitions

Enable buffers the packet which is to avoid the first packet drop.



```
OmniSwitch(TM) is a trademark of Alcatel-Lucent registered
in the United States Patent and Trademark Office.

NETC_6850E-U24X-->> ip multicast buffer-packet enable
```

Limitations:

This Feature will guarantee that first packet is not being dropped and user may see subsequent packet lost which normally happens in the initial processing of the New Multicast stream. Means for any specific stream, packet number 1 and packets after flow has been learnt is forwarded. Packet numbers 2 till learning timer are expected to drop.

33. HTTPS HIC Re-direction

Introduction:
This feature Enhancement provides the facility of HIC redirection when the client browser specifies a HTTPS URL on port 443. When a device is put in a HIC state, any web session will be redirected to the HIC web agent via HTTPS URL specified in the client's browser. Earlier HIC redirection only works when the client browser specifies a HTTP URL on port 80.

Platforms Supported: OmniSwitch 6850, 6850E, 6855, 6855U24X, 6400, 9000E

Commands usage: The commands are same as in previous build.

Limitations:
HTTP/HTTPS redirection is not recommended when ip-address configured in hic allowed-name is entered in the URL of the client

34. IP Helper per VLAN per VRF

Introduction
This feature enhancement facilitates to configure VRF instance per VLAN mode. Earlier, this feature is limited for Standard mode only. The commands which are supported in the existing mode supports here also and the commands are introduced for the feature introduced.

Platforms Supported
OS9800E, OS6850E and OS6850

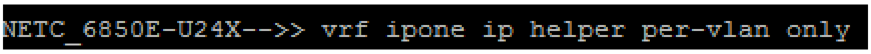
Commands usage

ip helper per-vlan only

Syntax Definitions
N/A

Usage Guidelines:
Using the per-vlan only forwarding option requires you to specify a DHCP server IP address for each VLAN that will provide a relay service. The ip helper address vlan command performs this function and at the same time enables relay for the specified VLAN.

Example

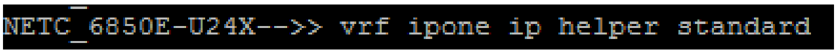


```
NETC_6850E-U24X-->> vrf ipone ip helper per-vlan only
```

ip helper standard

Syntax Definitions
N/A

Example



```
NETC_6850E-U24X-->> vrf ipone ip helper standard
```

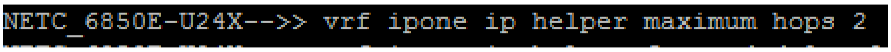
ip helper maximum hops <num>

Syntax Definitions
Hops The maximum number of relays (1-16)

Usage Guidelines:

If a packet contains a hop count equal to or greater than the hops value, DHCP Relay discards the packet.

Example



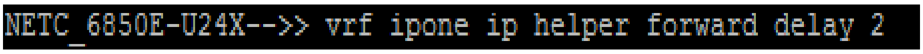
```
NETC_6850E-U24X-->> vrf ipone ip helper maximum hops 2
```

ip helper forward delay <seconds>

Syntax Definitions
Seconds Forward delay time value in seconds (1–65535). Do not use commas in the value.

Usage Guidelines:
If a packet contains an elapsed boot time value that is less than the specified forward delay time value, DHCP Relay discards the packet.

Example



```
NETC_6850E-U24X-->> vrf ipone ip helper forward delay 2
```

ip helper pxe-support {enable | disable}

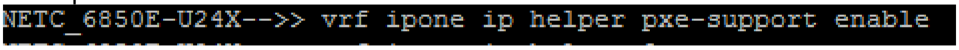
Syntax Definitions

Enable	Enables PXE support.
Disable	Disables PXE support.

Defaults

By default, PXE support is disabled for the switch.

Example



```
NETC_6850E-U24X-->> vrf ipone ip helper pxe-support enable
```

ip helper agent-information {enable | disable}

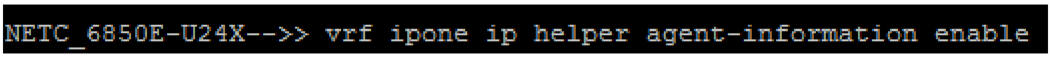
Syntax Definitions

Enable	Enables the relay agent Option-82 feature for the switch.
Disable	Disables the relay agent Option-82 feature for the switch.

Defaults

By default, this feature is disabled on the switch

Example



```
NETC_6850E-U24X-->> vrf ipone ip helper agent-information enable
```

ip helper agent-information policy {keep| replace | drop}

Syntax Definitions

Drop	Drop DHCP packets that already contain an Option-82 field.
Keep	Keep the existing Option-82 field information and continue to relay the DHCP packet.
Replace	Replace the existing Option-82 field information with local relay agent information and continue to relay the DHCP packet.

Defaults

By default, DHCP packets that already contain an Option-82 field are dropped

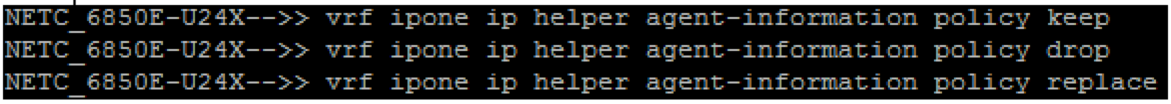
Usage Guidelines:

The policy configured with this command is only applied if the DHCP Option-82 feature is enabled for the switch.

The agent information policy is not applied if the DHCP relay agent receives a DHCP packet from a client that contains a non-zero value for the gateway IP address (giaddr). In this case, the agent will not insert the relay agent information option into the DHCP packet and will forward the packet to the DHCP server.

Note that if a DHCP packet contains a gateway IP address (giaddr) value that matches a local subnet and also contains the Option-82 field, the packet is dropped by the relay agent.

Example



```
NETC_6850E-U24X-->> vrf ipone ip helper agent-information policy keep
NETC_6850E-U24X-->> vrf ipone ip helper agent-information policy drop
NETC_6850E-U24X-->> vrf ipone ip helper agent-information policy replace
```

ip helper address <ip-address> {vlan <num>}

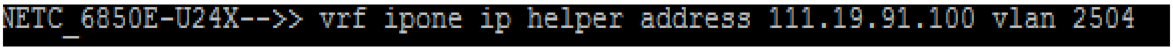
Syntax Definitions

ip_address	IP address (e.g. 21.0.0.10) of the DHCP server VLAN.
vlan_id	VLAN identification number (e.g. 3) of the DHCP server VLAN.

Defaults

If no VLAN identification number is entered, VLAN ID 0 is used by default.

Example



```
NETC_6850E-U24X-->> vrf ipone ip helper address 111.19.91.100 vlan 2504
```

Limitations:

When client and server are in different NI in case of non default VRF then resetting NI is not recommended

35. Stopping the Boot Sequence – Hit ‘s’

Introduction

In AOS 64X R01 products, boot sequence can be interrupted on entering any character. As part of this PER, boot sequence can be interrupted only on entering ‘s’ character. Entering any other characters will not allow stopping at uboot level rather the boot sequence continues.

Also as part of this change, there is a wait time is set for 2 seconds when user enters ‘s’. If any more characters entered during this wait time, then boot sequence continues without stopping at uboot. Thus, it is ensured that boot sequence can only be interrupted on entering character ‘s’ alone.

Platforms Supported

OS6400, OS6850E, OS6855, OS9E

Limitations:

For OS6400 products, mini-boot upgrade is not needed for the above change, only UBoot needs to be upgraded. On OS6400, upgrading mini-boot to the load after OS_644_407_R01 makes system unsteady state which is a known issue.

36. Multicast Table Optimization (*,G) Mode

Introduction:

This feature Enhancement prevents the exhaustion of multicast tables when numerous uPnP devices connects in a network and exchanges packets in group (239.255.255.250) and thereby ensures user multicast traffic to flow in the network. It is implemented by creating a single multicast entry for this group irrespective of the number of sources and provide space for other user multicast traffic when the star-g mode is enabled for this particular group in particular vlan. This feature can be extended to any multicast group in any vlan using the command explained in next section. We can configure maximum of 10 entries for vlan-group combinations in star-g mode.

Platforms Supported:
OS6855-U24X, OS6850E,OS6850, OS9000E. OS6450.

Commands usage:
There is new Command introduced for this feature. We can check the Multicast Performance for star-g-mode performance by using below commands

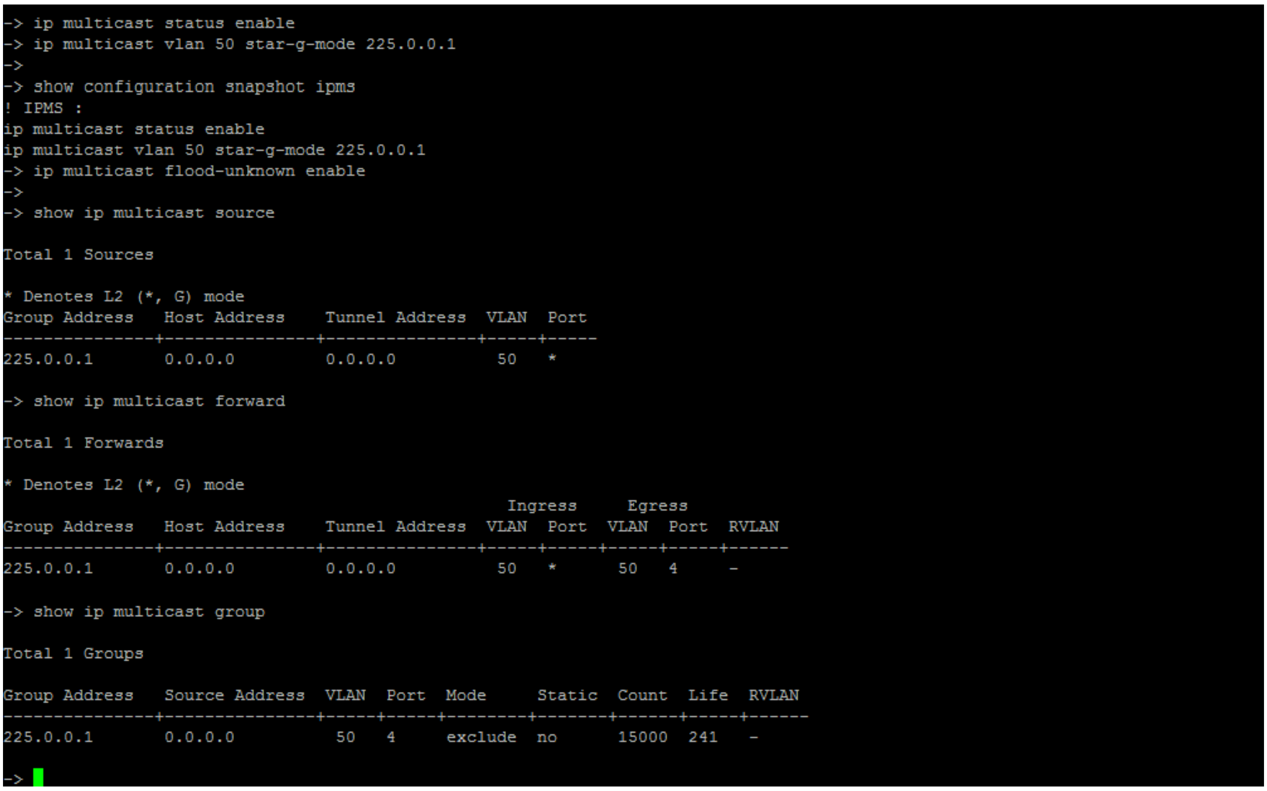
ip multicast vlan <vlan_id> start-g-mode <group_ip_address>

no ip multicast vlan <vlan_id> start-g-mode <group_ip_address>

Syntax Definitions

vlan_id the corresponding vlan for which star-g mode is needed.
group_ip_address the corresponding group for which star-g mode is needed.

Configuration snapshot:



```
-> ip multicast status enable
-> ip multicast vlan 50 star-g-mode 225.0.0.1
->
-> show configuration snapshot ipms
! IPMS :
ip multicast status enable
ip multicast vlan 50 star-g-mode 225.0.0.1
-> ip multicast flood-unknown enable
->
-> show ip multicast source

Total 1 Sources

* Denotes L2 (*, G) mode
Group Address   Host Address    Tunnel Address  VLAN  Port
---------------+---------------+---------------+-----+-----
225.0.0.1       0.0.0.0         0.0.0.0           50   *

-> show ip multicast forward

Total 1 Forwards

* Denotes L2 (*, G) mode
                                                  Ingress     Egress
Group Address   Host Address    Tunnel Address  VLAN  Port  VLAN  Port  RVLAN
---------------+---------------+---------------+-----+-----+-----+-----+------
225.0.0.1       0.0.0.0         0.0.0.0           50   *      50   4     -

-> show ip multicast group

Total 1 Groups

Group Address   Source Address  VLAN  Port  Mode      Static  Count  Life  RVLAN
---------------+---------------+-----+-----+---------+-------+------+-----+------
225.0.0.1       0.0.0.0           50   4     exclude  no      15000  241   -

->
```

Limitations:

Multicast Performance for Star-G-mode is limited to 10 groups.

37. OPTICAL PORT PHYSICAL BACKUP ON 6850, 6850E AND 6400

Introduction:
This enhancement enables configuration of a pair of ports in a physical layer as primary/backup mode. This means that only one port can be active at any point of time.
- When both ports are up, the backup port is put in a physical shutdown mode causing the upstream switch to see this port down.
- When the primary port goes down, the backup port is put back in a operational mode causing the upstream switch to see this port up
- When the primary port comes back up, it is expected that the primary port does NOT preempt the backup port. The backup port remains operational and the primary port is put in a shutdown mode.
- At any point only one port is attached to the hardware link aggregation table. Unless the port to which the transition is happening is down, the transient phase wherein none the ports are attached to the Link Aggregation will not trigger a Link Aggregation down event. The link aggregation will remain operational for the other AOS module. For instance, IPMS and IP are not affected by a port transition.
- When a static link aggregation is set in the PHY backup mode, STP is automatically disabled on the link aggregation

Platforms Supported:
OmniSwitch 6850/ OmniSwitch 6850E/ OmniSwitch 6400

Commands usage:

static linkagg <integer> size <integer> phy-backup enable

Example: static linkagg 1 size 2 phy-backup enable

The above command is used to signify that link aggregation is of a special"phy-backup" type and the ports configured in this OPPB link aggregate will operate in a physical layer primary/backup mode.

The "static linkagg" command is an existing command. It has various optional configuration parameters. To the set of optional configurable parameters, "phy-backup enable" is added.

When a link aggregation is defined to be of OPPB type, the size of the Link Aggregation has to be mandatorily 2. At any point, only one of the Link Aggregation port is operational and a "port join" for Link Aggregation is invoked on only this port. The other port is put to a SHUTDOWN state.

When this optional "phy-backup" type is not configured, the link aggregation behaves as a normal type. Meaning, all the ports defined on a Link Aggregation are operational. The "port join" is invoked for all ports. There is no specific restriction on the size of the link aggregate.

no static linkagg <integer>

The above command removes the link aggregation. This is an existing command. The same command holds good for removing a OPPB link aggregation.

static agg <slot/port> agg num <integer> phy-mode primary

Example: static agg 1/1 agg num 1 phy-mode primary

The above command configures the respective port as the PRIMARY port of the OPPB link aggregation.

The “static agg” is an existing command. To this command, the optional “phy-mode primary” is added which makes the port, the “PRIMARY” amongst the two ports of a special type link aggregate. The “phy-mode” can be configured only on a OPPB link aggregate.

Only one of the link aggregate ports has to be defined as “PRIMARY”. The other port automatically operates as the “BACKUP” port. If none of the ports are defined PRIMARY by CLI, the port with the lower port id operates as the primary port. This port is made PRIMARY by software and thereafter, the behavior of this port is synonymous to a port that was defined PRIMARY explicitly in CLI.

static agg no <slot/port>

The above is an existing command to remove a <slot/port> from a link aggregate. The same command holds good to remove a <slot/port> from an OPPB link aggregate.

When a port is removed from a Link Aggregation whose PRIMARY port was assigned by software, the primary port assignment is undone. The port that next joins this link aggregate is free to be defined as the PRIMARY port by CLI.

interfaces 1/5 clear-violation-all

The above is an existing command to clear all port violations set by various applications on the switch for the given port.

The “PRIMARY” port of an OPPB LinkAgg which has currently been put to a shutdown state can be put back to operational state by clearing all the violations on this port. The BACKUP port would now be moved from operational to a shutdown state.

Clearing the violations on the “BACKUP” port, does not make the backup port operational.

show linkagg

“show linkagg” is an existing command to display the link aggregations defined on the switch. This command output also displays the special type link aggregation.

Example:

```
> show linkagg
*  PHY-BACKUP enabled special type link aggregation

                                         Min
Number  Aggregate  SNMP Id   Size Size Admin State  Oper State     Att/Sel Ports
-------+----------+---------+----+----+------------+--------------+-------------
   1     Static*    40000001   2    1   ENABLED      UP          1   2
   2     Static      40000002   4    1   ENABLED      UP          2   2
   3     Static*    40000003   2    1   ENABLED      UP          1   2
```

Here, Linkagg 2 is a regular Link Aggregation, whereas linkagg 1 and 3 are OPPB Link Aggregation.

show linkagg port

“show linkagg port” is an existing command to display the ports of a link aggregate. The output of the same displays the ports of a special type link aggregation.

Example:

```
> show linkagg port
* Ports of a PHY-BACKUP enabled special type link aggregation
** Backup port of a PHY-BACKUP enabled special type link aggregation

Slot/Port Aggregate SNMP Id   Status   Agg  Oper Link Prim Standby
---------+---------+-------+----------+----+----+----+----+-------
   3/1    Static*     3001  ATTACHED           1  UP          UP         YES  NO
   3/2    Static*     3002  RESERVED-BKP     1  DOWN** DOWN   NO    NO
   3/3    Static       3003  ATTACHED           2  UP          UP         YES  NO
   3/4    Static       3004  ATTACHED           2  UP          UP         NO    NO
   3/5    Static       3005  ATTACHED           2  UP          UP         NO    NO
   3/6    Static       3006  ATTACHED           2  UP          UP         NO    NO
   3/7    Static*     3007  ATTACHED           3  UP**        UP         YES  NO
   3/8    Static*     3008  SELECTED             3  DOWN     DOWN   NO    NO
```

Ports 3/3-6 belong to a regular type Link Aggregation. All 4 ports of this Linkagg are UP and a “PORT JOIN” would be invoked for all the ports.

Ports 3/1 and 3/2 belong to an OPPB Link Aggregation. 3/1 is the PRIMARY port and is operational. 3/2 is the BACKUP port is put to a shutdown state.

3/7 and 3/8 are ports of another OPPB Link Aggregate. The port 3/7 is operational and is the PRIMARY port of linkagg 3. Port 3/8 is link down. This is illustrated by the port status being “SELECTED”. If the port 3/8 is later detected up, it would be put to a shutdown state and moved to port status “RESERVED-BKP”.

“RESERVED-BKP” is a new port status that is defined for this feature.

“**” indicates the configured BACKUP port. Note that 3/2 is a port configured BACKUP by CLI and is in a shutdown state. Port 3/7 is a port configured BACKUP by CLI, and is currently assuming the role of a PRIMARY port and is operational.

show interfaces <slot/port> port

This is an existing command to display the administrative status, link status, violations, recovery time, maximum recovery attempts and the value of the wait-to-restore timer for the specified port.

The link status for the backup port of OBBP would be down and the violation would be rightly described as applied by Link Aggregation application module.

Example:

```
> show interfaces 1/11 port
Legends: WTR - Wait To Restore
         #   - WTR Timer is Running & Port is in wait-to-restore state
         *   - Permanent Shutdown

Slot/    Admin     Link    Violations  Recovery   Recovery     WTR           Alias
Port     Status   Status                 Time       Max        (sec)
```

```
------+----------+---------+----------+----------+----------+----------+-----------------------------------------
* 1/11   enable     down     LinkAgg       300        10         0 ""
```

“show interfaces port” displays the above port interface details for all the ports in switch. The corresponding entry for backup port of OPPB would have the link down and violation by LinkAgg.

LIMITATIONS:
Hardware Limitations:
When the link aggregation ports come up after a switch reload, the backup port also comes up physically. This “link up” is detected and soon put to a physical shutdown state by the software. The “backup” port would be momentarily up till the phy backup configuration is honored by software.

Software Limitations:
The proposed solution only supports a pair of ports.

The convergence from primary to backup port will expose some packet loss. The convergence will be in a best effort basis and should be in mist of case less than 1 second. Also, the convergence is dependent on how fast a port down event is detected. For fiber interfaces, this is not an issue, but for copper interface, it can take up to 700ms.

No MAC Flush. The proposed solution does not support a mechanism to periodically “advertise” all the MAC addresses learned on the L2 CPE through a dummy multicast packet.

Usage Limitations:
By default, the interface in a shutdown mode is automatically recovered every 300 seconds for a maximum of 10 times. After this, the interface is put in a permanent shutdown state. For this feature, the recovery mechanism should be disabled on both ports of OPPB Link Aggregation:

```
> interfaces <slot/port> violation-recovery-time 0
> interfaces <slot/port> violation-recovery-maximum 0
```

38. Bring Your Own Device (BYOD)

Introduction:

The Alcatel-Lucent OmniSwitch implementation of BYOD leverages the Aruba ClearPass Policy Manager (CPPM) and Access Guardian features on the OmniSwitch. It allows guest access or onboarding of both wired or wireless devices such as employee, guest, employee owned or silent devices through an OmniSwitch edge device with ClearPass as a RADIUS server or RADIUS proxy. This feature supports the following functionalities:

- Unified access policy management solution for Wire line and Wireless networks using CPPM
- Integration with Access Guardian UNPs and 802.1x authentication
- Restricts access to the network and validation for end user devices including employees with IT supplied devices, IP phones, employees personal devices, guest devices, access points, cameras, and silent devices such as printers.
- CPPM can act as a RADIUS server for new deployments or RADIUS proxy for existing networks. Self-service/self-registration by Employees when they connect to the Enterprise network using their personal device through CPPM.
- Captive portal hosted on CPPM for this feature.

- Device Profiling and Posture Check. Registration and tracking of devices associated with Employees and approved for usage.
- Redirection and restricted access for non-compliant devices.
- Zero-touch Auto-configuration of employee personal devices based on pre-defined role-based Configuration profiles.
- Differentiated access & user experience policies based on Corporate or Employee Personal device, Applications and Role.
- Integration with RADIUS Server and CPPM for Authentication, Authorization and Accounting.
- Automatic provisioning of Applications such as NAC Agent, MDM Client as part of the device enrollment process on Employee Personal Devices.
- Automatic provisioning of Device Certificates that are dynamically requested, issued and installed on the Employee Personal Device with association to Employee corporate Credentials
- Provides notification of BYOD policy violations, usage statistics, time and cost information to the end-user in real-time.
- RADIUS Change of Authorization (CoA)
- A mechanism to change AAA attributes of a session after authentication
- New Profile sent as an attribute in the message
- Disconnect Message to terminate user session and discard all user context
- Port bounce capability can be configured on the OmniSwitch to ensure a clean re-authentication process for non-supplicant devices.
- URL redirect and port location information

In addition to BYOD section in OmniSwitch user guides additional configuration examples can be viewed on the Alcatel-Lucent Enterprise Demo channel:
http://www.youtube.com/playlist?list=PLrzAZN530GJ8kfUJCNsjIhJW6cAV5AACb

Platforms Supported:
OmniSwitch 6850E
OmniSwitch 9800E
Commands usage:

aaaredirect-server <name>ip-address <ip_address>url-list <redirect_url_name>

Usage:
The above command which is for BYOD feature which has redirection server name and its details.

aaa redirect <name> url <url>

Usage:
This command is used to represent the different kind of URL names which is applied on the UNP in which the actual re-direction happens.
We can have maximum of 5 redirect URLs as strings.

aaa port-bounce <enable/disable>

Usage:
When port is globally enabled then port bouncing is enabled in all slot/port
By default the global status of port bouncing is enabled.

aaa port-bounce <slot/port>|<slot>|<slot/port1-portn ><enable/disable>

Usage:
This is command is used to re-authenticate non-supplicant client to get new ip address and get full access of the network.

The port bouncing configuration for slot/port will be enabled once global port bounce is enabled. We can also enable/disable per port basis.

aaa redirect pause timer <seconds>

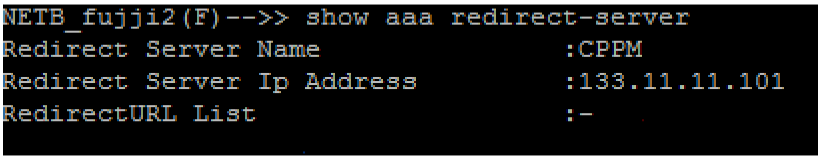
Usage:
This is command is used to configure the pause timer value. The pause timer values should be multiples of 5.
The redirect pause timer value is a global timer which takes 30 as default value. It should be multiples of 5.

aaa user-network-profile name <string> vlan <num> hic <enable|disable> | redirect <urlname>

Usage:
This is command is used to give the vlan/redirect url for the access of network through the re-direct url.

show aaa redirect-server

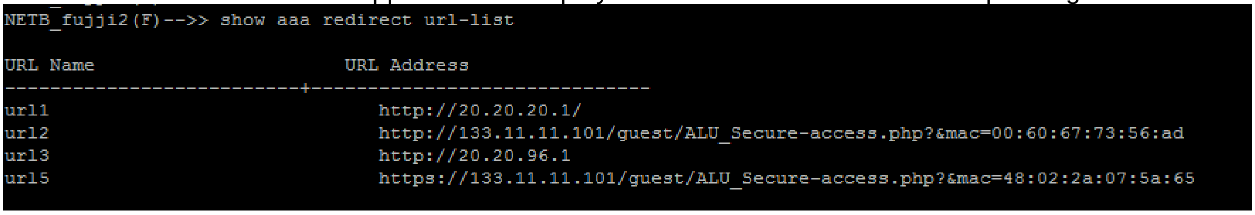
Usage:
The above command which is for BYOD feature which has redirection server name and its details.



```
NETB_fujji2(F)-->> show aaa redirect-server
Redirect Server Name                :CPPM
Redirect Server Ip Address          :133.11.11.101
RedirectURL List                    :-
```

show aaa redirect url-list

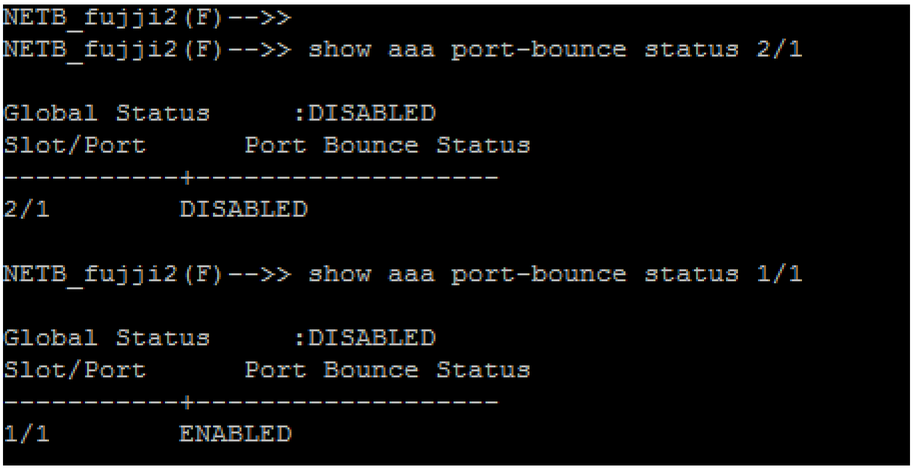
Usage:
This command is used to represent the different kind of URL names which is applied on the UNP in which the actual re-direction happens. It will display 5 redirect names with its corresponding url.



```
NETB_fujji2(F)-->> show aaa redirect url-list

URL Name                          URL Address
--------------------------+------------------------------
url1                                 http://20.20.20.1/
url2                                 http://133.11.11.101/guest/ALU_Secure-access.php?&mac=00:60:67:73:56:ad
url3                                 http://20.20.96.1
url5                                 https://133.11.11.101/guest/ALU_Secure-access.php?&mac=48:02:2a:07:5a:65
```

show aaa port-bounce status |<slot/port>

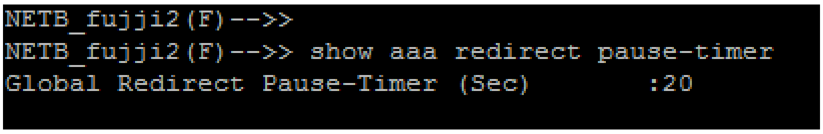
Usage:
This show command is used to display the status of global and slot/port port bounce configuration.



```
NETB_fujji2(F)-->>
NETB_fujji2(F)-->> show aaa port-bounce status 2/1

Global Status      :DISABLED
Slot/Port       Port Bounce Status
-----------+-------------------
2/1         DISABLED

NETB_fujji2(F)-->> show aaa port-bounce status 1/1

Global Status      :DISABLED
Slot/Port       Port Bounce Status
-----------+-------------------
1/1         ENABLED
```

show aaa redirect pause-timer

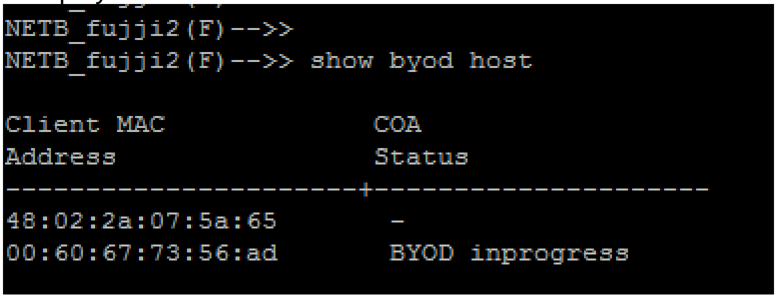
Usage:
This show command is used to display global pause-timer value in the range of 0-65535 seconds which should be multiples of 5.



```
NETB_fujji2(F)-->>
NETB_fujji2(F)-->> show aaa redirect pause-timer
Global Redirect Pause-Timer (Sec)        :20
```

show byod host

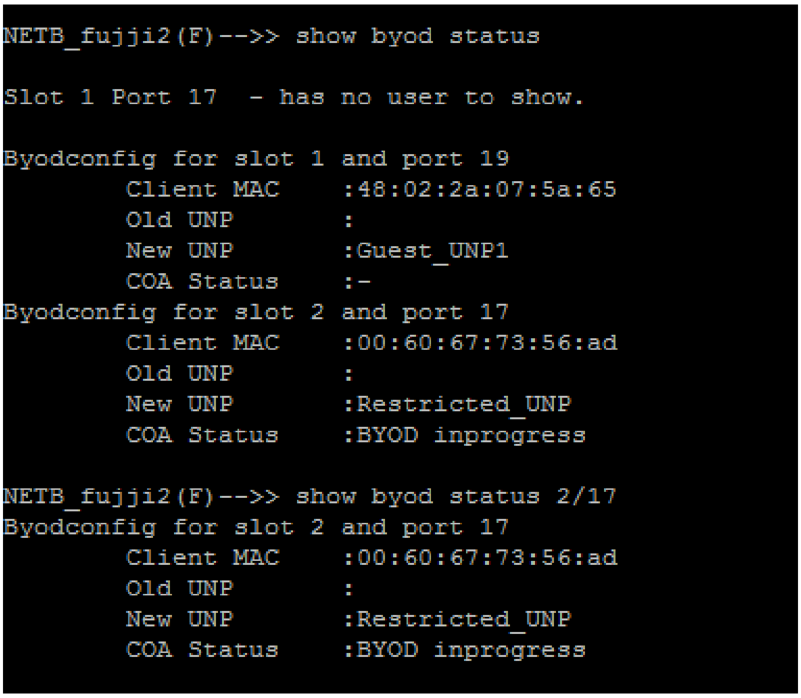
Usage:
It displays the status of the new client who comes to the network.



```
NETB_fujji2(F)-->>
NETB_fujji2(F)-->> show byod host

Client MAC              COA
Address                 Status
----------------------+----------------------
48:02:2a:07:5a:65         -
00:60:67:73:56:ad         BYOD inprogress
```

show byod status | <slot/port>

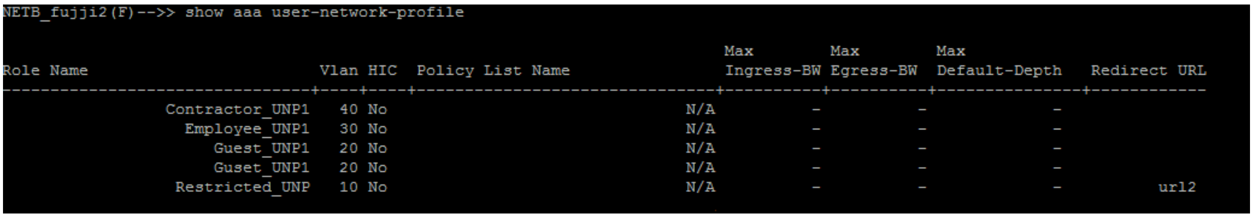
Usage:
It displays the status of the new client comes to the network.



```
NETB_fujji2(F)-->> show byod status

Slot 1 Port 17  - has no user to show.

Byodconfig for slot 1 and port 19
        Client MAC    :48:02:2a:07:5a:65
        Old UNP       :
        New UNP       :Guest_UNP1
        COA Status    :-
Byodconfig for slot 2 and port 17
        Client MAC    :00:60:67:73:56:ad
        Old UNP       :
        New UNP       :Restricted_UNP
        COA Status    :BYOD inprogress

NETB_fujji2(F)-->> show byod status 2/17
Byodconfig for slot 2 and port 17
        Client MAC    :00:60:67:73:56:ad
        Old UNP       :
        New UNP       :Restricted_UNP
        COA Status    :BYOD inprogress
```

show aaa user-network-profile

Usage:
This command is modified to display the Url-Name which has the url page associated with it.



```
NETB_fujji2(F)-->> show aaa user-network-profile

                                                                           Max        Max        Max
Role Name                        Vlan HIC  Policy List Name                Ingress-BW Egress-BW  Default-Depth   Redirect URL
--------------------------------+----+----+-------------------------------+----------+----------+---------------+------------
                 Contractor_UNP1   40 No                               N/A          -          -             -
                   Employee_UNP1   30 No                               N/A          -          -             -
                      Guest_UNP1   20 No                               N/A          -          -             -
                      Guset_UNP1   20 No                               N/A          -          -             -
                  Restricted_UNP   10 No                               N/A          -          -             -          url2
```

Note
As this feature was ported from AOS 6.4.6.R01 for OS6850E, please refer to the AOS 6.4.6.R01 User Guides for more information.

39. mDNS_Relay

Introduction:

MDNS is a zero configuration host name resolution service used to discover services on a LAN. MDNS allows resolving host names to IP addresses within small networks without the need of a conventional DNS server. The mDNS protocol uses IP multicast User Datagram Protocol (UDP) packets and is implemented by Apple Bonjour, Avahi (LGPL), and Linux NSS-MDNS. To resolve a host name, the mDNS client broadcasts a query message asking the host having that name to identify itself. The target machine then multicasts a message that includes its IP address. All machines in that subnet will use that information to update their mDNS caches.

As an example Apple's Bonjour architecture implements the following three fundamental operations to support zero configuration networking service:
- Publication (Advertising a service)
- Discovery (Browsing for available services)
- Resolution (Translating service instance names to address and port numbers for use)

The Aruba AirGroup feature provides optimization that limits the unnecessary flooding of Bonjour traffic to improve Wifi performance and also allow the Bonjour services to extend across VLANs. The OmniSwitch enhancement supports an mDNS relay function by configuring a GRE tunnel interface between the WLAN controller and the OmniSwitch. The OmniSwitch can intercept and relay the mDNS frames from the wired devices advertising a service using Bonjour messages to the WLAN controller thus preventing flooding of the mDNS frames.

Note: mDNS relay is only supported for wireless clients. Wired clients are not supported.

Platforms Supported:

OmniSwitch 6850E/ OmniSwitch 9800E/ OmniSwitch 6855/ OmniSwitch 6400/ OmniSwitch 6850

Commands usage:

mdns-relay {enable/disable}

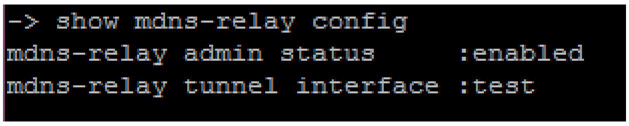
Usage:
This command is used to enable/disable the Multicast DNS relay feature.

mdns-relay tunnel {IP interface Name}
no mdns-relay tunnel {IP interface Name}

Usage:
- This command is used to associate a GRE tunneling interface for the Multicast DNS relay feature.
- Using no option with this command, GRE interface is disassociated from the Multicast DNS relay feature.

show mdns-relay config

Usage:
- This command shows the Multicast DNS relay configuration



```
-> show mdns-relay config
mdns-relay admin status      :enabled
mdns-relay tunnel interface :test
```

Limitations:
None.

40 . Multicast dynamic control (MDC)

Platforms: OS 6850E, OS 6855-U24X, OS 6855, OS 97E, OS 6850, OS 6400

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.

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

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.

Usage

To enable/disable global multicast dynamic-control status
ip multicast dynamic-control status [{enable|disable}]

Guidelines: By default this status is disabled. If it is enabled, IPv4 multicast well-known protocol packets alone will be trapped to CPU and the other multicast packets will be dropped. Well-known IPv4 protocols are given below in Note section

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.

Note:

- Drop-all status can be enabled only after enabling global dynamic control status.
- Below are the well-known IPv4 multicast protocol packets,

OSPF:	224.0.0.5/32 + IP protocol 89
OSPF:	224.0.0.6/32 + IP protocol 89
VRRP:	224.0.0.18/32 + IP protocol 112
RIPv2:	224.0.0.9 + UDP port 520
PIM:	224.0.0.13/32
DVMRP:	224.0.0.4/32

Examples

```
ip multicast dynamic-control status enable
ip multicast dynamic-control status disable

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 status enable
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.

New SNMP Traps:

No.	Trap Name	Platforms	Description
183	alaDhcpBindingDuplicateEntry		
184	esmStormThresholdViolationStatus		
191	chassisTrapsLowFlashSpace		