Omni Switch 6250/ 6450

Release 6.6.5.134.R02

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 Lucent Enterprise Technical Support Department.

Problems Fixed Between Builds 64 and 77

PR	**204200**	Build:	6.6.5.69.R02
Summary:	OS6450 switch crashed with open flow configuration.		
Explanation:	Hardware buffer is handled properly		

PR	**204101**	Build:	6.6.5.72.R02
Summary:	OS6250 Power supply type display issue		
Explanation:	Fix done to show proper power supply status for OS6250 switches.		

PR	**204505**	Build:	6.6.5.72.R02
Summary:	DHCP Offer packet dropped Between Ni to CMM		
Explanation:	Clear the congestion bit in udprelay Ni socket when its disconnected from CMM		

Problems Fixed Between Builds 78 and 101

PR	**204755**	Build:	6.6.5.78.R02
Summary:	Impact analysis on your products with CVE-2015-0291 t1_lib.c in OpenSSL 1.0.2.		
Explanation:	OpenSSL Vulnerability - CVE-2015-0287,CVE-2015-0289,CVE-2015-0292,CVE-2015-0209,CVE-2015-0288		

PR	**204982**	Build:	6.6.5.78.R02
Summary:	Comments in 'show configuration snapshot' are misinterpreted as history commands.		
Explanation:	Fix to display the cli command from history properly.		

PR	**202977**	Build:	6.6.5.78.R02
Summary:	Switch unable to send out traps.		
Explanation:	Fix done to send traps out of the switch when the switch was reloaded with no aaa authentication and later configured with aaa authentication.		

PR	**205907**	Build:	6.6.5.80.R02
Summary:	OS6450: BYOD ip addresses does not show in configuration		
Explanation:	CLI, SNMP and Webview support to display BYOD_WHITELIST ip address		

PR	**204353**	Build:	6.6.5.80.R02
Summary:	OS6450-P24 High CPU and show commands are not working		
Explanation:	Fix high CPU by closing aged out QOS FDs		

PR	**205150**	Build:	6.6.5.80.R02
Summary:	Alcatel-Lucent OmniSwitch 6450 Web Interface Weak Session ID CVE-2015-2804.		
Explanation:	Vulnerability has been fixed		

PR	**201474**	Build:	6.6.5.82.R02
Summary:	Qos profile (up=4 dscp=36) not created error message is been displayed in swlogs continuously.		
Explanation:	Prevent deletion of the QOS object which is in use		

PR	**206348**	Build:	6.6.5.82.R02
Summary:	OS6450 - When validated the open flow rules to be registered / inserted properly, found irregular rules		
Explanation:	Fix Done to correct the packet length for empty instruction set		

PR	**205395**	Build:	6.6.5.83.R02
Summary:	clarification for logs on OS6450 priority disconnect function		
Explanation:	Log message on port OFF/ON due to priority-disconnect		

PR	**206577**	Build:	6.6.5.84.R02
Summary:	OS6450 TCAM resource error		
Explanation:	Qos Rules Validated Properly Per Asic		

PR	**206763**	Build:	6.6.5.84.R02
Summary:	Randomly ARP entry for permanent gateway is not resolved		
Explanation:	Vrf-id is corrected while updating PBR data in the QosNI		

PR	**207125**	Build:	6.6.5.86.R02
Summary:	DSCP / 802.1P marking is not working when mixed with permanent gateway in the same policy action		
Explanation:	Changes done to update PBR data without overwriting hardware Action		

PR	**179918**	Build:	6.6.5.88.R02
Summary:	Switch crashed with tCsCSMtask2,tCS_CCM,tCS_PRB tasks suspended		
Explanation:	Defensive check added to avoid null pointer access		

PR	**207403**	Build:	6.6.5.89.R02
Summary:	A non-supplicant stays in auth-server-down UNP even after RADIUS server is reachable again		
Explanation:	In AuthServerDown scenario, Re-authentication will be allowed for IP Phones if voice policy UNP is not configured.		

PR	**207643**	Build:	6.6.5.90.R02
Summary:	Command required in 6450: debug source-learning forced aging cycle time threshold		
Explanation:	Introduced "debug source-learning forced aging cycle time <HH:MM> threshold <num>" to flush mac-address-table		

PR	**206591**	Build:	6.6.5.90.R02
Summary:	With reference to PR# 206348, Open Flow: Port - Hw Addr: It shows all zero 00:00:00:00:00:00		
Explanation:	code changes done to update Port Mac-address from ESM driver		

PR	**207310**	Build:	6.6.5.91.R02
Summary:	OS6450 switch polling with RADIUS Access request every 50sec.		
Explanation:	CLI to disable/enable radius server reachability feature		

PR	**205267**	Build:	6.6.5.91.R02
Summary:	Need swlog appid for NTP for OS6450.		
Explanation:	Suppressed ntp warning messages to debug		

PR	**204070**	Build:	6.6.5.92.R02
Summary:	Fan status not changing even when the physical fan is stopped working.		
Explanation:	Changed the default fan speed in order to let hardware update on proper fan status		

PR	**207171**	Build:	6.6.5.93.R02
Summary:	QoS policies are not applied after "qos port reset"		
Explanation:	Changes to Handle Qos Flag while updating the Port group properly is done		

PR	**205148**	Build:	6.6.5.93.R02
Summary:	Alcatel-Lucent OmniSwitch 6450 Web Interface Cross-Site Request Forgery, CVE- 2015-2805.		
Explanation:	Vulnerability has been fixed		

PR	**207193**	Build:	6.6.5.96.R02
Summary:	Request for log/ traps while manual admin down/up of an interface is done in INFO (default)		
Explanation:	Code changes done to update the admin up/admin down message in the swlog.		

PR	**205491**	Build:	6.6.5.96.R02
Summary:	Fan status not changing even when the physical fan is stopped working.		
Explanation:	Changed the default fan speed for 6450-U24 in order to let hardware update on proper fan status		

Problems Fixed Between Builds 102 and 134

PR	**202167**	Build:	6.6.5.102.R02
Summary:	Switch is sending eap failure message before starting the authentication process.		
Explanation:	Added the global variable authServEapFail to control the EAPOL fail packet.		

PR	**206963**	Build:	6.6.5.103.R02
Summary:	OS6450 Ni 2 rebooted after issue with its linkagg port		
Explanation:	Code changes done to fix memory leak in sspNi task.		

PR	**209378**	Build:	6.6.5.103.R02
Summary:	"NTP warning clock_select: no clock survivors" warning message is seen swlog		
Explanation:	"peer_clear and new_peer " warning messages can be seen via debugs		

PR	**208074**	Build:	6.6.5.103.R02
Summary:	Problem with IP phones of certain model with AOS6250.		
Explanation:	Introduced the cli "qos user-port link-shutdown bpdu" to administratively disable the port		

PR	**208840**	Build:	6.6.5.103.R02
Summary:	3XOS6450-P48 stack crash and memory issue.		
Explanation:	Code changes done to fix memory leak in sspNi task.		

PR	**209047**	Build:	6.6.5.103.R02
Summary:	aaa redirect server not working and switch is not classifying the packet as BYOD		
Explanation:	Programming the MAC Address in hardware correctly when UNP and default vlan of the port are same		

PR	**208595**	Build:	6.6.5.103.R02
Summary:	SNMP result incorrect for OS6400 fan status		
Explanation:	Correct FAN details updated via SNMP		

PR	**207820**	Build:	6.6.5.105.R02
Summary:	OS6450: output:3 is missing in the statistics.		
Explanation:	Changes done to properly validate the length for the outports		

PR	**209640**	Build:	6.6.5.105.R02
Summary:	static dhcp binding entry over written to dynamic entry when client receives an ip dynamically on that port		
Explanation:	If the client can successfully acquire an IP address, and when the DHCP snooping enabled device writes a binding entry, if a static entry for the same client is already present, do not replace the static entry with the dynamic entry.		

PR	**208513**	Build:	6.6.5.105.R02
Summary:	The 1GB port stops working after installing 10G license on 6450		
Explanation:	Code changes done to detect copper SFPs properly.		

PR	**209468**	Build:	6.6.5.105.R02
Summary:	NTP Warning message seen in logs on 6.6.5.101.R02		
Explanation:	NTP "peer_clear and new_peer " warning messages can be seen via debugs.		

PR	**209618**	Build:	6.6.5.106.R02
Summary:	OS6450: sendL2StatisticsToHealthMon, zcBufCreate fail		
Explanation:	Code changes done to enable logging to ipcTech log file by default.		

PR	**209412**	Build:	6.6.5.106.R02
Summary:	OS6450: Issue with RIP when Primary switch is power OFF in the stack		
Explanation:	Properly update route flags in IPNI		

PR	**210239**	Build:	6.6.5.107.R02
Summary:	Bogus DHCP packet to customer dhcp server.		
Explanation:	Only the ACK received for the DHCP address of the switch is used to change the "dhcpInfoFromServer.serverIp".		

PR	**209348**	Build:	6.6.5.112.R02
Summary:	OS6450 Qos not working		
Explanation:	Flush the L4 Port Comparator Database on qos apply		

PR	**210612**	Build:	6.6.5.116.R02
Summary:	OS6450: show vlan members port 1/1/47 is blocking but spanning Tree showing forwarding		
Explanation:	Poll complete Spanning Tree Database for proper VPA status		

PR	**210059**	Build:	6.6.5.116.R02
Summary:	Linkagg went down while performing write-memory flash synch		
Explanation:	Code changes done to prevent linkagg flap while doing write-memory flash synchro.		

PR	**210651**	Build:	6.6.5.116.R02
Summary:	When port security is enabled on OS6450 switch, vlan mobile-tag is not working as expected.		
Explanation:	Add VLAN classification for user with Port-MAC classification		

PR	**209491**	Build:	6.6.5.118.R02
Summary:	VSTK VLAN MAC addresses are learnt though source-learning is disabled in 6450		
Explanation:	Ensured source learning status is being set properly for vlans during bootup.		

PR	**200402**	Build:	6.6.5.120.R02
Summary:	On OS6450 stack getting error: hal_qos_read_block_counter:89: operation on non-initialized application:-113		
Explanation:	Program Qos entries correctly in appropriate hardware tables		

PR	**211115**	Build:	6.6.5.120.R02
Summary:	6450 are looping a DHCP offer frame from one port to the second of a static linkagg		
Explanation:	DHCP offer packet should not be flooded back, if client port and port received belongs to same Agg.		

PR	**208258**	Build:	6.6.5.121.R02
Summary:	Mac address is hopping from port to port without the device is physically changed		
Explanation:	Avoid MAC Move issue when both SFLOW and port mobility configurations are present.		

PR	**209469**	Build:	6.6.5.126.R02
Summary:	OS6450: info messages memPartAlloc		
Explanation:	Handling DHCP packets with no end options on trust ports		

PR	**211193**	Build:	6.6.5.126.R02
Summary:	ip multicast vlan XX status disable not working properly		
Explanation:	Hardware status not updated for per vlan, when global status is disabled or when vlan is destroyed.		

PR	**211400**	Build:	6.6.5.126.R02
Summary:	DHL name is getting removed after switch bootup.		
Explanation:	Store DHL name correctly in boot configuration		

PR	**211360**	Build:	6.6.5.127.R02
Summary:	Mcast pkts not getting dropped when the client entry is not present in the dhcp binding table with ISF enabled		
Explanation:	1. Control packets (ex: multicast report packets) are trapped to CPU in a VLAN where multicast and ISF is enabled. Control packet which does not have the appropriate binding entry are also trapped and the switch ends up learning the client using this packet. 2. Control packets were being logged as DROP irrespective of whether the client has a ISF binding entry or not. 3 NI ISF DB was not deleting binding entries ever. This will lead to wrong results.		

PR	**211275**	Build:	6.6.5.127.R02
Summary:	Multicast packet dropped as per qos logs when ip source filtering is enabled		
Explanation:	1. Control packets (ex: multicast report packets) are trapped to CPU in a VLAN where multicast and ISF is enabled. Control packet which does not have the appropriate binding entry are also trapped and the switch ends up learning the client using this packet. 2. Control packets were being logged as DROP irrespective of whether the client has a ISF binding entry or not. 3 NI ISF DB was not deleting binding entries ever. This will lead to wrong results.		

PR	**211269**	Build:	6.6.5.128.R02
Summary:	Flood rate config missing in the show configuration snapshot and in boot.cfg		
Explanation:	Mip overflow is handled for interface flood rate configuration		

PR	**207203**	Build:	6.6.5.131.R02
Summary:	"DHCP Snooping message: FFP Resource exhaustion" logged in SWLOG		
Explanation:	Counter that is incrementing for vlan, port ISF configuration and trust port dhcp-snooping configuration is removed		

PR	**210326**	Build:	6.6.5.131.R02
Summary:	Vlan port association not configured properly in the hardware		
Explanation:	Default VPA not deleted when port mobility rule is deleted		

PR	**210944**	Build:	6.6.5.134.R02
Summary:	While configuring the fifth port group, error is thrown		
Explanation:	The number of supported port groups was reduced from 8 to 5. This is now corrected and 8 port groups are supported.		

Under Verification:

PR	**202480**	Build:	6.6.5.75.R02
Summary:	Need to bypass the authentication for a server when user is in restricted role		
Explanation:	Implementation of Byod White-list Ip-address		

PR	**198851**	Build:	6.6.5.77.R02
Summary:	Unable to configure dhcp snooping source filter on mobile port		
Explanation:	Allowed to configure the ISF on mobile port when the port is not in forward state.		

PR	**203975**	Build:	6.6.5.78.R02
Summary:	Need clarification on power utilization and PoE (lanpower) info Switch OS6450 P10 & OS6450-P10L		
Explanation:	Updated power supply to 150W and PoE max power to 120W for 6450-P10L		

PR	**204081**	Build:	6.6.5.78.R02
Summary:	2xOS6450-P48 Stack Crash with task		
Explanation:	Increased the debug level in hal-traces to avoid the memory corruption		

PR	**204237**	Build:	6.6.5.78.R02
Summary:	Unable to display serial number of external Power supply in stack from OV2500 inventory page.		
Explanation:	Display serial number of Back up Power supply in secondary and idle units		

PR	**203897**	Build:	6.6.5.81.R02
Summary:	6450 - QOS not dropping MultiCast streams while Active Policy Rule is matched		
Explanation:	Multicast policy rule with destination port can be configured in Default List		

PR	**205215**	Build:	6.6.5.88.R02
Summary:	6450 lanpower fails to start after power outage		
Explanation:	Retry lanpower controller initialization on failure		

PR	**207160**	Build:	6.6.5.88.R02
Summary:	Not all rules configured in hardware		
Explanation:	Fix Done to accommodate 926 Qos Rules		

PR	**206885**	Build:	6.6.5.88.R02
Summary:	Primary and secondary unit on OS6450-P48 stack loses configuration after outage.		
Explanation:	Code changes done to prevent 802.1x config loss during consecutive takeover.		

PR	**203349**	Build:	6.6.5.88.R02
Summary:	OS6450 getting crashed while processing the ARP packets sent by the SDN controller and in the crash		
Explanation:	Proper software buffer allocation done for openflow software actions		

PR	**207341**	Build:	6.6.5.90.R02
Summary:	OS6250-24 stack of 4 units / Unit 1 crashed, with tCsCSMtask2 & EsmDrv task Suspended		
Explanation:	Code changes done to prevent memory corruption by hal_trace.		

PR	**205509**	Build:	6.6.5.93.R02
Summary:	6450: Number of clients supported when VLAN IP Source Filtering is enabled. Ref_PR#205340		
Explanation:	Display binding entry when Ip source filter is enabled on VLAN level		

PR	**207087**	Build:	6.6.5.93.R02
Summary:	OS6450 sending DHCP inform packet with destination IP as 0.0.0.0, which is triggered as Dos in OS690		
Explanation:	Set destination ip of DHCP inform packet as broadcast incase server ip not updated		

PR	**206892**	Build:	6.6.5.93.R02
Summary:	lanpower issue seen on a stack of 2 OS6450-P48.		
Explanation:	Prevent auto lanpower restart on takeover when capacitor-detection enabled		

PR	**211363**	Build:	6.6.5.128.R02
Summary:	Using auth-server-down UNP feature, when an authentication server is unreachable, the supplicants are facing issues with connectivity every 15-20 secs even after getting the mobile ports in the VLAN mentioned in the auth-server down UNP policy		
Explanation:	802.1x re-authentication is controlled using global variable "authServEapFail".		

Known Issues:

PR	**182150**
Summary:	Inconsistent QoS Manager when programming egress policy rules
Explanation:	Combined validation for Ingress and Egress Policies not available in software. To avoid error, User to calculate requisite Hardware entries before configuring.

PR	**212126**
Summary:	Openflow: OF Condition with source port link aggregation doesn't get applied
Explanation:	OF Flow Entry message with Ingress Port = Trunk ID will be accepted without any errors, but actual entry will not be applied in hardware. This will be fixed in a later release.

PR	**212127**
Summary:	Inconsistent behavior noticed while configuring UserPorts group in ACL condition
Explanation:	Only 8 port groups are supported in hardware. However, it is possible the system allows an ACL configuration using 8 port groups plus the "UserPorts" port group. When the "UserPorts" port group is also used in a ACL as condition, it is recommended to only configure a maximum of 7 port groups.

PR	**209623**
Summary:	OS6450 port is flapping with no device connected to it.
Explanation:	Solution identified, will be provided in next Release.

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

New Features:

1. DHCP Snooping Global Mode Enhancement

Platforms: OS6450, OS6250

Hosted AOS SW Release: 665.77.R02

In order to provide flexibility and additional security mechanism for enterprise customer to implement DHCP snooping in their environment the following additional options are provided. This would enable the AOS device in the network to operate as expected with configurable flag settings to be chosen based on expected behavior listed below.

udpGblSbUturn Mode	665R02
0	Default legacy behavior as in GA release
1	If this variable is set then unicast BOOTP packets will not follow dhcp snooping functionality and binding table will not be build using this.
2 Hardware Mode	New hardware settings where the combination of UDP Ports 68/67 as source and destination port will only be treated as DHCP Packets i.e if we receive any packet with source port 67 destination port 67 this will not be treated as DHCP and will not be trapped during dhcp snooping
3 Software Mode	New hardware settings to trap packets with 67/67 pair to CPU in addition to 67/68 and 68/67 New software forwarding logic in DHCP snooping context enhanced to take care of L2, L3 switching (ARP) and L3 routing (IP Route)

Usage
In AlcatelDebug.cfg
debug set udpGblSbUturn { 1 | 2 | 3 }

Limitations
It is still recommended to only use udpGblSbUturn=2 mode.

The udpGblSbUturn=3 mode is not recommended. In this mode, all DHCP packets in the DHCP transaction between the DHCP Relay and DHCP server will be trapped to CPU for packet type validations and then forwarded by software when allowed; applicable for even unicast packets which are destined to specific relay agent. This adds delay and unwanted parsing by non-participating routers originally.

2. Critical Voice Vlan – Phase 1

Platforms: OS6450, OS6250

Hosted AOS SW Release: 665.77.R02

Existing behavior is when the radius server becomes unresponsive or unreachable an IP phone getting authenticated will be moved to default vlan, which need not be the Voice vlan. This may cause phones to not connect. As an enhancement, current auth-server down feature is leveraged to support the critical voice vlan. A new policy is introduced to support one “Voice” User Network-Profile.

With this enhancement, when RADIUS authentication fails for server not responsive, the device mac-address is checked against the LLDP database. If it is deemed to be an IP Phone, mac-address is learned and classified in the configured “Voice-user-network-profile”. If no such voice profile is configured, then it is classified as that of a non-IP phone device as below.

If the mac-address is not an IP Phone, the normal policy is enforced. In the normal policy, if user-network profile is configured, mac-address is learned and classified in the respective profile. If user-network profile is not configured, mac-address is blocked and learned as filtering

Note: SNMP Trap implementation for this feature is planned as Phase-2 in future release.

LLDP Database Check

The following LLDP signature will be used to classify device as IP Phone:

System is a “Telephone”
System is a LLDP-MED Endpoint Class III
System is a LLDP-MED endpoint supporting LLDP-MED Network Policy and Extended Power via MDI

Re-Authentication

The automatic re-authentication is not applicable for the Voice User Network Profile. Mac-address learned and classified in the configured “voice-user-network-profile” will remain attached in the profile until mac-address is aged out or port goes down. The mac-address will not be flushed at every “re-authperiod” interval to force a new authentication request.

Mac-address learned and classified in the configured “user-network-profile” or block will be flushed at every “re-authperiod” interval forcing a new authentication request.

Usage

1) Command to enable/ disable auth server down feature

-> 802.1x auth-server-down {enable | disable}

2) Command to set the re-auth period in seconds. Configurable values are 1 – 9999 with 30 being default

-> 802.1x auth-server-down re-authperiod <num>

Example: 802.1x auth-server-down re-authperiod 45

3) Command for UNP Voice policy

-> 802.1x auth-server-down [no] voice-policy [user-network-profile <name>]

Example: 802.1x auth-server-down voice-policy user-network-profile “unp2”

4) Command for UNP normal policy

-> 802.1x auth-server-down policy [block | user-network-profile <name>]

Example: 802.1x auth-server-down policy user-network-profile unp1

Sample Configuration

```
-> show configuration snapshot aaa
! AAA :
aaa tacacs server-wait-time 30
aaa radius-server "rad_down" host 1.5.5.2 key
1d734304ae524c6a9da8c126348f3765848a51e7ba0dd44ad38fc877d5ed30b5 retransmit 3 timeout 2 auth-
port 1812 acct-port 1813
aaa authentication console "local"
aaa authentication telnet "local"
aaa authentication ftp "local"
aaa authentication http "local"
aaa authentication snmp "local"
aaa authentication 802.1x "rad_down"
aaa authentication mac "rad_down"
aaa user-network-profile name "unp1" vlan 20 hic disable
aaa user-network-profile name "unp2" vlan 10 hic disable maximum-ingress-bandwidth 1.00M maximum-
egress-bandwidth 1.00M
! PARTM :
! 802.1x :
802.1x auth-server-down enable
802.1x auth-server-down policy user-network-profile unp1
802.1x auth-server-down voice-policy user-network-profile unp2
```

Limitations

- The feature is only supported for POE IP Phone that supports LLDP-MED

- Re-authentication mechanism is not supported for an IP Phone classified in critical voice vlan

3. Critical voice VLAN when RADIUS down – Phase 2

Platforms: OS6450, OS6250

Hosted AOS SW Release: 665.80.R02

The feature provides the functionality to test the reachability of RADIUS server. This will be useful in validating the status of the configured radius servers.

An SNMP trap would be raised on the first polling cycle for the radius servers configured. And on the subsequent polling cycles, a snmp trap would be raised only if the server status gets changed from up to down and from down to up. Events would be logged in both these scenarios. If there are four radius servers configured, there should be only four entries of snmp trap and swlogs, until the status of the server is

changed. If backup server is configured, then server status will be updated as “UP” if either of the primary/backup servers are reachable and as “DOWN” when both primary and backup server s are not reachable.

Server status will be updated and trap will be raised even in the normal onex authentication (such as mac authentication, 802.1x, captive-portal supplicant and non-supplicant authentication), if a status change is detected during authentication. This happens only if the server status gets changed (UP/DOWN) in between the polling cycle and at that period a user tried to authenticate and found the status change in the server.

Existing cli command ‘show aaa server’ is enhanced to verify the reachability of the configured radius server.

Usage

1) Command to display the status of the configured radius-server

show aaa server rad

‘rad’ is the name of the radius server configured.

Example:
```
6450_DUT1-> show aaa server rad
aaa tacacs server-wait-time 30
Server name = rad
   Server type            = RADIUS,
   IP Address 1           = 140.140.10.100,
   IP Address 2       = 140.140.10.101,
   Retry number           = 3,
   Time out (sec)         = 2,
   Authentication port    = 1812,
   Accounting port        = 1813,
   Nas port               = default,
   Nas port id            = disable,
   Nas port type          = ethernet,
   Mac Addr Format Status  = disable,
   Mac Address Format      = uppercase,
   Unique Acct Session Id  = disable,
   Server oper status     = DOWN
```

Sample configuration outputs

1) 6450_DUT1-> aaa radius-server "rad" host 140.140.10.100 140.140.10.101 key alcatel

```
6450_DUT1-> show aaa server rad
aaa tacacs server-wait-time 30
Server name = rad
   Server type            = RADIUS,
   IP Address 1           = 140.140.10.100,
   IP Address 2       = 140.140.10.101,
   Retry number           = 3,
   Time out (sec)         = 2,
   Authentication port    = 1812,
   Accounting port        = 1813,
   Nas port               = default,
   Nas port id            = disable,
   Nas port type          = ethernet,
   Mac Addr Format Status  = disable,
   Mac Address Format      = uppercase,
```

Unique Acct Session Id = disable,
Server oper status = DOWN

Limitations

1.On takeover, the new primary would start the polling process and would raise a trap again if a server is found to be not reachable .The server status would not be synced across units.

4. ISF – Support for exceptional Subnets

Platforms Supported: OS6450

Hosted AOS SW Release: 6.6.5.80.R02

IP source filtering applies to DHCP Snooping VLANs and restricts traffic to only packets that contain the client source MAC address and IP address and belong to that VLAN obtained dynamically from the attached dhcp server. The DHCP Snooping binding table is used to verify the client information for the VLAN that is enabled for IP source filtering.

Hence when IP Source Filtering enabled, only the data originating/incoming from the client's MAC address, port and IP address will be allowed. All other packets will be dropped by default.

Customer needs a provision to bypass the IP source filtering on subnet basis. Hence maximum of 16 subnets are allowed to exclude from ISF.

Usage:

1. To enable/disable ISF on vlan level
   ip helper dhcp-snooping ip-source-filter vlan {num} {enable | disable}

   Enables or disables the IP source filtering capability at VLAN level. When this function is enabled, the switch allows the traffic that matches the client IP address, MAC address, interface number and VLAN combination obtained from the DHCP snooping binding table entry.

2. To enable/disable ISF on port level
   ip helper dhcp-snooping ip-source-filter port {slot/port} {enable | disable}

   Enables or disables the IP source filtering capability at a port or link aggregation level. When this function is enabled, the switch allows the traffic that matches the client IP address and source MAC address obtained from the DHCP snooping binding table entry.

3. To allow/disable the exceptional subnets on vlan level
   ip helper dhcp-snooping ip-source-filter {vlan num } {allow [ipaddress][mask subnet_mask]|enable|disable}

   By default this status is disabled. If it is enabled, the mentioned subnets will be excluded from IP source Filtering.

4. To show excluded subnets on vlan
   show ip helper dhcp-snooping ip-source-filter vlan

Displays the VLANs on which IP source filtering is enabled and the excluded subnets information.

Example:

show ip helper dhcp-snooping ip-source-filter vlan

```
VLAN     Ip Src      Excluded Subnets
ID          Filtering        IP                Mask
------+------------+---------------+--------------
4050     Enabled     10.55.40.4       255.255.255.252
```

Sample configuration outputs

```
->ip helper address 10.55.40.10
->ip helper forward delay 0
->ip helper dhcp-snooping option-82 policy keep
->ip helper dhcp-snooping enable
->ip helper dhcp-snooping binding enable
->ip helper dhcp-snooping bypass option-82-check enable
->ip helper dhcp-snooping linkagg 1 trust
->ip helper dhcp-snooping ip-source-filter vlan 4050 enable
->ip helper dhcp-snooping ip-source-filter vlan 4050 allow 10.55.40.4 mask 255.255.255.252 enable

->show ip helper dhcp-snooping ip-source-filter vlan
VLAN     Ip Src      Excluded Subnets
ID          Filtering        IP                Mask
------+------------+---------------+--------------
4050     Enabled     10.55.40.4       255.255.255.252
```

Limitations

1. ISF and allow subnets would consume TCAM entries which would impact on the user qos rules.

5. SSH Port

Platforms: OS6450, OS6250

Hosted AOS SW Release: 665.101.R02

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

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

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

Usage

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

ssh tcp-port <port-number>

<port-number >in the range 0-65535

Example: ssh tcp-port 35

Note: Well-known reserved TCP port numbers in the range (1-1024)and the IP ports which are internally used in AOS are excluded in assigning to SSH TCP port.

Limitations

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

2) Well-known reserved TCP port numbers in the range (1-1024) and the IP ports which are internally used(defined in system_ipport.sh) are excluded in assigning to SSH TCP port. Error will be thrown when these ports are tried to be configured for SSH port.

3) If we try to SSH from any other client which does not support option to provide remote port to be used for establishing the connection, then SSH will not work

6. C-Vlan Insertion for Untagged Packets

Platforms: OS6450, OS6250

Hosted AOS SW Release: 665.101.R02

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

Usage

1) To enable/disable the cvlan insertion for untagged packets

   ethernet-service untagged-cvlan-insert [enable/disable]

2) To associate the cvlan as untagged to the uni port

   ethernet-service sap <sap_id> uni <slot/port> untagged-cvlan <cvlan_id>

   <sap_id> The SAP ID number identifying the service instance (1-1024).
   <slot/port> The slot number for the module and the physical port number on that module
   <cvlan_id> Applies the SAP profile to frames untagged with this CVLAN ID

3) To configure an svlan interface which would map the svlan to the cvlan

ip interface <name> address <ip_address> mask<subnet_mask> vlan <svlan_id> cvlan <cvlan_id>

<name> Text string up to 20 characters. Use quotes around string if description contains multiple words with spaces between them

<ip_address> An host IP address

<subnet_mask> A valid IP address mask to identify the IP subnet for the interface

<svlan_id> Specifies the SVLAN number identifying the instance

<cvlan_id> Customer VLAN ID associated with the SVLAN

4) To show the status of the cvlan insertion for untagged packets feature.

show ethernet-service untagged-cvlan-insert

5) The below command is modified to display the cvlan associated to a uni port

show ethernet-service uni

6) To show cvlan mapped interface

show ip interface cvlan

Example

```
->ethernet-service untagged-cvlan-insert enable
->ethernet-service svlan 1001 name "VLAN 1001"
->ethernet-service svlan 1001 nni 3/1
->ethernet-service service-name "CustomerA" svlan 1001
->ethernet-service sap 10 service-name "CustomerA"
->ethernet-service sap 10 uni 1/7 untagged-cvlan 10
->ethernet-service sap 10 cvlan untagged
->ip interface "vlan10" address 10.10.10.1 mask 255.255.255.0 cvlan 10 vlan 1001
```

Sample configuration outputs:

```
->show ethernet-service untagged-cvlan-insert

Cvlan Insertion on Untagged Frames Feature: Enabled

->show ethernet-service uni

Port         UNI Profile     CVLAN
--------+-------------------------+-----------
  1/7      default-uni-profile          100

->show ip interface cvlan

Total 1 CVLAN interfaces
          Name               IP Address     Subnet Mask   Status Forward  Device  CVLAN
-------------------------------+---------------+---------------+------+-------+-------+--------
vlan10                       10.10.10.1      255.255.255.0       UP     YES vlan 1001  10
```

Limitations

1) Enabling “Cvlan insertion for untagged packets” feature on the switch would imply that the existing legacy behavior of UNI and NNI ports will no longer hold good.
2) Control traffic other than IP traffic destined to the switch out of scope of this feature.
3) The “show ip interface” will not display the mapped interfaces.
4) The feature is meant for all IP traffic which is supported by the switch. Any other traffic which in-turn goes through the same interface will also be double tagged.
5) As CVLAN-SVLAN is a one to one mapping, only one interface which uses the same SVLAN can hold the CVLAN. When we try to create another interface using the same SVLAN, and try to give a CVLAN value, it is expected to throw an error.
6) CVLAN tag is supported only for normal interfaces and not for dhcp-client ip addresses.
7) If the Cvlan insertion for untagged packets feature is enabled the legacy behavior of the UNI and NNI port will no longer hold good.
8) Only one cvlan can be associated to an UNI port.
9) The feature cannot be enabled or disabled when vlan stacking configurations already exists.
10) When the feature is enabled sap-profile cannot be created with priority value “map-inner-to-outer-p”.
11) When the feature is enabled sap-profile cannot be created with cvlan-tag mode “translate”.
12) When the feature is enabled, no new uni-profile creation will not be allowed and by default “default-uni-profile” will associated to a uni.
13) A UNI can be associated to only one SAP.
14) The uni-profile for the uni ports can be only “default-uni-profile”.
15) Trying to associate a sap-profile with translate option to a SAP will not be accepted.
16) Trying to associate a sap-profile with priority “MAP-INNER-TO-OUTER-P” will not be accepted.

7. Logging mechanism for traffic from in-eligible clients in ISF enabled network

Platforms Supported: OS6450, OS6250

Hosted AOS SW Release: 6.6.5.101.R02

This feature enables the user to see the packets getting dropped by IP-source-filter entries. Currently when ISF(ip-source-filter) is enabled on a port, it restricts all the IP-traffic on that port except the Dhcp traffic & the traffic from the client, whose binding entry exists on that port. But there is no way a customer/user can come to know which port/MAC/IP was dropped. This might help them in isolating the problem area/spoof attacks etc.

ISF Drop Log feature works in such a way that whenever a packet is dropped by ISF drop entry in hardware, drops will be logged in qos log which can be seen via “show qos log” command

Usage:

1. To view the ISF drop entries

   Show qos log

   a. This command is used to view the ISF drop entry
   b. ISF drop logging is enabled by default (currently there is no provision to disable them). Hence if the packets are getting dropped due to ISF-Drop rule, packets will start getting logged

   Example:

```
6450_test# show qos log
**QOS Log**
```

```
9/16/01 18:09:18 [@18:09:18] rule ISF-DROP matched
9/16/01 18:09:18  Tagged.     802.1p 0
9/16/01 18:09:18  svlan 10 VRF (null) port 1/9
9/16/01 18:09:18  MAC 00:00:1E:1D:EE:14 -> E8:E7:32:77:BB:A2
9/16/01 18:09:18  TOS 0x00 (p255) 10.10.10.10   -> 10.10.10.100
9/16/01 18:09:18 [@18:09:18] rule ISF-DROP matched
```

Limitations:

1. Logging of packets are done at 64pps, i.e. if there is a wire-rate attack, we would log 64 packets per second. However this has a short-coming, wherein if there are multiple attackers then some of the IPs might not get logged.

8. Monitoring interstack connection

Platforms: OS6450-OS6250

Hosted AOS SW Release: 665.101.R02

In the existing implementation, there are no CLI commands to monitor the status and statistics of Stacking interfaces. The requirement is to provide the ability for the user to monitor the status and statistics/counters of the stacking links (if the product is stackable) in addition to normal user interfaces using the below CLI Commands

Following new CLI commands are introduced to store the stacking ports details.

show stacking interfaces

show stacking interfaces status

show stacking interfaces counters

show stacking interfaces counters errors

Usage

1) To display general interface information for the stacking ports

   show stacking interfaces

2) To display interface counters information (for example, unicast, broadcast, and multi-cast packets received or transmitted) for the stacking ports

   show stacking interfaces counters

3) To display interface error frame information (for example, CRC errors, transit errors, and receive errors) for the stacking ports

   show stacking interfaces counters errors

4) To display the interface line settings (for example, speed, and mode) for the stacking ports

   show stacking interfaces status

5) To display the interface line settings (for example, speed, and mode)information for the specific stack port entered in the command

show stacking interfaces <slot/port> status

6) To display interface counter information (for example, unicast,packets received/transmitted) for the specific stack port entered in the command

show stacking interfaces <slot/port> counters

7) To display interface error frame information (for example, CRC errors, transit errors, and receive errors) for the specific stack port entered in the command.

show stacking interfaces <slot/port> counters errors

8) This command will clear the counter statistics related to the stack port specified in the command
stacking interfaces <slot/port> no l2 statistics

Examples

```
-> show stacking interfaces
 Slot/Port  1/51 :
  Operational Status     : down,
  Last Time Link Changed : TUE JUL 28 19:04:01 ,
  Number of Status Change: 0,
  Type                   : Stacking,
  BandWidth (Megabits)   :    -   ,          Duplex          : -,
  Rx             :
  Bytes Received  :                0, Unicast Frames :                0,
  Broadcast Frames:                0, M-cast Frames  :                0,
  UnderSize Frames:                0, OverSize Frames:                0,
  Lost Frames     :                0, Error Frames   :                0,
  CRC Error Frames:                0, Alignments Err :                0,
  Tx             :
  Bytes Xmitted   :                0, Unicast Frames :                0,
  Broadcast Frames:                0, M-cast Frames  :                0,
  UnderSize Frames:                0, OverSize Frames:                0,
  Lost Frames     :                0, Collided Frames:                0,
  Error Frames    :                0
 Slot/Port  1/52 :
  Operational Status     : up,
  Last Time Link Changed : TUE JUL 28 19:04:01,
  Number of Status Change: 0,
  Type                   : Stacking,
```

```
  BandWidth (Megabits)  :   10000,          Duplex         : Full,
  Rx            :
  Bytes Received  :         103100016, Unicast Frames :          85856,
  Broadcast Frames:             0, M-cast Frames  :          12,
  UnderSize Frames:             0, OverSize Frames:           0,
  Lost Frames     :             0, Error Frames   :          0,
  CRC Error Frames:             0, Alignments Err :           0,
  Tx            :
  Bytes Xmitted   :          3883702, Unicast Frames :          45872,
  Broadcast Frames:          1948, M-cast Frames  :          813,
  UnderSize Frames:             0, OverSize Frames:           0,
  Lost Frames     :             0, Collided Frames:          0,
  Error Frames    :             0

-> show stacking interfaces status
Slot/ AutoNego  Speed  Duplex
Port          (Mbps)
-----+--------+-------+--------
  1/51  -       -     -
  1/52  -     10000   Full
  3/27  -     10000   Full
  3/28  -       -     -

-> show stacking interfaces counters
 1/52,
  InOctets      =         108040828,  OutOctets      =         4065016,
  InUcastPkts   =           89957,  OutUcastPkts   =           48056,
  InMcastPkts   =             12,  OutMcastPkts   =           868,
  InBcastPkts   =             0,  OutBcastPkts   =          2006,
  InPauseFrames =             0,  OutPauseFrames =             0,
  Sampling Interval 5 seconds
  InPkts/s      =             28,  OutPkts/s      =           16,
  InBits/s      =          268016,  OutBits/s      =           9720
 3/27,
  InOctets      =          4012826,  OutOctets      =         108129633,
  InUcastPkts   =           48045,  OutUcastPkts   =           89945,
  InMcastPkts   =             868,  OutMcastPkts   =           12,
  InBcastPkts   =            2006,  OutBcastPkts   =           0,
  InPauseFrames =             0,  OutPauseFrames =             0,
  Sampling Interval 5 seconds
  InPkts/s      =             16,  OutPkts/s      =           29,
  InBits/s      =           9840,  OutBits/s      =          270352

-> show stacking interfaces counters errors
1/52,
IfInErrors      =             0,
```

```
Undersize pkts    =              0,  Oversize pkts =              0

->stacking interfaces 1/27 no l2 statistics
show stacking interfaces 1/27 counters
1/27,
  InOctets      =              0,  OutOctets      =              0,
  InUcastPkts   =              0,  OutUcastPkts   =              0,
  InMcastPkts   =              0,  OutMcastPkts   =              0,
  InBcastPkts   =              0,  OutBcastPkts   =              0,
  InPauseFrames =              0,  OutPauseFrames =              0,
  Sampling Interval 5 seconds
  InPkts/s      =              0,  OutPkts/s      =              0,
  InBits/s      =              0,  OutBits/s      =              0
```

9 . Ethernet-OAM Remote Fault Propagation

Introduction:
Remote Fault propagation (RFP) propagates connectivity fault events into the interface that is attached to a MEP. Once the fault is detected for a MEP, the MEP's interface is shutdown. Unlike other violation mechanisms that keep the link up when an interface is shutdown, this fault propagation mechanism will effectively shutdown the link so that the remote end of the interface also detects a link down.The feature is configurable on per MEP basis and is supported only for UP MEPs. Remote Fault Propagation detects only Loss of connectivity and Remote MAC defect.

Platforms Supported:
Omni Switch 6450
Omni Switch 6250

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

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

Usage Guidelines
The domain and association must be created before RFP can be enabled.
The end point must be configured in the MEP list, before it can actually be created.
The MEP must be an UP MEP. If down MEP is specified, CLI returns with an error.
The admin state of the MEP must be enabled in order to report faults.
RFP cannot be enabled on virtual UP MEP since it is not associated with a physical interface.

If RFP is enabled on an UP MEP created on a linkagg, then detection of RFP violation will shutdown the individual member ports. No new ports should be added to or removed from the linkagg at this time. This will not be blocked from configuration, but is left to the user.
It is recommended that if RFP is enabled on a port, then any other violation feature (Link Mon or LFP) should not be configured.
It is recommended that if RFP is enabled on a port, then automatic recovery is disabled for that port
If Link Mon is configured on a RFP enabled port, then the WTR timer must be less than the CCM interval.

Example:

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

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

Limitations: None

10. TWAMP

Platforms: OS6450,OS6250

Hosted AOS SW Release: 665.133.R02

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

Following are the functionality provided by the feature.

- AOS S/w implements TWAMP server/reflector functionality specified in RFC 5357.

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

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

Usage

1) Command to enable TWAMP server.

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

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

2) Command to display TWAMP server

-> show twamp server info

Example: show twamp server info
TWAMP Server
Port: 862
Inactivity timeout: 15
Allowed-Client:
200.200.200.2 / 255.255.255.255

3) Command to show the TWAMP server connections

-> show twamp serverconnections

Example: show twamp server connections

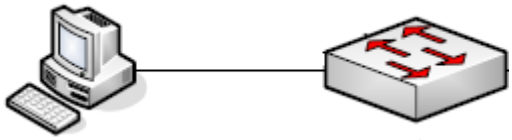
Client IP	Conn Status	Time of Last Run	Pkts Sent	Pkts Received	Session Identifier
200.200.200.2	SETUP_DONE	0	0	0	96969696d83c6bea0fe502a0a01de548
200.200.200.2	SETUP_DONE	0	0	0	96969696d83c6bea0fe502a0af889d1e

Sample Use Cases

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

The DUT should be enabled for TWAMP server functionality
DUT should have configurations for TWAMP server like the TWAMP port number ,allowed-client IP address

TWAMP packets should be sent from ixia which acts like a TWAMP client



DUT

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

Limitations

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

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

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

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

11. Network Address Translation

Platforms: OS6250, OS6450

Hosted AOS SW Release: 665.133.R02

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

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

Following are the functionality provided by the feature:

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

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

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

Usage

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

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

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

- To enable NAT policy action

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

The rewrite ip should be an interface ip on the device

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

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

- To enable qos at the global level
  qos enable

- To apply qos at the global level
  qos apply

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

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

- To delete a NAT policy action
  no policy action “action_name”

- To show the NAT policy configuration
  show configuration snapshot qos

- To check the NAT traffic flow
  show qos nat flows

Example

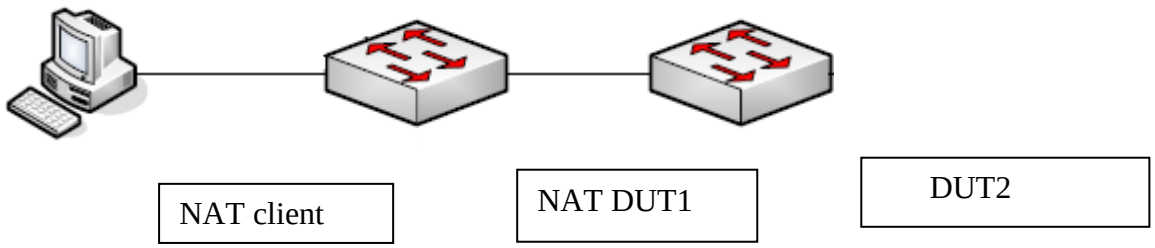
```
->policy condition nat source ip 99.99.99.0 mask 255.255.255.0
->policy action nat source rewrite ip 9.9.9.2
->policy rule nat condition nat action nat
->qos apply

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

->>show qos nat flows
```

Proto	Inbound Private	Inbound Public	Outbound	Inbound Rx/Tx	Outbound Rx/Tx
TCP	100.100.100.2:0	30.30.30.1:0	99.99.99.2:0	51746/51746	10821/10821

Sample Use Cases

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

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



NAT DUT1:

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

Limitations

1. NAT feature is not supported in stacks.
2. This feature is CPU intensive, sessions like webview(HTTP), SSH, Telnet, FTP would not be working when the traffic rate crosses 1300pps (both forward + reverse direction combined).
3. DNS transaction not supported.

12. NTP SNMP Traps

Platforms: OS6250, OS6450

Hosted AOS SW Release: 665.133.R02

Current 66x AOS release provides support for configuring NTP in client mode. NTP client will select a synchronization peer from among the configured NTP servers for performing clock synchronization. The new requirement is that, SNMP trap needs to be raised for few scenarios

Following are the functionality provided by the feature:

1) When NTP client is enabled in AOS, it will select a clock synchronization peer from among the configured NTP servers. If for some reason, the synchronization peer changes from one server to another, then SNMP trap should be raised to indicate that the NTP synchronization server has changed.

2) When NTP client is enabled in AOS and if none of the configured NTP servers is reachable or cannot be selected as the synchronization peer (all falsetickers), then SNMP trap should be raised to indicate the unavailability of all NTP servers

Usage

This feature is enabled by default. No user configuration required.

Trap Details

alaNtpSyncPeerChangeTrap : This trap is generated when the synchronization peer changes. It will contain the alaNtpSyncPeerIpAddress parameter, which will provide the IP address of the new Synchronization peer.

alaNtpAllPeerUnreachableTrap : This trap is generated when there are no synchronization peers. It will contain the alaNtpAllServerDown parameter, which will display that there are no active/reachable NTP peers /servers available.