Omni Switch 6450/ 6350

Release 6.7.2.85.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 50 and 85

PR Number	PR summary	Explanation	Build
227348	AOS 6x sending LLC packet with 64 bytes data for AMAP packets -seen as malformed in wireshark	Code change done to calculate and send the correct length value in the amap packet.	672.68.R01
226677	OS6450 crash with tahw_l2 task suspended after upgrade to 6.7.2 R01.	Code changes done to generate memory debug file in primary unit during high memory scenario. Fix controlled by a global variable 'hmonDebugEnable'	672.68.R01
227485	OS6450 crash	Defensive Fix done to prevent accessing wrong address in dhcp that in turn prevents crash	672.68.R01
226162	stack reboot after upgraded to 6.7.2.R01	Code changes done to continue fetching the values from RBT tree where overflow occurred previously	672.52.R01
223679	port going down due to STP violation even through no bpdu is received on the port	Debugs are added in Qdispatcher to check why unicast packets are trapped in STP. Option to redirect STP debug logs to swlog	672.59.R01
215927	6450 - packets looping on LACP ports during few seconds after rebooting 6450, causing loop detection on remote HP switch	When linkagg ports in configured state, removed the vlan port association only from hardware to avoid loop in the network.	672.68.R01
225348	100% CPU utilization when accessing the switch via HTTP	Code changes done to prevent infinite loop while fetching MAC address entries in LPS ports via web view/SNMP.	672.68.R01
226041	After installing KB3212646 in Windows 2012 Radius server, fragmented EAP-TLS header are stripped by the switch to the client.	Code changes has been done that the Radius packets are processed if the value of EAP fragment is of 1 byte. The data in the packet will be forwarded to the client correctly and hence the authentication will succeed.	672.80.R01
224568	2xOS6900 - packet loss in adjacent switch (OS6450) connected to slave unit when the slave unit is powered OFF electrically.	Code changes done to prevent intermittent packet loss in ERP ring when ring goes to protection state.	672.68.R01
224136	OV2500 unable to read serial number. of the SEC/SLAVE units power supply.	Changes done to show serial number of the power supplies of SEC/SLAVE units other than 900W power supplies	672.68.R01
203334	100% CPU with task vstkcmm after OS6850 NI takeover	Fix high CPU seen in vstkcmm on repeated takeover	672.68.R01
224913	OS6450-U24SXM: User Port is showing up even if it is admin down (100MB SFP)	Workaround done to power down the port when admin status is down with 100M SFP	672.68.R01

223256	ip-ping SAA probe got stuck on OS6450	Code change done to clear the particular SAA id in the global array after the all the processing is done for that particular SAA id.	672.68.R01
224350	OS6450: SSH into OS6450, the password prompt is not displayed until 'Enter Key is hit 5 times	Code changes done to handle empty space displayed before displaying password prompt	672.68.R01
226286	OS6450 crashed when executing aaa test-radius-server command	Fixed crash seen when giving aaa test-radius-server	672.68.R01
223577	health-check doesn't work during 4-5 min after a takeover	Sending a dummy request to radius server every 10 sec from takeover in the newly formed primary as the ip stack is already running and the task has spawned. Dummy request will reach the radius server only during the next iteration when the server is reachable from new primary.	672.68.R01
226641	Configuration Missing after port 5/37:ip helper dhcp-snooping ip-source-filter port 5/37 enable	Code changes done to handle MIP_OVERFLOW of all the commands of the DHCP relay.	672.68.R01
223409	OS6350: Frames not forwarding	Frames are forwarded successfully from OS6350 switch.	672.68.R01
226138	AOS switch does not generate a logs message when the violation occurred due to VRRP/OSPF packets	Code changes done to log in swlogs when user port is shut down due to ingressing of OSPF/VRRP packets.	672.68.R01
226615	show running directory" command shows that it is synchronized even though AAA configuration were changed	show running directory command shows stack is not synchronized when onex configuration are done.	672.68.R01
225608	OS-6450-P10 hanged and rebooted	Changes done to handle memLeak in taUdldni	672.80.R01
226809	Connectivity issue between OS6900-T20 and OS6450-P48	Code changes done to handle the link status change events properly.	672.68.R01
225974	OS6450 802.1x mobile port display issue	8021x display issue fixed	672.68.R01
224085	Linkagg timeout with reason " linkAggNi main info(5) lacp_rxm_expired 1/1/9(8)"	Code changes done to admin disable/enable port when change in linkagg config	672.68.R01
221808	6450 client MAC learnt on 802.1x and MAC table (connected by hub) though the device is disconnected.	Check added to delete a Mac-address in OnexCmm	672.68.R01
227285	Systrace Error "taRadiusst [CTRACE] Task 7e2e530 call circ_trace_put3 of task AAA(7e43e20)" clarifi	systrace message in "taRadiusStats " should not access the circular buffer owned by AAA . . Message should log only in SYSTRACE.	672.68.R01
212278	Issue with WebView File management when accessed with TACACS user	Changes done to authorize a command based on the partition management family name (PM_FAMILY_SYSTEM_SERVICES) with the remote authentication server.	672.68.R01

212677	ICMP latency is noticed in ERP network	Ignoring RAPS packet with DNF bit as 0 when ERP ring is in IDLE state to stop frequent flush	672.68.R01
213044	SSH and Console access to the switch unresponsive	Memory is freed properly in AAA module.	672.68.R01
213614	“show aaa switch-access priv-mask” results in memory leak in AAA	Memory is released in AAA module.	672.68.R01
213742	Memory leak seen due to continuous show configuration snapshot	Port admin state is disabled and then enabled again whenever we modify a linkagg port property to update the port context	672.68.R01
213448	show module long doesn’t display the full 16 digit serial number of the stack cable	Serial Number which are more than 16 digits are displaying properly.	672.68.R01
212322	Enabling S-Flow Interrupts Traffic to the switch	Changes done to not trapping the ARP packets to CPU for sampling.	672.68.R01
225118	OS^450 first icmp packet loss	Changes have been done to make the source wait for reply for the "timeout" value we specify in cli.	672.68.R01
223191	Dying Gasp trap not seen randomly after the cold reboot	Increased the priority of the dying gasp packet which is send to SNMP station.	672.68.R01
224923	UNP with number for auth-server-down policy creating boot.cfg.err	Code changes done to retain the double quotes in snapshot while configuring UNP name for supplicant/non-supplicant/ captive portal policies as well as in auth serv down command.	672.68.R01
225421	"show stack split-protection helper status" show enabled in case helper status is disabled	Changes done to display linkagg id status based on ssp status	672.68.R01
225347	OS6450- Crashed with PMD relating to SSH	Check whether the session ID is valid before user authorization is done through TACACS server [Defense fix].	672.68.R01
228104	Traffic loss in port 1/1 after upgrade	VLAN configuration fails on port 1/1 causing traffic loss after upgrade to 6.7.2.80.R01, when any dynamic linkagg configuration is present in the switch. Fix done to modify invalid condition, so that proper linkagg status is returned for port 1/1.	672.85.R01

Known Issues:

PR **226368** Build:

Summary: With "Show ip helper dhcp-snooping global-counters" cli the Binding error (TCAM Unavailable) Entry gets incremented for 253 clients, instead of 256.

Explanation:	OS6450 ASIC supports total 256 H/W entries for ISF. When we enable ISF itself 3 entries will be used by the switch and allows 253 user associated entries.

PR	**217634** Build:
Summary:	SFP ports do not come up after a reboot or disconnection of SFP due to uplink ports auto-neg issue.
Explanation:	There is an interop issue for auto-negotiation working, when 6450 and 6350 are connected using UPLINK ports at both ends. Workaround in this case, is to disable auto-negotiation and force set say, 1000 Mbps full duplex on both ends. This issue is not seen when connection between 6450 & 6350 is done using uplink port on one end and network/user port at another end.

PR	**228172** Build:
Summary:	When user enables “debug dhcp port 1/1” “debug show dhcp” is showing logs from other ports also.
Explanation:	When the filter at port level is set to 1/1, the “debug show dhcp” output displays logs from DHCP clients on all the ports including 1/1. Workaround is to use MAC and VLAN based filtering instead of port based filtering. We need to specify the MAC address and VLAN of the client for which dhcp debug logs needs to be enabled with the command “debug dhcp mac-address<MAC-ADDRESS> vlan <VLAN-ID>”. Example: debug dhcp mac-address 11:22:33:44:55:66 vlan 10

New Features:

1. Topology Change Notice Logging

Platforms Supported: OmniSwitch 6450 and OmniSwitch 6350

Hosted AOS SW Release: 672.85.R01

In the customer network, flat STP is used with a core infrastructure of OS6900 and OS6450 managed by the network administrator. However, on the edge network, other vendor switches can be attached for specific use. Instability on these local networks has a severe impact on the entire network as TCN are getting generated causing MAC flushes and connectivity issues. Typically, the root cause is a port flapping situation. Troubleshooting such issue is difficult as it takes a lots of time to identify the source of the problem. Also, the troubleshooting usually starts in the few Core routers/switches, but there is currently no information on the show commands or switch logs that will give a hint that STP is not stable due to TCN received on some ports.

Current implementation of STP doesn’t have any information to debug the Topology changes that trigger mac-flushes in a switch. There is only counter information to specify the amount of TCN received. In a typical customer network there will be lot of ports which can be part of a single STP instance and finding out which port has received that TCN is a big challenge. So this enhancement is focused to add additional debugging information to help the customers in order to know the frequency and the magnitude of topology changes which is happening in the ports for a given instance in the switch.

Usage:

a. *debug show spantree { CIST | MSTI | VLAN } <vlan_id | msti_id> Ports*

This command is used to display the stp bpdu stats for particular vlan or msti instance

The allowed CLI combinations are as follows:
hash-control chain-length default
hash-control chain-length extend

Syntax Definitions:

vlan_id	:	The vlan_id for which the bpdu stats should be fetched.
Msti_id	:	The msti_id for which the bpdu stats should be fetched in FLAT mode.

Usage Guidelines:

1. Vlan Id is mandatory in case of switch running in 1x1 mode.
2. Msti_id is mandatory in case of switch is running in FLAT mode and protocol mstp configured.
3. For Cist no vlan or msti_id is required.
4. Error will be displayed if invalid vlan or msti id is provided.

b. *debug stp reset cumulative-stats [stp_id]*

This command is used to clear the counter information in CMM and NI based on specific stp instance or all instances.

Syntax Definitions:

stp id	:	The stp instance for which the counters has to be cleared.

Usage Guidelines:

1. It is used to clear the bpdu stats for specific or all instance.
2. If no stp instance is provided, then the counters will be cleared for all stp instances.
3. Stp_id should be given in the format of 4096+vlan_id for 1x1 mode.
4. In flat mode either 0 or msti_id can be given.

c. Whenever there is a root port or root bridge change we will be adding a info level swlog.

Sample Output:

For Root Port Change:
MON JAN 31 06:37:41 2000 STP info Root port Change for VLAN/STP-ID 3/4099 on port 2/21

For Root Bridge Change:
MON JAN 31 08:00:51 2000 STP info New Root Bridge Change for VLAN/STP-ID 3/4099

d. When Excessive number of TCN's are received in a bridge it causes unnecessary mac-flushes. In order to notify that there is an excessive amount of TCN we will log a swlog.

Sample Output:

For VLAN + RSTP:
MON JAN 31 06:37:41 2000 STP warning Topology Change Storm detected for VLAN 3 on PORT 2/21

For FLAT + CIST:
MON JAN 31 06:30:11 2000 STP warning Topology Change Storm detected on PORT 1/1

For FLAT + MSTP CIST:
MON JAN 31 07:27:41 2000 STP warning Topology Change Storm detected for CIST on PORT 2/5

For FLAT + MSTP MSTI:
MON JAN 31 06:30:11 2000 STP warning Topology Change Storm detected for MSTI 1 on PORT 2/6

e. TCN logging starts basically in finding out which port in a switch is responsible for the TC's. It is required to have the port information which receives the Topology change to be displayed in spantree command.

Sample Output:

```
L2-DUT1-> show spantree 1
Spanning Tree Parameters for Vlan 1
  Spanning Tree Status :                ON,
  Protocol             :       IEEE Rapid STP,
  mode                 : 1X1 (1 STP per Vlan),
  Priority             :       32768 (0x8000),
  Bridge ID            :   8000-00:e0:b1:e2:b0:5c,
  Designated Root      :   8000-00:e0:b1:e2:b0:5c,
  Cost to Root Bridge  :                 0,
  Root Port            :              None,
  Next Best Root Cost  :                 0,
  Next Best Root Port  :              None,
  TxHoldCount          :                 3,
  Topology Changes     :                 0,
  Topology age         :          00:00:00,
  Last TC Rcvd Port    :   Slot 1 Interface 1,
    Current Parameters (seconds)
      Max Age            =    20,
      Forward Delay      =    15,
      Hello Time         =     2
    Parameters system uses when attempting to become root
      System Max Age       =    20,
      System Forward Delay =    15,
      System Hello Time    =     2
```

2. Enhancement for Supplicant and Non-Supplicants

Platforms Supported: OmniSwitch 6450 and OmniSwitch 6350

Hosted AOS SW Release: 672.85.R01

'Enhancement for Supplicant and Non-supplicants' fulfil the customer requirements where the customer has deployed a BYOD solution with Clear Pass that uses the RADIUS attribute Session-Timeout and User-Name. Below two requirements are met as a part of this enhancement.

1. Two CLI commands are introduced for MAC/non-supplicant users and for 802.1x/supplicant users to handle the re-authentication process based on the RADIUS returned attributed "Session-Timeout" from Clear Pass/RADIUS Server.
2. Username will be displayed for both MAC user and 802.1x user based on the returned "User-Name" attribute from Access Accept frame.

The enhancement made updates the username for MAC user also and is displayed in all the show commands of non-supplicants. Also, the RADIUS returned "user-name" attribute will be updated in the radius request/Accounting Request message.

Usage:

The requirement is to control the re-authentication process for both supplicant users as well as non-supplicant users based on the 'session-timeout' attribute returned from the server.
When "Session-Timeout" attribute is sent by the server in an Access-Accept packet with a Termination-Action set to RADIUS-REQUEST (1), the returned attribute from the server would specify the number of seconds provided prior to re-authentication.

In order to implement this, we need to use two RADIUS attributes “termination-action” and “session-timeout” to take the termination action value as well as session-timeout value from the access-accept packet sent by the server. Only if the termination-action is set to 1, the session-timeout value returned from the server would be considered as valid.

Once the session-timeout or fixed-interval value has reached,

- For non-supplicants - MAC address would be flushed from hardware thereby triggering re-authentication.
- For supplicants - EAP logoff message would be sent to the client which would trigger new authentication process.

Commands:

For supplicants:

802.1x slot/port trust-radius {enable | disable}

Usage guidelines:

The above CLI specifies whether to use the Session-Timeout attribute value for the re-authentication time interval or to use the locally configured re-authentication time interval value. The Session-Timeout attribute can be returned from the server in an Accept-Accept message.

The allowed CLI combinations are as follows:

802.1x slot/port trust-radius enable
802.1x slot/port trust-radius disable

Syntax Definitions:

trust-radius	Specifies whether the re-authentication interval should be taken from the Session-Timeout attribute of Access-Accept message returned by the RADIUS server.

Defaults:

The default value of trust-radius parameter is disable.

802.1x re-authentication and re-auth period can be specified using the already existing CLI command.

802.1x slot/port [re-authperiod seconds] [reauthentication | no reauthentication]

Syntax Definitions:

re-authperiod	Specifies re-authentication period which can be configured by the user. Session-timeout interval takes the precedence even if re-authperiod is configured by user
reauthentication	Specifies whether reauthentication should be enabled so as to reauthenticate the supplicant user based on the session-timeout interval (if it is sent through access-accept) or based on the re-authperiod specified by the user

Defaults:
Since the parameters “re-authperiod” and “reauthentication” belongs to IEEE MIB standards, the 802.1x re-authentication is disabled by default and 802.1x re-authperiod default value is 3600 seconds.

Usage Guidelines:

1. When the trust-radius option is enabled, the timeout value returned in Session-Timeout attribute of Access-Accept message takes precedence over the configured re-authentication interval.

2. If re-authentication is disabled, then there is no effect for the trust-radius parameter.
3. The change in re-authentication interval takes effect immediately for all users that are authenticated after the configuration. For users who are already authenticated the re-authentication interval takes effect only after the user is flushed out or when the user is re-authenticated again.

For non-supplicants:

Command:

802.1x <*slot/port*> non-supplicant **session-timeout** {enable|disable} **[interval** <num>] **[trust-radius** {enable|disable}]

This CLI enables/disables the session timeout and set the session timeout interval for MAC authenticated users.

Syntax Definitions

Specifies the MAC session timeout in seconds.

trust-radius	Specifies whether the session timeout should be taken from the Session-Timeout attribute of Access-Accept message returned by the RADIUS server.

Defaults: The default session timeout interval is set to 43200 seconds (12 hrs).

Usage Guidelines

- The 802.1x non-supplicant session-timeout is disabled by default and when enabled the default session timeout interval is set to 43200 seconds.
- The allowed range for session timeout interval is between 12000 to 86400 seconds.
- The trust-radius option is disabled by default for MAC authenticated users.
- If the session-timeout is disabled, there is no effect for the interval that is configured in the command and there is no effect even if the trust-radius parameter is enabled.
- When the trust-radius option is enabled the timeout value returned in Session-Timeout attribute of Access-Accept message takes precedence over the configured session-timeout. After the session timeout is reached, the MAC user is automatically logged out and its MAC address is flushed.
- The change in session timeout interval takes effect immediately for all users that are authenticated after the configuration. For users who are already authenticated the session timeout interval takes effect only after the user is flushed out or when the user is re-authenticated again.

Example

```
802.1x 1/1 non-supplicant session-timeout enable interval 13000
802.1x 1/1 non-supplicant session-timeout enable interval 14000 trust-radius enable
802.1x 1/1 non-supplicant session-timeout enable trust-radius enable
802.1x 1/1 non-supplicant session-timeout disable
```

Display Commands:

1. *show configuration snapshot aaa*

Usage Guidelines

The * symbol displayed in the show output (FDB Hash Chain Length = EXTEND*) indicates that the configured hash chain length will be applied only after reloading the switch.

Example

```
➔  Show configuration snapshot aaa
! aaa :
802.1x 1/1 trust-radius enable
802.1x 1/2 trust-radius disable
802.1x 1/1 non-supplicant session-timeout enable interval 14000 trust-radius enable
```

2. *show 802.1x non-supplicant detail*

Usage Guidelines:
If the session-timeout is disabled for MAC/non-supplicant users and if the re-authentication is disabled for 802.1x/supplicant users, then the ReAuthPeriod Value in the above show command will display the timer value in which the user is authenticated at last.

Example

```
-> show 802.1x non-supplicant detail

Slot 1 Port 36  - has no non-supplicant to show.

Slot/Port              = 02/13
  MAC Address            = 00:00:c3:de:79:b8
  MAC Authen Status      = Authenticated
  Classification Policy  = Basic-VLAN ID
  VLAN Learned           = 100
  Dynamic UNP            = Disabled
  Username             = NAMEXYZ
  ReAuthPeriod           = 40
  HIC Status           = Not Started



-> show 802.1x users detail
Slot/Port              = 02/13
  MAC Address            = 00:00:c3:de:79:b8
  Port State           = Authenticated
  Classification Policy  = Basic-VLAN ID
  VLAN Learned           = 100
  Username             = NAMEXYZ
  ReAuthPeriod           = 60
  Dynamic UNP            = Disabled
  HIC Status           = Not Started
```

show 802.1x non-supplicant

Usage Guidelines:
This is an existing command that can be used to display a list of all non-802.1x supplicants learned on one or more 802.1x ports. The below show command is modified to display the user-name column. The ‘user-name’ column displays the user-name entered through MAC authentication if the user is a MAC user.

Example

```
➔       show 802.1x non-supplicant
Slot  MAC             MAC Authent     Classification     Vlan     User
Port  Address         Status          Policy             Learned  Name
-----+-----------------+---------------+------------------+--------+------------
01/13 00:00:00:00:2c:83 Authenticated   Basic-GM          10       000000002c83
01/13 00:00:00:00:3c:82 Authenticated   Basic-GM          10       000000003c82
02/10 00:00:00:00:7c:86 Authenticated   Basic-GM          10       000000007c86
```

show 802.1x non-supplicant detail

Usage Guidelines:

This is an existing command that can be used to display the detailed information about the MAC user. This show command is modified to display the user-name.

Example

```
➔  show 802.1x non-supplicant detail
Slot/Port              = 01/13
  MAC Address          = 00:00:00:00:2c:83
  MAC Authen Status    = Authenticated
  Classification Policy  = Basic-GM
  VLAN Learned         = 10
  Dynamic UNP          = Disabled
  UserName             = 000000002c83
  ReAuthPeriod         = 40
  HIC Status           = Not Started
```

show 802.1x non-supplicant unp

Usage Guidelines:

This is an existing command that can be used to display the UNP information of the MAC user. The below show command is modified to display the user-name column. The ‘user-name’ column displays the user-name entered through MAC authentication if the user is a MAC user.

Example

```
➔  show 802.1x non-supplicant unp
Slot  MAC             Vlan  HIC           Dynamic   User
Port  Address               Status        UNP       Name
-----+-----------------+-----+---------------+--------------------
03/01 00:00:00:00:00:01    10 Not Started     unp     000000000001
```

show aaa-device non-supplicant users

Usage Guidelines:

This is an existing command that can be used to display the detailed information about the MAC user. The below show command is modified to display the user-name. The ‘user-name’ column displays the user-name entered through MAC authentication if the user is a MAC user.

Example

```
➔  show aaa-device non-supplicant-users
Slot  MAC             User             Addr IP         Authentication User Network
Port  Address         Name             Vlan Mode Address       Type Result Profile Name
-----+-----------------+---------------+----+----+---------------+----+----+---------------
1/13 00:00:00:00:2c:83  000000002c83        --   10 Brdg -             MAC  Pass -
```

show aaa-device all-users

Usage Guidelines:

This is an existing command that can be used to display the detailed information about all the users connected to OmniSwitch. This show command is modified to display the user-name for MAC users. The 'user-name' column displays the user-name entered through MAC authentication if the user is a MAC user (non-supplicant) and also displays the user-name entered through Onex authentication if the user is a 802.1x user (Supplicant).

Example

```
➔       show aaa-device all-users

Slot  MAC             User             Addr IP        Authentication User Network
Port  Address         Name             Vlan Mode Address       Type Result Profile Name
-----+----------------+----------------+----+----+---------------+----+----+---------------
 3/ 1 00:00:00:00:00:01   000000000001   10 Brdg -           MAC  Pass          unp
```

show aaa-device non-supplicant-users unp <string>

Usage Guidelines:

It is an existing command that can be used to display the detailed information about the non-supplicant clients. The below show command is modified to display the user-name. The 'user-name' column displays the user-name entered through MAC authentication if the classified non-supplicant user belongs to any user-network-profile.

Example

```
➔     show aaa-device non-supplicant-users unp unp
Slot  MAC             User             Addr IP        Authentication User Network
Port  Address         Name             Vlan Mode Address       Type Result Profile Name
-----+----------------+----------------+----+----+---------------+----+----+---------------
 3/ 1 00:00:00:00:00:01   000000000001   10 Brdg -           MAC  Pass          unp
```

show aaa-device non-supplicant-users unp <string> port <slot/port>

Usage Guidelines:

It is an existing command that can be used to display the detailed information about the non-supplicant clients. The below show command is modified to display the user-name. The 'user-name' column displays the user-name entered through MAC authentication if the classified non-supplicant user belongs to user-network-profile for a particular port.

Example:

```
➔     show aaa-device non-supplicant-users unp unp port 3/1
Slot  MAC             User             Addr IP        Authentication User Network
Port  Address         Name             Vlan Mode Address       Type Result Profile Name
-----+----------------+----------------+----+----+---------------+----+----+---------------
 3/ 1 00:00:00:00:00:01   000000000001   10 Brdg -           MAC  Pass          unp
```

show aaa-device mac-address <mac-address>

Usage Guidelines:

It is an existing command that can be used to display the detailed information about the non-supplicant clients. The below show command is modified to display the user-name. The 'user-name'

column displays the user-name entered through MAC authentication if the classified non-supplicant user belongs to user-network-profile for a particular port.

Example:

```
➔  show aaa-device mac-address 00:00:00:00:88:54

Detail status for device:
  MAC Address                    = 00:00:00:00:88:54
  IP Address                     = None.
  Port                           = 1/1
  Authentication Type            = MAC Authentication
  Authentication Result          = Successful
  Classification Policy          = VLAN ID
  VLAN Learned on                = 10  (SUN FEB 11 2001  00:26:52 (UTC))
  MAC Address Mode Learnt on System  = Bridging
  UserName                               = 000000008854
  HIC                            = no
```

Limitations:
None

3. Clear Command for DHCP Snooping violation counters and Enhanced DHCP Snooping Troubleshooting

Platforms Supported: OmniSwitch 6450 and OmniSwitch 6350

Hosted AOS SW Release: 672.85.R01

In production network, troubleshooting DHCP and ISF is a pain area since not much information is available from CLI. The current debug logs available with swlog and systrace are not much helpful since it prints too many logs and is not easily interpretable to an end user. This enhancement focus is on providing new CLI debug and show commands that can help an end customer to troubleshoot the DHCP snooping feature easily.

Usage:

a. ip helper dhcp-snooping clear violation-counters {all | slot <num> | linkagg <num> | <slot/port> | <slot/port1-port2>}

This command is used to clear DHCP snooping violation counters

Usage Guidelines:

all	Clear DHCP snooping violation counters on all ports.
<slot/port>	Clear DHCP snooping violation counter for the specified physical port.
<slot/port1-port2>	Clear DHCP snooping violation counter for the specified physical port range.
slot <num>	Clear DHCP snooping violation counter for all port of the specified slot.
linkagg <num>	Clear DHCP snooping violation counter for the specified linkagg.

b. debug dhcp admin-status {enable | disable}

Usage Guidelines:

enable	Enable DHCP on demand debugging globally.
disable	Disable DHCP on demand debugging globally

c. debug dhcp {mac-address <MAC-ADDRESS> | port <PORT-ID> | linkagg <LINKAGG-ID>} [vlan <VLAN-ID>] <cr>

Usage Guidelines:

mac-address	*Specifies the client for which the transactions needs to be logged.*
port	*Specifies the port on which DHCP transactions should be logged.*
linkagg	*Specifies the linkagg on which DHCP transactions should be logged.*
Vlan	*Specifies the VLAN on which the clients are connected. If vlan is not specified, clients on all VLANs on the specified port/linkagg/MAC will be logged.*

d. debug dhcp dump-packet admin-status {enable | disable}

Usage Guidelines:

enable	*Enables DHCP packet dump for the clients which are monitored.*
disable	*Disables DHCP packet dump for the clients which are monitored.*

e. debug show dhcp

This command displays the logs collected. Maximum log line length will be 160 characters and maximum number of logs will be 600 lines.

Sample Output:

```
-> debug dhcp admin-status enable
-> debug dhcp mac-address 11:22:33:44:55:66 vlan 100
-> debug dhcp dump-packet admin-status enable

-> debug show dhcp

Debug Configurations:
------------------------------------------------------
DHCP Debug          : Enabled
DHCP Packet Dump     : Enabled
Debugging on         : MAC: 11:22:33:44:55:66
Debugging on VLAN    : 100
DHCP Snooping Status : Switch Level Enabled

Date      Time       Log Message
---------+----------+------------------------------------------------------------------------------
12/18/00  22:18:39   In enqueue_to_ip_using_ipc:2847: DHCP Discovery: Received in
DHCP Application:Port:1/47, Mac:11:22:33:44:55:66 VLAN:100
12/18/00  22:18:39   In enqueue_to_ip_using_ipc:2847: DHCP Packet Dump:
ff ff ff ff ff e8 e7 32 76 85 a4 81 00 00 64 08 00 45 00 01 48 00 00 00
00 40 11 f2 e0 c3 c3 c3 01 ff ff ff ff 00 43 00 44 01 34 6f 5d 02 01 06
00 00 00 00 00 00 00 00 00 00 00 00 c3 c3 c3 0a c3 c3 c3 01 00 00 00
00 e8 e7 32 1f 1d 9e 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00 00
```

1/18/15 2:12:40 In udprelayProcessDHCPSnooping:6008: DHCP Discovery: Processing Successfull: Port:1/47, Mac: 11:22:33:44:55:66 VLAN: 100
1/18/15 2:12:40 In udprelayProcessDHCPSnoopingInRequest:6533: DHCP Discovery Received From: Port 1/47 Mac: 11:22:33:44:55:66 VLAN: 100.

Limitations:

1. All log are limited in size and log size is not configurable.
2. ISF packet logging and counters are limited to the packet sampling (64 Kbits/sec) done in hardware for logging.

4. Control Directed Broadcasts - Wake on LAN

Platforms Supported: OmniSwitch 6450 and OmniSwitch 6350

Hosted AOS SW Release: 672.85.R01

IP directed-Broadcast is globally controlled by *"ip directed-broadcast enable|disable"*. When ip directed-broadcast is enable, packet is processed by software and flooded on the destination vlan. If the ip directed-broadcast is disabled, then the broadcast packet will not be processed. The Control Directed broadcast – wake ON LAN is to direct only the packet from trusted source to the destined network, while the other directed broadcast packets are dropped. To implement the control directed broadcast, the user need to define the set of source-ip, destination-ip and vlan information.

For example after enabling the control directed broadcast mode by using the command "ip directed-broadcast controlled" & if the user is written the rule in CLI like "ip directed-broadcast allow source-ip 192.168.0.2/24 destination-ip 192.169.0.255/24", then all the broadcast packet from that source ip 192.168.0.2 will be processed by the Software and flooded in to destination network.

Usage:

a. ***ip directed-broadcast {on | off | controlled}***
This command is used to enable or disable the ip directed broadcast control mode.

Syntax Definitions:
ON : Enable IP directed broadcast.
OFF : Disable IP directed broadcast.
Controlled : Enable IP directed broadcast controlled mode.

Usage Guidelines:
1. If the controlled mode is set then the user needs to mention the trusted information such as source-ip, destination-ip and vlan information to broadcast the packet. If the information is not specified then all the broadcast packets will not be processed.

b. ip directed-broadcast allow {source-ip <ipv4_address> [mask <subnet_mask>]} {destination-ip <ipv4_address> [mask <subnet_mask>]} {vlan <vlan_num>}

This command is used to configure the particular rule to process the particular broadcast packet in to destination network, ie source ip with subnet mask and destination ip with subnet mask and destination vlan.

Syntax Definitions:
{source-ip <ipv4_address> [mask <subnet_mask>]} : Source ip with source subnet mask of the broadcast packet.

{destination-ip <ipv4_address> [mask <subnet_mask>]} : Destination ip with destination subnet mask to which broadcast packet to be flooded into the destination network.

{vlan <vlan_num>} : Destination vlan where the broadcast packet to be flooded.

Usage Guidelines:

1. The Ip directed broadcast command will be made to broadcast the packets in controlled manner by specifying the source-ip, destination-ip and vlan information. The specified information are considered as the trusted information to broadcast the packets which are received only from the defined source and the remaining broadcast packets will be dropped.

2. User can configure up to 32 source ip and each source can have 30 destination ip and vlan information's. The global variable "ipedr_cdb_max_entry" will be set to 32 to maintain the IP entries in the switch, this can be modified to define the max entries.

c. ***no ip directed-broadcast {source-ip <ipv4_address>}***
This command is used to remove particular ip directed broadcast entry in CLI. While removing a particular source IP, all the 30 destination IPs that are mapped to that same source IP are also removed.

Syntax Definitions:
{source-ip <ipv4_address>} : Source ip of the particular rule to be removed.
Usage Guidelines:
1. The command to remove the trusted information configured with the source-ip for controlled ip directed-broadcast.

d. *ip directed-broadcast clear*
This Command to clear all the trusted information configured at once.

e. *show ip config*
This command is used to display all configured directed broadcast control mode entries.

Usage Guidelines:
1. The show ip config command is modified to display the source-ip, destination-ip and vlan information of the control directed-broadcast. Each row will have each source-ip and the respective destination and vlan information defined. The non-defined parameters will be mentioned as '-'. The show output would display all the configured control directed broadcast entries irrespective of ip directed broadcast mode

Limitations:
1. The ingress/egress rate for the directed broadcast is ~700 pkts/sec for an interface configured. Increasing above could result in CPU spike and packet drops.

2. If the destination IP is not reachable or if the destination subnet is not directly connected, packet will be dropped.

3. Feature is rate limited to ~850 packets per interface. When the packets are sent at line rate, packets higher than rete limit will be dropped.

4. Controlling of Broadcast packet through vlan stacking will not be support