Aruba Networks | Mobility Access Switch

Troubleshooting Basic L2/L3 and Role-Based Access

Based on AOS 7.2 | Created by Tim Cappalli

BASIC L2 / L3 TROUBLESHOOTING

> ARP TABLE

`show arp`

local L3 interfaces
(on stack)

```
Protocol    IP Address      Hardware Address    Interface
---------   ----------      ----------------    ---------
* Internet  172.30.67.8     00:0b:86:6c:b7:80   mgmt
* Internet  10.  .2         00:0b:86:6c:b7:80   vlan100
* Internet  129.  .1        00:0b:86:6c:b7:80   vlan11
* Internet  10.  .2         00:0b:86:6c:b7:80   vlan200
* Internet  10.  .8.1       00:0b:86:6c:b7:80   vlan21
* Internet  10.  .8.1       00:0b:86:6c:b7:80   vlan64
* Internet  10.  .8.1       00:0b:86:6c:b7:80   vlan66
* Internet  10.  .8.1       00:0b:86:6c:b7:80   vlan69
* Internet  10.  .8.1       00:0b:86:6c:b7:80   vlan70
* Internet  129.  .65       00:0b:86:6c:b7:80   vlan71
  Internet  172.30.67.5     90:B1:1C:           mgmt
  Internet  10.  .8.19      00:20:4a:           vlan64
  Internet  10.  .8.56      00:c0:b7:           vlan64
  Internet  10.  .8.79      18:ef:63:           vlan64
```

> MAC ADDRESS TABLE / CAM TABLE

`show mac-address-table`

```
Total MAC address: 187
Learnt: 20, Static: 0, Auth: 167, Phone: 0

MAC Address Table
-----------------
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  ----------------
00:01:e6:   :     /  Auth          0011  GE4/0/18
00:05:b9:   :4    e  Auth          0011  GE4/0/6
00:0c:29:   :6    1  Auth          0011  GE4/0/3
00:10:83:   :f    4  Auth          0011  GE0/0/17
00:11:0a:   :7    4  Auth          0011  GE3/0/30
00:13:72:   :d    1  Auth          0011  GE4/0/5
00:13:72:   :4    4  Auth          0011  GE5/0/12
00:13:72:   :5    8  Auth          0011  GE3/0/14
00:14:38:   :e    1  Auth          0011  GE7/0/18
00:14:38:   :5    5  Auth          0011  GE2/0/39
00:14:38:   :d    8  Auth          0011  GE2/0/20
00:16:cb:   :f    d  Auth          0011  GE4/0/11
00:16:cb:   :1    0  Auth          0011  GE7/0/15
00:17:f2:   :b    4  Auth          0011  GE1/0/43
00:19:b9:   :1    a  Auth          0011  GE5/0/0
00:1b:78:   :7    f  Auth          0011  GE3/0/17
```

> MAC LEARNING LOGS

`show mac-learning-log`

This command will give you a log of recent MAC addresses that were learned on a specific port. It can be handy when trying trace an issue back a few days.

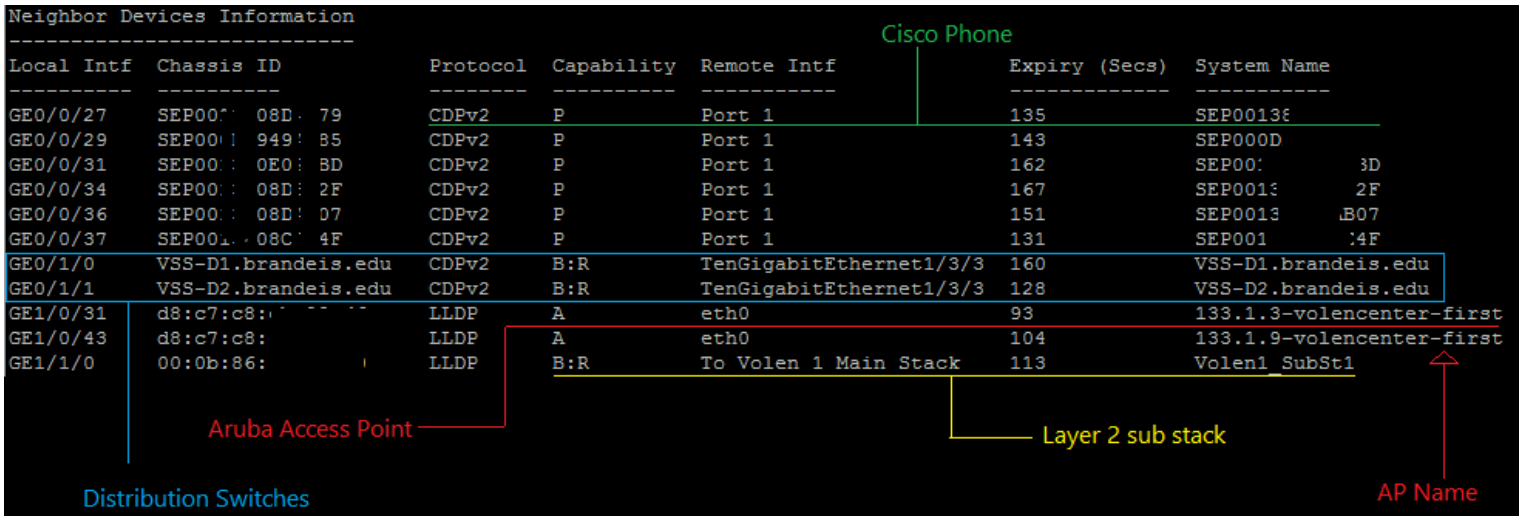
TIP: add " | include <macaddress>" after the command to search a single MAC
`(show mac-learning-log | include ab:cd:ef:12:34:56)`

```
MAC Learning Logs
-----------------
Time             Log
----             ---
Dec 13 06:05:53  Vlan 71, MAC b8:ca:3a:[illegible], Learnt on Pc10
Dec 13 06:07:26  Vlan 71, MAC b8:ca:3a:[illegible], Aged
Dec 13 06:07:48  Vlan 71, MAC b8:ca:3a:[illegible], Learnt on Pc10
Dec 13 06:08:04  Vlan 71, MAC b8:ca:3a:[illegible], Learnt on Pc10
Dec 13 06:19:16  Vlan 71, MAC f8:b1:56:[illegible], Learnt on Pc10
Dec 13 06:20:23  Vlan 71, MAC b8:ca:3a:[illegible], Learnt on Pc10
Dec 13 07:53:09  Vlan 71, MAC b8:ca:3a:[illegible], Aged
Dec 13 07:53:37  Vlan 71, MAC b8:ca:3a:[illegible], Learnt on Pc10
Dec 13 08:01:36  Vlan 71, MAC b8:ca:3a:[illegible], Aged
Dec 13 08:10:08  Vlan 71, MAC b8:ca:3a:[illegible], Learnt on Pc10
Dec 13 08:17:17  Vlan 71, MAC b8:ca:3a:[illegible], Aged
Dec 13 08:17:54  Vlan 71, MAC b8:ca:3a:[illegible], Learnt on Pc10
Dec 13 08:18:20  Vlan 71, MAC b8:ca:3a:[illegible], Aged
Dec 13 08:18:25  Vlan 71, MAC b8:ca:3a:[illegible], Aged
```

> NEIGHBOR DEVICES

`show neighbor-devices`

This command is a personal favorite. It will show you all LLDP and CDP neighbors and some basic information about each neighbor. Aruba APs will show you the AP name under the system name column.



AUTHENTICATION SERVERS

> AUTHENTICATION SERVER STATUS

```
show aaa authentication-server all
```

```
Auth Server Table
-----------------
Name                        Type    FQDN  IP addr          AuthPort  AcctPort  Status   Requests
----                        ----    ----  -------          --------  --------  ------   --------
Internal                    Local   n/a   127.0.0.1        n/a       n/a       Enabled  0
CLEAR-PASS-PROD1-B          Radius  none  1[illegible]       1812      1813      Enabled  60759
CLEAR-PASS-PROD2-B          Radius  none  12[illegible]      1812      1813      Enabled  11
NETREG-RADIUS-PROD-B        Radius  none  1[illegible]       1812      1813      Enabled  0
TACACS-SERVER-CPPM-AUTH1-B  Tacacs  n/a   1[illegible]       49        n/a       Enabled  1534
TACACS-SERVER-CPPM-AUTH2-B  Tacacs  n/a   12[illegible]  2   49        n/a       Enabled  29
Total:6
```

> RADIUS SERVER STATISTICS

```
show aaa authentication-server radius statistics
```

```
RADIUS Server Statistics
------------------------
Statistics              CLEAR-PASS-PROD1-B  CLEAR-PASS-PROD2-B
----------              ------------------  ------------------
Accounting Requests     0                   0
Raw Requests            0                   0
PAP Requests            60713               13
CHAP Requests           0                   0
MS-CHAP Requests        0                   0
MS-CHAPv2 Requests      0                   0
Mismatch Response       1                   0
Bad Authenticator       0                   0
Access-Accept           60529               11
Access-Reject           178                 0
Accounting-Response     0                   0
Access-Challenge        0                   0
Unknown Response code   0                   0
Timeouts                30                  8
AvgRespTime (ms)        35                  6206
Total Requests          60713               13
Total Responses         60708               11
Uptime (d:h:m)          0:17:20             0:17:10
SEQ Total/Free          255/255             255/255
Orphaned requests = 0
```

ROLE-BASED ACCESS

> THE “GO-TO” COMMAND FOR ROLE-BASED ACCESS (UNTRUSTED)

`show user-table`

```
Users
-----
    IP              MAC            Name            Role              Age(d:h:m)  Auth  VPN link  AP name  Roaming  Essid/Bssid/Phy  Profile
----------    ------------       ------            ----              ----------  ----  --------  -------  -------  ---------------  -------
10.[redacted].227  64:d9:89:[redacted]  noc  CISCO-PHONE-ROLE-B  120:07:36  MAC  2/0/35  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].231  00:26:99:[redacted]:d5  noc  CISCO-PHONE-ROLE-B  120:07:35  MAC  7/0/3  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].238  b4:a4:e3:[redacted]:ee  noc  CISCO-PHONE-ROLE-B  120:07:43  MAC  3/0/4  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].244  54:78:1a:[redacted]:db  noc  CISCO-PHONE-ROLE-B  120:07:43  MAC  0/0/12  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].246  04:fe:7f:[redacted]:07  noc  CISCO-PHONE-ROLE-B  57:23:36  MAC  7/0/17  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].250  c0:62:6b:[redacted]:3c  noc  CISCO-PHONE-ROLE-B  120:07:43  MAC  4/0/19  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].44  9c:1c:12:[redacted]:b8  noc  AP-ROLE-B  64:04:29  MAC  7/0/14  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].60  9c:1c:12:[redacted]:32  noc  AP-ROLE-B  64:00:58  MAC  1/0/37  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].61  9c:1c:12:[redacted]:a0  noc  AP-ROLE-B  64:07:15  MAC  5/0/15  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].64  9c:1c:12:[redacted]:7c  noc  AP-ROLE-B  66:06:05  MAC  1/0/1  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].66  9c:1c:12:[redacted]:a8  noc  AP-ROLE-B  64:07:06  MAC  1/0/41  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].103  9c:1c:12:[redacted]:70  v[redacted]  AP-ROLE-B  66:06:09  MAC  6/0/13  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].127  9c:1c:12:[redacted]:18  noc  AP-ROLE-B  64:04:30  MAC  6/0/14  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].135  9c:1c:12:[redacted]:8a  noc  AP-ROLE-B  64:07:09  MAC  1/0/39  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].137  9c:1c:12:[redacted]:22  noc  AP-ROLE-B  64:07:05  MAC  0/0/21  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].140  9c:1c:12:[redacted]:82  noc  AP-ROLE-B  66:06:11  MAC  0/0/20  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].141  9c:1c:12:[redacted]:9c  noc  AP-ROLE-B  64:07:14  MAC  3/0/47  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].143  9c:1c:12:[redacted]:78  noc  AP-ROLE-B  64:07:02  MAC  3/0/44  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].144  9c:1c:12:[redacted]:a4  noc  AP-ROLE-B  64:07:12  MAC  2/0/16  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].147  9c:1c:12:[redacted]:5c  noc  AP-ROLE-B  42:05:58  MAC  5/0/16  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].152  9c:1c:12:[redacted]:ec  noc  AP-ROLE-B  64:07:08  MAC  3/0/46  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].153  9c:1c:12:[redacted]:38  noc  AP-ROLE-B  66:06:06  MAC  7/0/22  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].162  9c:1c:12:[redacted]:96  noc  AP-ROLE-B  25:05:22  MAC  0/0/22  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted].233  9c:1c:12:[redacted]:6a  noc  AP-ROLE-B  58:02:51  MAC  0/0/0  Wired  UNTRUSTED-AAA-PROFILE-B
10.[redacted]55.2  00:16:cb:[redacted]:dc  ga[redacted]  ACCESS-ROLE-B  00:00:00  MAC  4/0/11  Wired  UNTRUSTED-AAA-PROFILE-B
129.[redacted].13  00:22:19:[redacted]:20  jr[redacted]n  ACCESS-ROLE-B  36:03:47  MAC  2/0/24  Wired  UNTRUSTED-AAA-PROFILE-B
129.[redacted].18  00:0c:29:[redacted]  n[redacted]a  ACCESS-ROLE-B  21:04:04  MAC  4/0/3  Wired  UNTRUSTED-AAA-PROFILE-B
```

+ Some useful options for the command:

`show user-table role <rolename>` [show users in role]

```
(Feldberg_ST1) #show user-table role AP-ROLE-B

Users
-----
    IP          MAC              Name    Role       Age(d:h:m)  Auth  VPN link  AP name  Roaming
----------   ------------       ------   ----       ----------  ----  --------  -------  -------
10.[redacted].44  9c:1c:12:[redacted]:b8  noc  AP-ROLE-B  64:04:38  MAC   7/0/14  Wired
10.[redacted]6.[redacted].60  9c:1c:12:[redacted]:32  noc  AP-ROLE-B  64:01:07  MAC   1/0/37  Wired
10.[redacted]6.[redacted].61  9c:1c:12:[redacted]:a0  noc  AP-ROLE-B  64:07:24  MAC   5/0/15  Wired
10.[redacted]6.[redacted].64  9c:1c:12:[redacted]:7c  noc  AP-ROLE-B  66:06:14  MAC   1/0/1   Wired
10.[redacted]6.[redacted].66  9c:1c:12:[redacted]:a8  noc  AP-ROLE-B  64:07:15  MAC   1/0/41  Wired
```

`show user-table ip <ipaddress>` [show details for IP]

```
(Feldberg_ST1) #show user-table ip 129.64.

Name: cappalli, IP: 129.64.  , MAC: 90:b1:1c:  , Role:ACCESS-ROLE-B, ACL:39/0/40, Age: 32:02:23
Authentication: Yes, status: started, method: MAC, protocol: PAP, server: CLEAR-PASS-PROD1-B
Bandwidth = No Limit
Bandwidth = No Limit
Role Derivation: Aruba VSA
VLAN Derivation: VLAN Defined in Derived Role
Idle timeouts: 0, ICMP requests sent: 0, replies received: 0
Mobility state: Wired, HA: Yes, Proxy ARP: No, Roaming: No Tunnel ID: 0 L3 Mob: 0
Flags: internal=0, trusted_ap=0, l3auth=0, mba=1
Flags: innerip=0, outerip=0, guest=0, nodatapath=0, wispr=0
Phy_type: Wired, reauth: 0, BW Contract: up:0 down:0, user-how: 1
Vlan default: 1, Assigned: 11, Current: 11 vlan-how: 6
Mobility Messages: L2=0, Move=0, Inter=0, Intra=0, ProxyArp=0, Flags=0x0
SlotPort=0x214d, Port=0x214d (5/0/13)
Role assigment - L3 assigned role: n/a, VPN role: n/a, Dot1x cached role : n/a
    Current Role name: ACCESS-ROLE-B, role-how: 7, L2-role: ACCESS-ROLE-B, L3-role: ACCESS-ROLE-B
Essid: , Bssid:  AP name/group: 5/0/13/ Phy-type: Wired
RadAcct sessionID:n/a, Start TS: n/a
User stats (packets/bytes) In:16449846/6004473361 Out:0/0
Timers: ping_reply 0, spoof reply 0, reauth 0
Profiles AAA:UNTRUSTED-AAA-PROFILE-B, dot1x:, mac:MAC-AUTH-B CP: def-role:'denyall' sip-role:'' via-auth
ncfg flags udr 0, mac 1, dot1x 0, RADIUS interim accounting 0
IP Born: 1384184466 (Mon Nov 11 10:41:06 2013)
Core User Born: 1384184457 (Mon Nov 11 10:40:57 2013)
Upstream AP ID: 0, Downstream AP ID: 0
DHCP assigned IP address 129.64.  , from DHCP server 0.0.0.0
Acctauth = 1
Session Timeout from Radius: No, Session Timeout Value: 0
```

`show user-table mac <macaddr>` [show entries matching MAC]

```
(Feldberg_ST1) #show user-table mac 00:14:38:

Users
-----
    IP            MAC             Name      Role             Age(d:h:m)   Auth
----------   ------------       ------    ----             ----------   ----
129.64.      00:14:38:6         tu:       PRINTER-ROLE-B   64:02:32     MAC
```

> ACCESS RIGHTS FOR USER ROLE

`show rights <role-name>`

```
(Feldberg_ST1) #show rights AP-ROLE-B

Derived Role = 'AP-ROLE-B'

 L2TP Pool = default-l2tp-pool
 PPTP Pool = default-pptp-pool
 Assigned VLAN = 66
 Periodic reauthentication: Disabled
 ACL Number = 43/0/44
 Max Sessions = 65535
access-list List
----------------
Position  Name      Type       Location
--------  ----      ----       --------
1         AP-ACL-B  stateless
AP-ACL-B
--------
Priority  Source                    Destination               Service   Action  TimeRange
--------  ------                    -----------               -------   ------  ---------
1         10.(    .0 255.255.255.0  AP-DEST-B                 any       permit
2         0.0.0.0                   255.255.255.255           svc-dhcp  permit
3         any                       10.[illegible].0 255.255.255.0  any       permit
4         any                       10.2[illegible].0 255.255.255.0  any       permit
5         any                       10.2[illegible].0 255.255.255.0  any       permit
6         any                       129.[illegible].0 255.255.255.0  any       permit
7         any                       any                       any       permit
Expired Policies (due to time constraints) = 0
```

> STATION TABLE

`show station-table`

This command is a good starting point if you see the device in the MAC and ARP tables, but don't see it in user-table. The station table will most likely show that the device is connected but has not authenticated. It's more a "layer 2 device-table" as opposed to the layer 3 user-table.

```
(Feldberg_ST1) #show station-table

Station Entry
-------------
    MAC           Name              Role                 Age(d:h:m)  Auth  AP name  Essid  Phy  Remote  Profile
-----------       ------            ----                 ----------  ----  -------  -----  ---  ------  -------
00:01:e6:    :7b  v       .        PRINTER-ROLE-B       120:08:30   Yes   N/A      " "         No      UNTRUSTED-
00:04:f2:    ':1f  noc              CISCO-PHONE-ROLE-B   09:01:31    Yes   N/A      " "         No      UNTRUSTED-
00:04:f2:    ::00  noc              CISCO-PHONE-ROLE-B   120:08:41   Yes   N/A      " "         No      UNTRUSTED-
00:04:f2:    l:3e  noc              CISCO-PHONE-ROLE-B   46:03:07    Yes   N/A      " "         No      UNTRUSTED-
00:05:b9:    ':e8  wr     1        ACCESS-ROLE-B        120:08:35   Yes   N/A      " "         No      UNTRUSTED-
00:08:30:    .:dc  noc              CISCO-PHONE-ROLE-B   120:08:27   Yes   N/A      " "         No      UNTRUSTED-
00:0c:29:    ':17  nr       .       ACCESS-ROLE-B        21:04:57    Yes   N/A      " "         No      UNTRUSTED-
00:10:83:    .:49  r[illegible]       ACCESS-ROLE-B        115:22:41   Yes   N/A      " "         No      UNTRUSTED-
00:11:0a:    ':45  j[illegible]       ACCESS-ROLE-B        120:07:30   Yes   N/A      " "         No      UNTRUSTED-
```