aruba
a Hewlett Packard
Enterprise company

ARUBA INSTANT DOT1X TROUBLESHOOTING

Technical Climb Webinar

12:00 GMT | 13:00 CET | 15:00 GST
June 21st, 2016

Presenter: Barath Srinivasan

barath.srinivasan@hpe.com

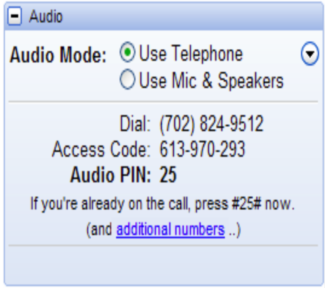
AIRHEADS
COMMUNITY

Welcome to the Technical Climb Webinar

Listen to this webinar using the computer audio broadcasting or dial in by phone.

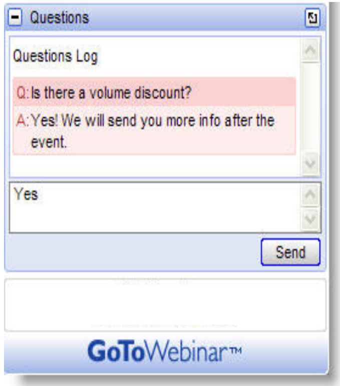
The dial in number can be found in the audio panel, click additional numbers to view local dial in numbers.

If you experience any difficulties accessing the webinar contact us
using the questions panel.



Audio Mode: ● Use Telephone
○ Use Mic & Speakers

Dial: (702) 824-9512
Access Code: 613-970-293
Audio PIN: 25
If you're already on the call, press #25# now.
(and additional numbers ..)



Questions Log

Q: Is there a volume discount?
A: Yes! We will send you more info after the event.

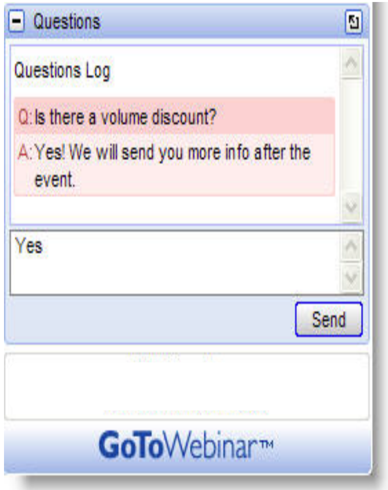
Yes

Housekeeping

This webinar will be recorded

All lines will be muted during the webinar

How can you ask questions?
Use the question panel on your screen



Questions Log

Q: Is there a volume discount?

A: Yes! We will send you more info after the event.

Yes

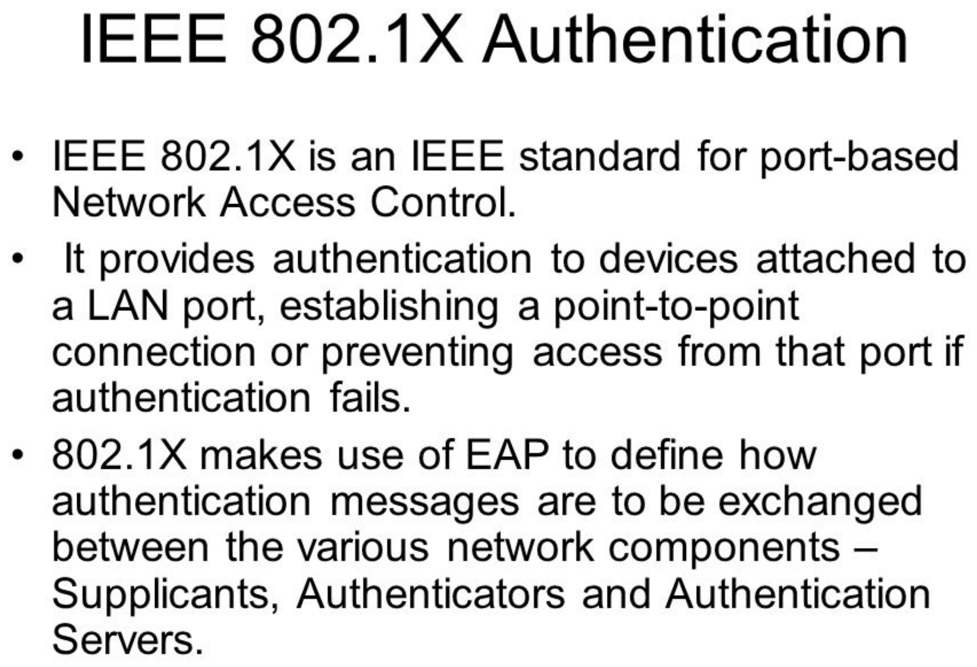
The recorded presentation will be posted on Arubapedia for Partners (https://arubapedia.arubanetworks.com/afp/)

TROUBLESHOOTING 802.1X ISSUES

How to identify, diagnose and debug 802.1x related user authentication issues

a Hewlett Packard Enterprise company

Why 802.1x?



IEEE 802.1X Authentication

- IEEE 802.1X is an IEEE standard for port-based Network Access Control.
- It provides authentication to devices attached to a LAN port, establishing a point-to-point connection or preventing access from that port if authentication fails.
- 802.1X makes use of EAP to define how authentication messages are to be exchanged between the various network components – Supplicants, Authenticators and Authentication Servers.

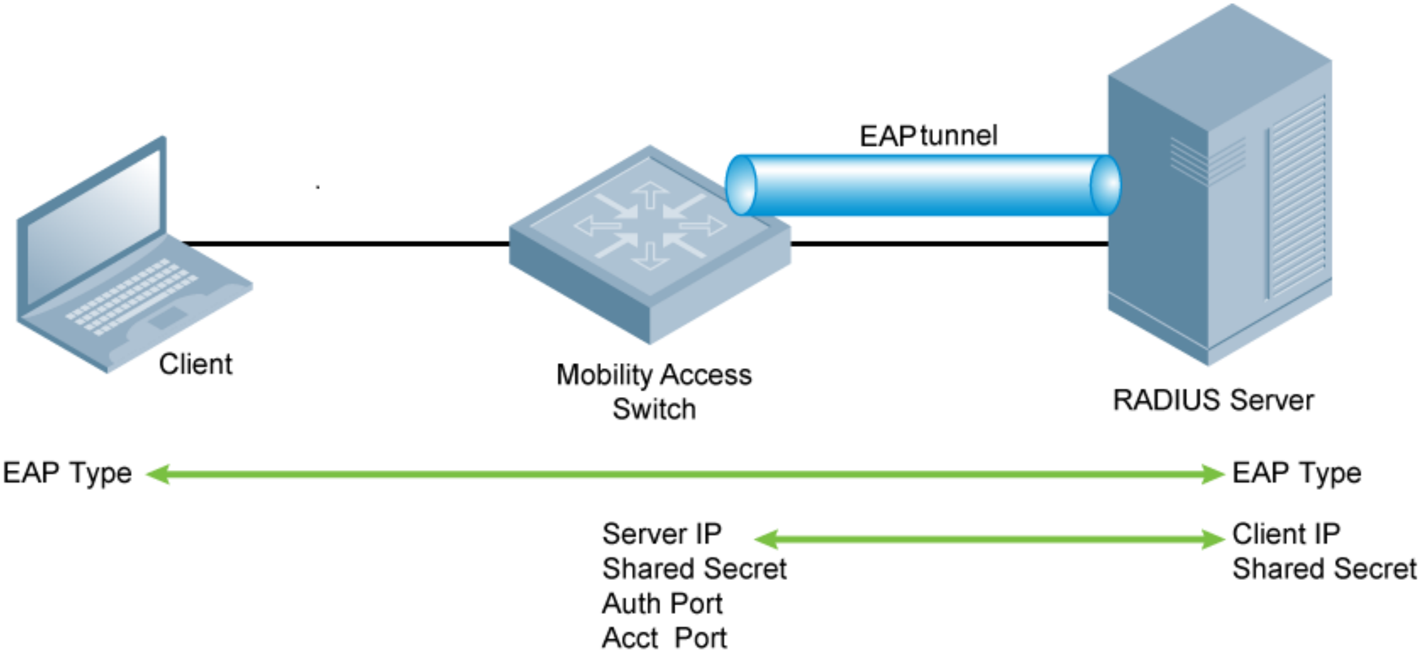
Prerequisites isolating 802.1x client connectivity

Ensure to have the following information made available to you by the End-User or Customer, Before beginning to work on client connectivity issues.

- Nature of the problem – Frequent disconnection, Unable to associate, Does not work in specific area, Low speed, etc
- Magnitude of the issue reported – How many clients are affected, Partial or complete outage
- Client specific information – Mac or IP address, Client device type, OS and driver version, SSID to which client connects
- Replicable – Is the issue replicable consistently or occurs on a random basis
- Deployment History – Was the issue present since deployment? Did the customer do a code upgrade or config change?

Method of troubleshooting approach

The three main entities of 802.1x authentication, troubleshooting begins with isolation of potential symptoms



What are the symptoms reported by users?

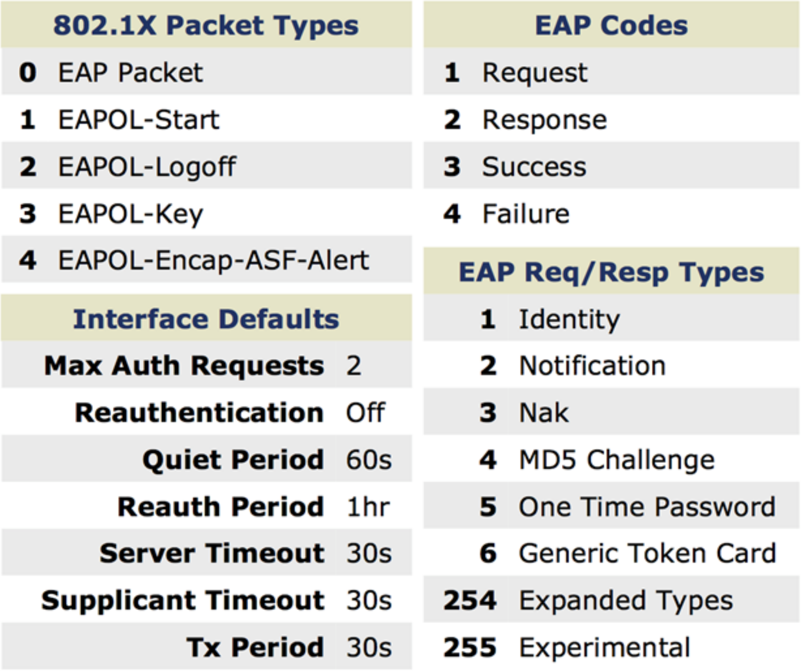
Depending on the type of EAP authentication being performed by the user, they can experience multiple forms of errors, understanding the type of error is a key factor in quickly and efficiently isolating the potential entity which has triggered the issue.

End-User Symptoms:

i.e., Users are being repeatedly asked to enter credentials and they eventually never get connected to the Corp WLAN.

Users get a pop-up which says it is unable to verify the server
Certificate.

Users keep getting dropped off from the WLAN, although they did get associated initially with their credentials.



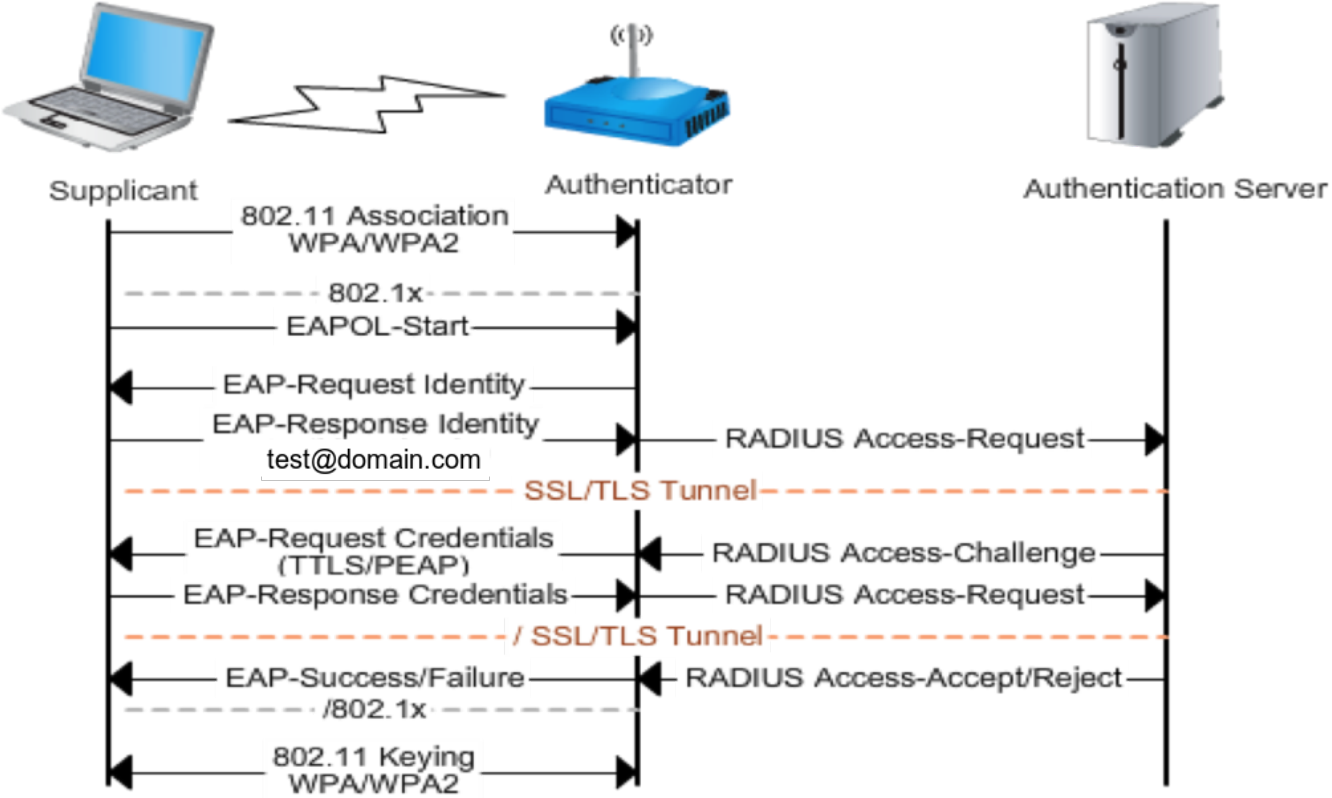
802.1X Packet Types	
0	EAP Packet
1	EAPOL-Start
2	EAPOL-Logoff
3	EAPOL-Key
4	EAPOL-Encap-ASF-Alert

Interface Defaults	
Max Auth Requests	2
Reauthentication	Off
Quiet Period	60s
Reauth Period	1hr
Server Timeout	30s
Supplicant Timeout	30s
Tx Period	30s

EAP Codes	
1	Request
2	Response
3	Success
4	Failure

EAP Req/Resp Types	
1	Identity
2	Notification
3	Nak
4	MD5 Challenge
5	One Time Password
6	Generic Token Card
254	Expanded Types
255	Experimental

Understanding the EAP authentication process



Verifying baseline config on Aruba Instant AP

```
(Instant Access Point) (config)# wlan ssid-profile  <SSID-Name>
(Instant Access Point) (SSID Profile <"profile-name>")# type {<Employee>|<Voice>}

(Instant Access Point) (SSID Profile <"profile-name>")# opmode {<opensystem>  |<wpa2-ae>|<wpa2-psk-aes>|<wpa-
tkip>|<wpa-psk-tkip>|<wpa-tkip>|<wpa2-aes> |<wpa-psk-tkip>|<wpa2-psk-aesstatic-wep>|<dynamic-wep>}

(Instant Access Point) (SSID Profile <"profile-name>")# leap-use-session-key
(Instant Access Point) (SSID Profile <"profile-name>")# termination
(Instant Access Point) (SSID Profile <"profile-name>")# external-server
(Instant Access Point) (SSID Profile <"profile-name>")# auth-server <server-name>
(Instant Access Point) (SSID Profile <"profile-name>")# auth-survivability
(Instant Access Point) (SSID Profile <"profile-name>")# auth-survivability cache-time-out <hours>
(Instant Access Point) (SSID Profile <"profile-name>")# radius-reauth-interval <minutes>
(Instant Access Point) (SSID Profile <"profile-name>")# end
```

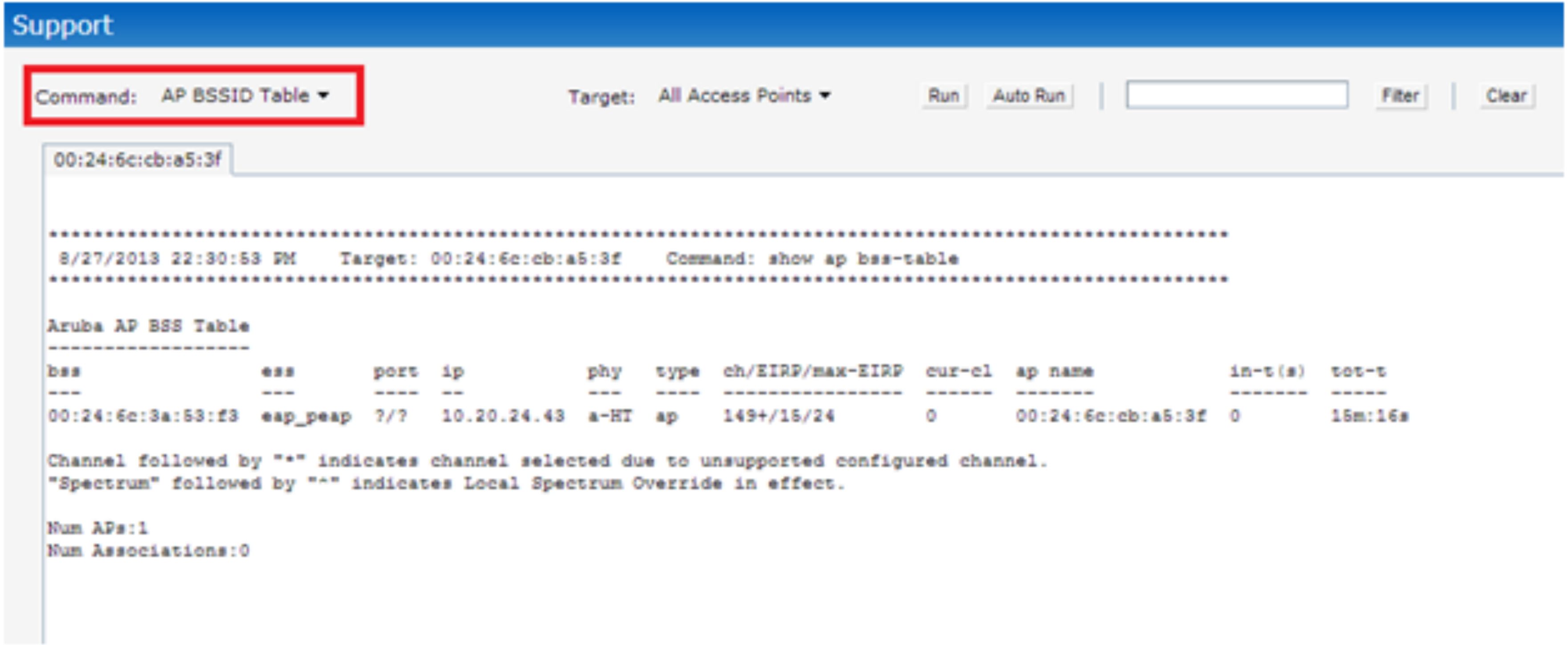
Instant Access point Overview

What should be checked on the Aruba IAP side without fail?

- While configuring a WLAN network for EAP-PEAP authentication, the vlan assignment can be either VC assigned or Network assigned, similar to all other types of authentication.
- The dynamic keys can be WPA/WPA2, Mixed or Dynamic WEP with 802.1x
- EAP - Termination can be optionally enabled on the IAP, by default ‘Disabled’.
- It is possible to upload a customized certificate for 802.1x authentication on the IAP.
- We can use the auth server as RADIUS when EAP Termination is disabled and we can additionally use LDAP as an option when EAP termination is enabled on the AP.

Are users able to view the SSID name?

the command ‘show ap bss-table’ can be run from individual AP’s that have issues

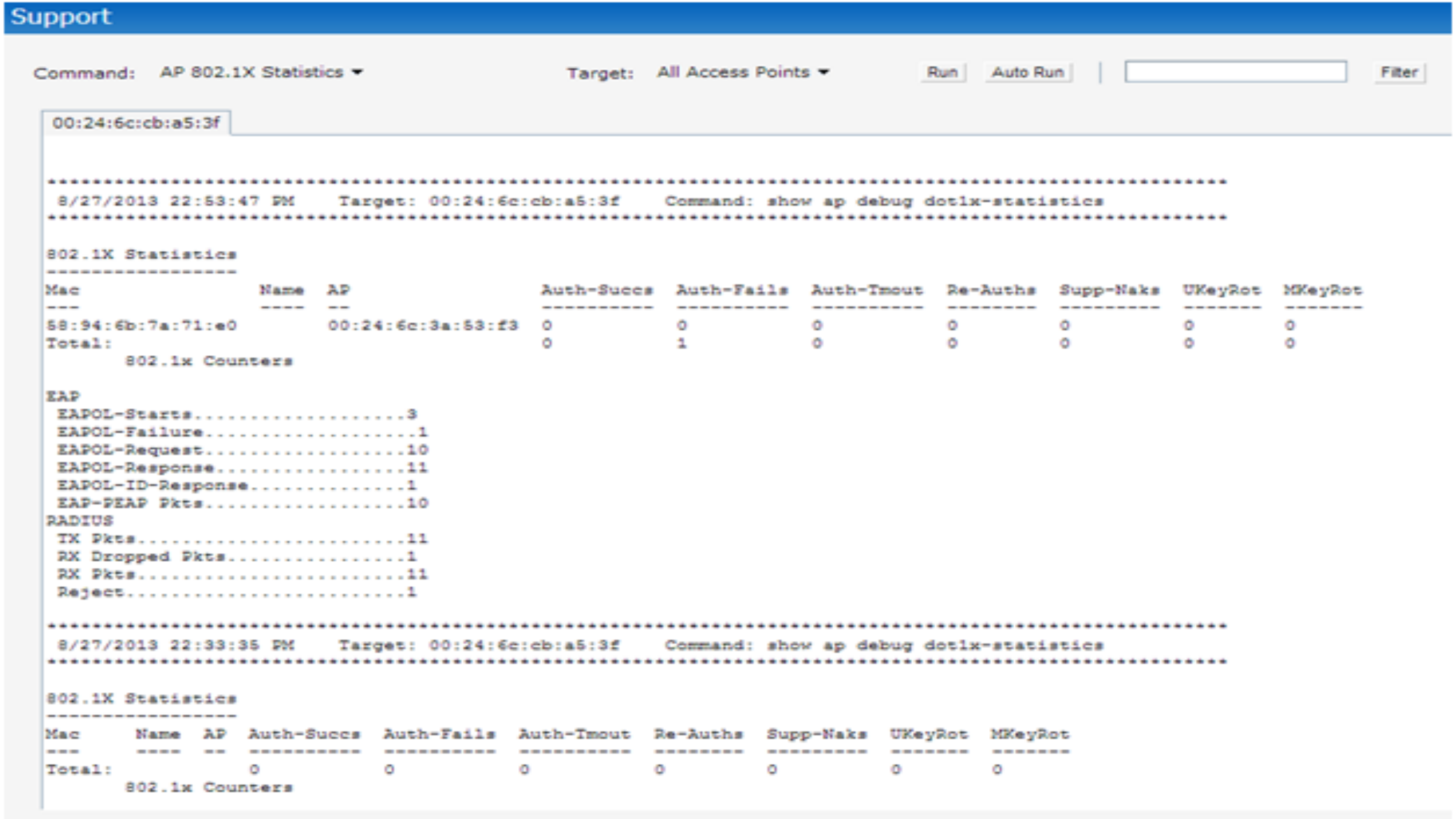


Command: AP BSSID Table

Target: All Access Points

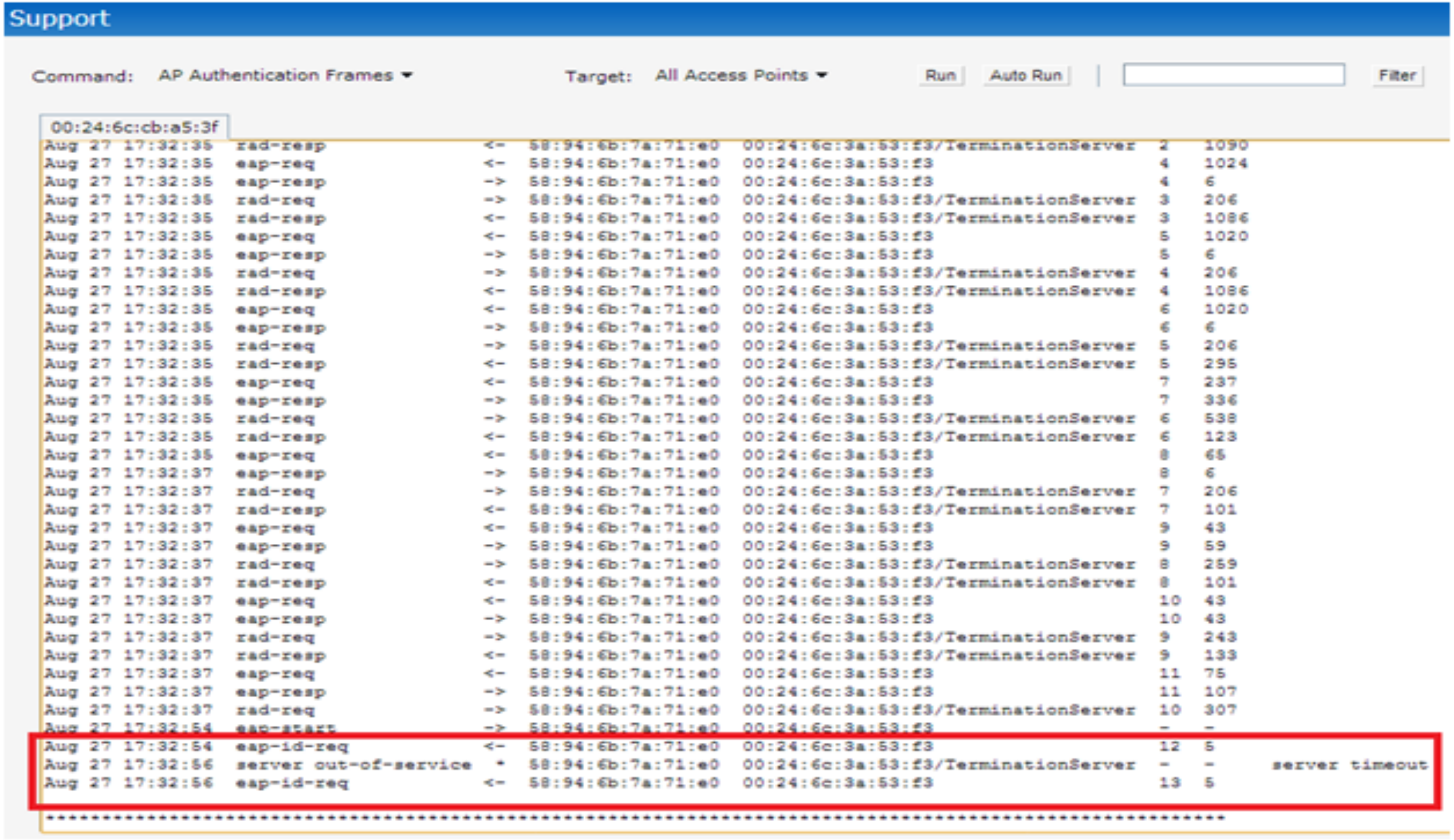
```
****************************************************************************************
 8/27/2013 22:30:53 PM    Target: 00:24:6c:cb:a5:3f    Command: show ap bss-table
****************************************************************************************

Aruba AP BSS Table
------------------
bss                ess       port  ip           phy   type  ch/EIRP/max-EIRP  cur-cl  ap name            in-t(s)  tot-t
---                ---       ----  --           ---   ----  ----------------  ------  -------            -------  -----
00:24:6c:3a:53:f3  eap_peap  ?/?   10.20.24.43  a-HT  ap    149+/15/24        0       00:24:6c:cb:a5:3f  0        15m:16s

Channel followed by "*" indicates channel selected due to unsupported configured channel.
"Spectrum" followed by "^" indicates Local Spectrum Override in effect.

Num APs:1
Num Associations:0
```

What auth-data is the IAP reading from the client?



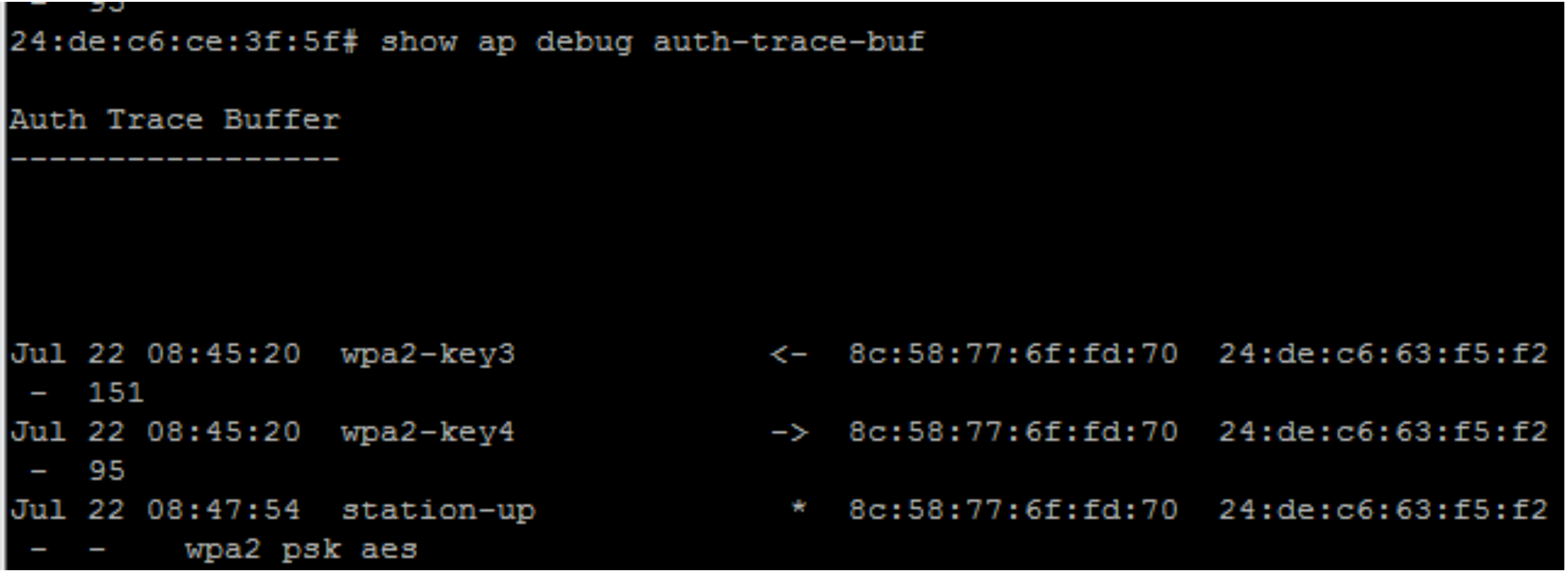
```
*****************************************************************************************
 8/27/2013 22:53:47 PM    Target: 00:24:6c:cb:a5:3f    Command: show ap debug dot1x-statistics
*****************************************************************************************

802.1X Statistics
-----------------
Mac                  Name  AP                 Auth-Succs  Auth-Fails  Auth-Tmout  Re-Auths  Supp-Naks  UKeyRot  MKeyRot
---                  ----  --                 ----------  ----------  ----------  --------  ---------  -------  -------
58:94:6b:7a:71:e0          00:24:6c:3a:53:f3  0           0           0           0         0          0        0
Total:                                        0           1           0           0         0          0        0
       802.1x Counters

EAP
 EAPOL-Starts..................3
 EAPOL-Failure..................1
 EAPOL-Request.................10
 EAPOL-Response................11
 EAPOL-ID-Response.............1
 EAP-PEAP Pkts.................10
RADIUS
 TX Pkts.......................11
 RX Dropped Pkts...............1
 RX Pkts.......................11
 Reject........................1

*****************************************************************************************
 8/27/2013 22:33:35 PM    Target: 00:24:6c:cb:a5:3f    Command: show ap debug dot1x-statistics
*****************************************************************************************

802.1X Statistics
-----------------
Mac     Name  AP  Auth-Succs  Auth-Fails  Auth-Tmout  Re-Auths  Supp-Naks  UKeyRot  MKeyRot
---     ----  --  ----------  ----------  ----------  --------  ---------  -------  -------
Total:            0           0           0           0         0          0        0
       802.1x Counters
```

IAP to RADIUS server communications


Support
Command: AP Authentication Frames ▾
Target: All Access Points ▾
Run
Auto Run
Filter
00:24:6c:cb:a5:3f

```
Aug 27 17:32:35  rad-resp             <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  2   1090
Aug 27 17:32:35  eap-req              <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    4   1024
Aug 27 17:32:35  eap-resp             ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    4   6
Aug 27 17:32:35  rad-req              ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  3   206
Aug 27 17:32:35  rad-resp             <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  3   1086
Aug 27 17:32:35  eap-req              <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    5   1020
Aug 27 17:32:35  eap-resp             ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    5   6
Aug 27 17:32:35  rad-req              ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  4   206
Aug 27 17:32:35  rad-resp             <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  4   1086
Aug 27 17:32:35  eap-req              <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    6   1020
Aug 27 17:32:35  eap-resp             ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    6   6
Aug 27 17:32:35  rad-req              ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  5   206
Aug 27 17:32:35  rad-resp             <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  5   295
Aug 27 17:32:35  eap-req              <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    7   237
Aug 27 17:32:35  eap-resp             ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    7   336
Aug 27 17:32:35  rad-req              ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  6   538
Aug 27 17:32:35  rad-resp             <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  6   123
Aug 27 17:32:35  eap-req              <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    8   65
Aug 27 17:32:37  eap-resp             ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    8   6
Aug 27 17:32:37  rad-req              ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  7   206
Aug 27 17:32:37  rad-resp             <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  7   101
Aug 27 17:32:37  eap-req              <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    9   43
Aug 27 17:32:37  eap-resp             ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    9   59
Aug 27 17:32:37  rad-req              ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  8   259
Aug 27 17:32:37  rad-resp             <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  8   101
Aug 27 17:32:37  eap-req              <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    10  43
Aug 27 17:32:37  eap-resp             ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    10  43
Aug 27 17:32:37  rad-req              ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  9   243
Aug 27 17:32:37  rad-resp             <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  9   133
Aug 27 17:32:37  eap-req              <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    11  75
Aug 27 17:32:37  eap-resp             ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    11  107
Aug 27 17:32:37  rad-req              ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  10  307
Aug 27 17:32:54  eap-start            ->  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    -   -
Aug 27 17:32:54  eap-id-req           <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    12  5
Aug 27 17:32:56  server out-of-service  *  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3/TerminationServer  -   -      server timeout
Aug 27 17:32:56  eap-id-req           <-  58:94:6b:7a:71:e0  00:24:6c:3a:53:f3                    13  5

********************************************************************************************
```

Auth tracing on IAP



```
 -   95
24:de:c6:ce:3f:5f# show ap debug auth-trace-buf

Auth Trace Buffer
-----------------




Jul 22 08:45:20  wpa2-key3            <-  8c:58:77:6f:fd:70  24:de:c6:63:f5:f2
 -   151
Jul 22 08:45:20  wpa2-key4            ->  8c:58:77:6f:fd:70  24:de:c6:63:f5:f2
 -   95
Jul 22 08:47:54  station-up            *  8c:58:77:6f:fd:70  24:de:c6:63:f5:f2
 -   -     wpa2 psk aes
```

Auth tracing on IAP

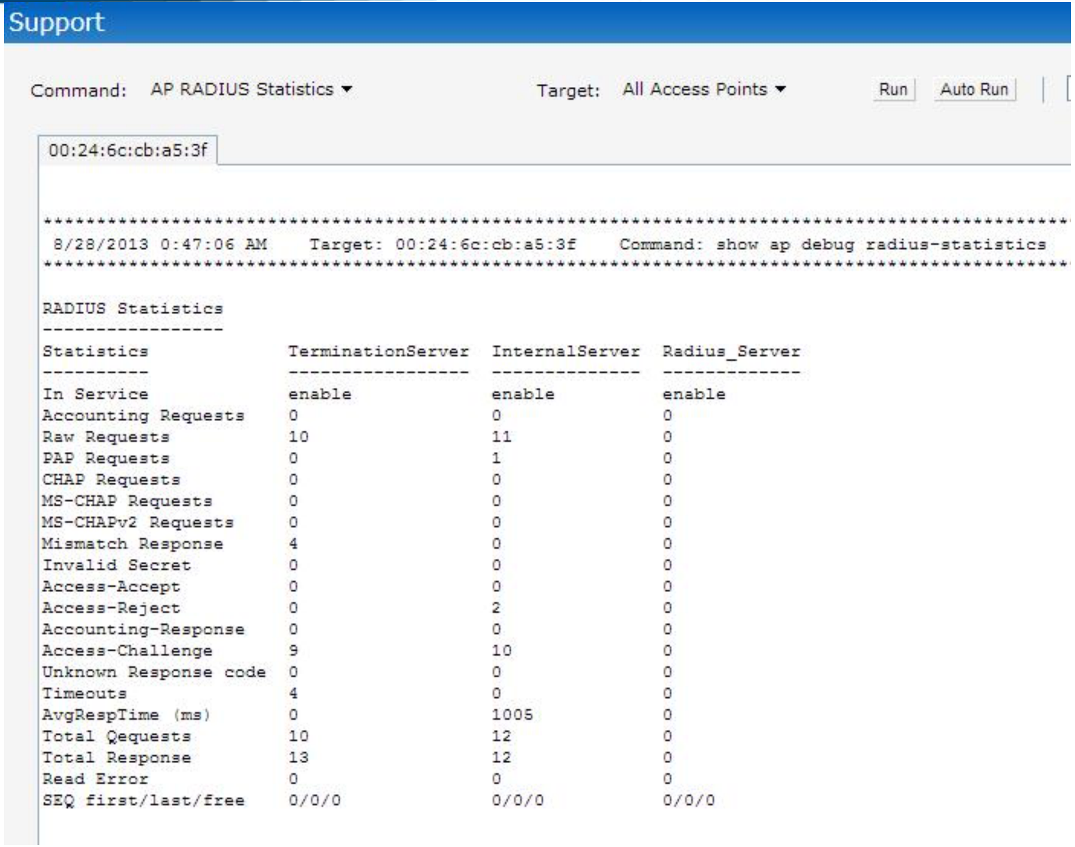
Typical key exchange between AP and client

```
Auth Trace Buffer
-----------------
May 10 13:05:09 station-up * ac:81:12:59:5c:12 d8:c7:c8:3d:42:13 - - wpa2 psk aes
May 10 13:05:09 wpa2-key1 <- ac:81:12:59:5c:12 d8:c7:c8:3d:42:13 - 117
May 10 13:06:30 station-up * 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - - wpa2 psk aes
May 10 13:06:30 wpa2-key1 <- 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 117
May 10 13:06:30 wpa2-key2 -> 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 117
May 10 13:06:30 wpa2-key3 <- 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 151
May 10 13:06:30 wpa2-key4 -> 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 95
May 10 13:07:03 station-up * 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - - wpa2 psk aes
May 10 13:07:03 wpa2-key1 <- 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 117
May 10 13:07:03 wpa2-key2 -> 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 117
May 10 13:07:03 wpa2-key3 <- 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 151
May 10 13:07:03 wpa2-key4 -> 08:ed:b9:e1:51:7d d8:c7:c8:3d:42:12 - 95
```

RADIUS Statistics on Aruba IAP

The key here is to check for whether the RADIUS server which is mapped to the 802.1x authentication service is “IN-SERVICE” or not.

These counters play a key role in terms of identifying server-end communication or authentication issues



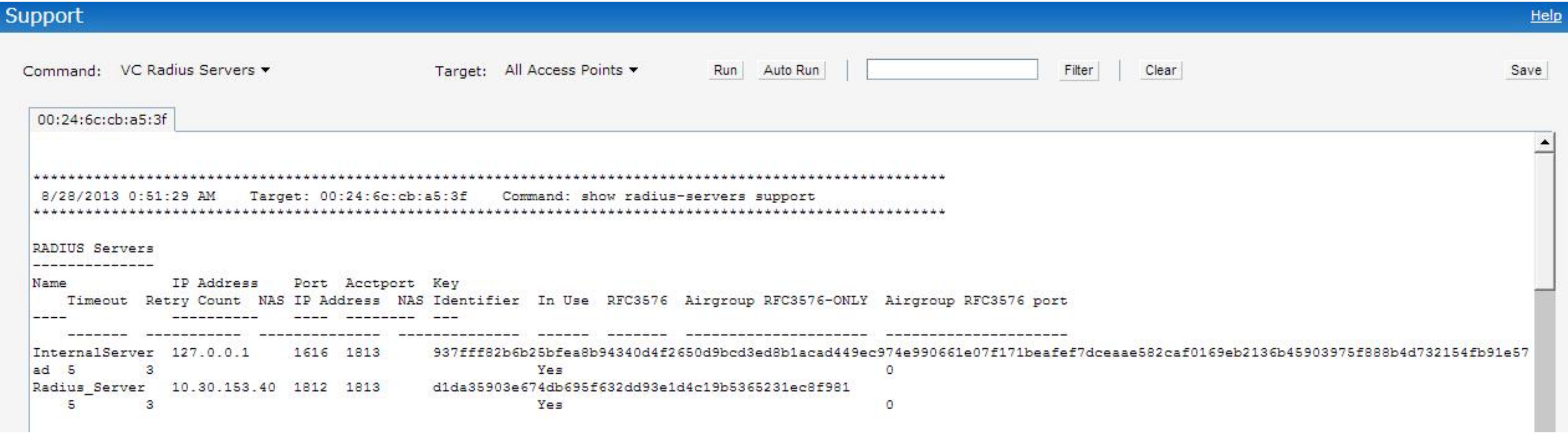
Command: AP RADIUS Statistics

Target: All Access Points

```
********************************************************************************************
 8/28/2013 0:47:06 AM    Target: 00:24:6c:cb:a5:3f    Command: show ap debug radius-statistics
********************************************************************************************

RADIUS Statistics
-----------------
Statistics              TerminationServer  InternalServer  Radius_Server
----------              -----------------  --------------  -------------
In Service              enable             enable          enable
Accounting Requests     0                  0               0
Raw Requests            10                 11              0
PAP Requests            0                  1               0
CHAP Requests           0                  0               0
MS-CHAP Requests        0                  0               0
MS-CHAPv2 Requests      0                  0               0
Mismatch Response       4                  0               0
Invalid Secret          0                  0               0
Access-Accept           0                  0               0
Access-Reject           0                  2               0
Accounting-Response     0                  0               0
Access-Challenge        9                  10              0
Unknown Response code   0                  0               0
Timeouts                4                  0               0
AvgRespTime (ms)        0                  1005            0
Total Qequests          10                 12              0
Total Response          13                 12              0
Read Error              0                  0               0
SEQ first/last/free     0/0/0              0/0/0           0/0/0
```

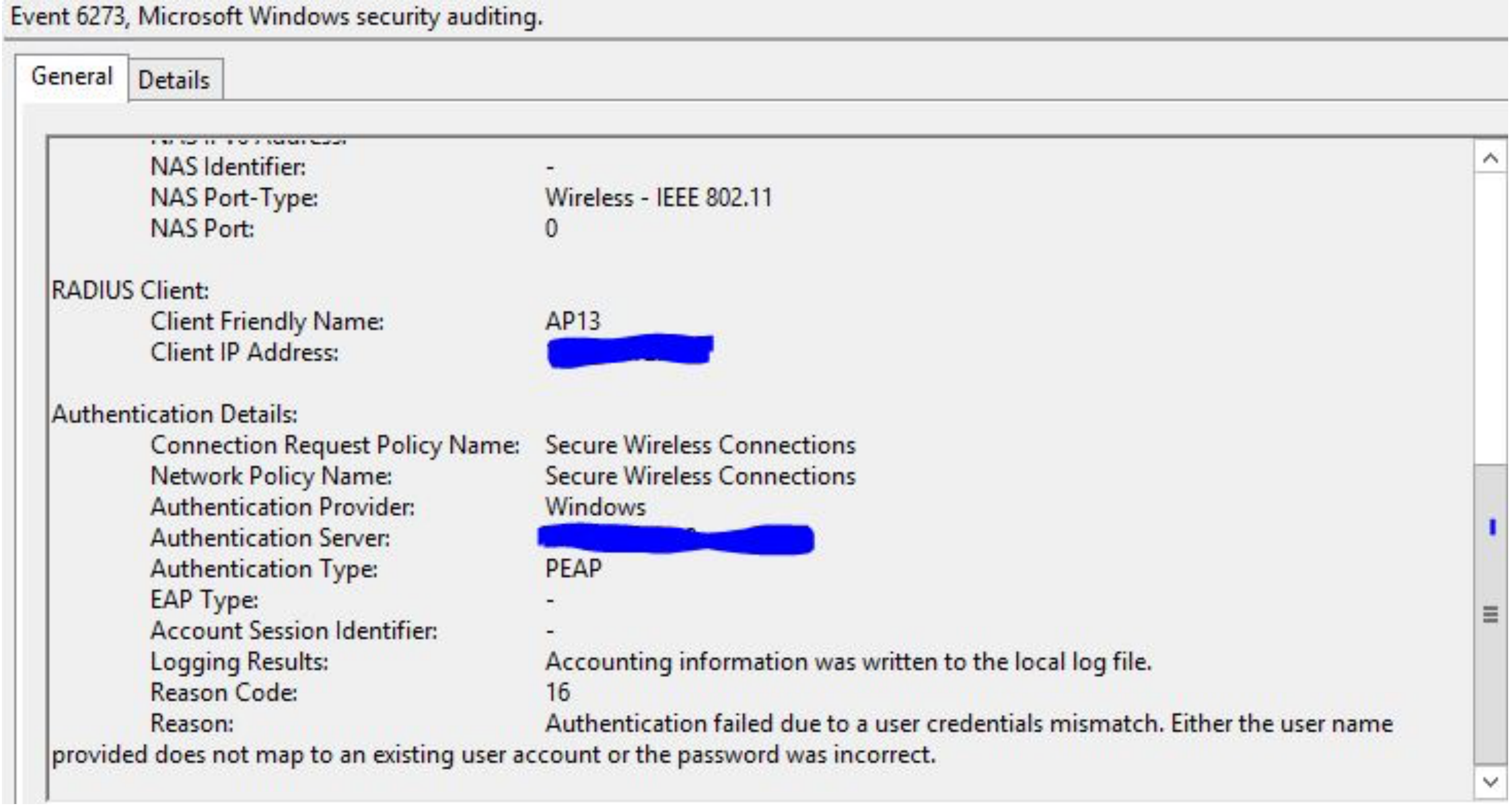
RADIUS Status Overview

RADIUS status overview can be performed using ‘show radius-servers support’



```
*********************************************************************************************************
 8/28/2013 0:51:29 AM    Target: 00:24:6c:cb:a5:3f    Command: show radius-servers support
*********************************************************************************************************

RADIUS Servers
--------------
Name            IP Address    Port  Acctport  Key
    Timeout  Retry Count  NAS IP Address  NAS Identifier  In Use  RFC3576  Airgroup RFC3576-ONLY  Airgroup RFC3576 port
----            ----------    ----  --------  ---
    -------  -----------  --------------  --------------  ------  -------  ---------------------  ---------------------
InternalServer  127.0.0.1     1616  1813      937fff82b6b25bfea8b94340d4f2650d9bcd3ed8b1acad449ec974e990661e07f171beafef7dceaae582caf0169eb2136b45903975f888b4d732154fb91e57
ad  5        3                                              Yes                                     0
Radius_Server   10.30.153.40  1812  1813      d1da35903e674db695f632dd93e1d4c19b5365231ec8f981
    5        3                                              Yes                                     0
```

Always check the event viewer



Event 6273, Microsoft Windows security auditing.

```
          NAS IPv6 Address:
          NAS Identifier:                  -
          NAS Port-Type:                   Wireless - IEEE 802.11
          NAS Port:                        0

RADIUS Client:
          Client Friendly Name:            AP13
          Client IP Address:               [redacted]

Authentication Details:
          Connection Request Policy Name:  Secure Wireless Connections
          Network Policy Name:             Secure Wireless Connections
          Authentication Provider:         Windows
          Authentication Server:           [redacted]
          Authentication Type:             PEAP
          EAP Type:                        -
          Account Session Identifier:      -
          Logging Results:                 Accounting information was written to the local log file.
          Reason Code:                     16
          Reason:                          Authentication failed due to a user credentials mismatch. Either the user name
provided does not map to an existing user account or the password was incorrect.
```

Useful bits & bytes, when in a hurry!

Complete list of IAP CLI commands with definition of the debug command – http://www.arubanetworks.com/techdocs/InstantMobile/Advanced/Content/Troubleshooting.htm

Setting up IAP with Clearpass for 802.1x authentication

https://www.youtube.com/watch?v=9x5uvhn2pHg

Troubleshooting Cheat sheet

http://community.arubanetworks.com/aruba/attachments/aruba/84/106/1/Troubleshooting+Cheat+Sheet-.pdf

QUESTIONS

Any Questions?

aruba
a Hewlett Packard
Enterprise company

THANK YOU FOR YOUR TIME!

aruba
a Hewlett Packard
Enterprise company