Contents

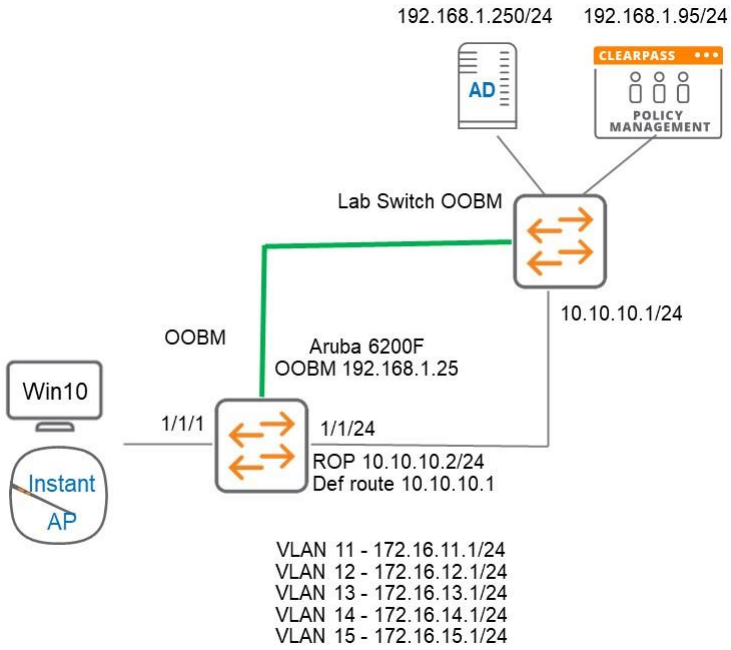
1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
08 Jan 2023	0.1	Ariya Parsamanesh	Initial creation

2 ClearPass Wired Enforcement for CX Switches Part 3

This is the third part of 6x part series on Aruba CX switch wired enforcement and the main objective of this guide is to build on the part 1 and 2. Here we'll cover

- Captive Portal redirection with MAC Auth using RADIUS VSA
- Dot1x Wired Enforcement for Aruba Instant APs using Local user roles
- MAC auth Wired Enforcement for Aruba Instant APs using Local user roles



2.1 Things you need

- ClearPass Policy Manager 6.9.7 (VM)
- Aruba CX switch running firmware version 10.10.1020
- Instant AP running firmware version 8.11.0.1
- A wired connected laptop.

We assume the reader has gone through the part 2 and 3 of this 6x part series.

3 Captive Portal with MAC Auth using RADIUS VSA

Previously we looked at Guest Captive portal and MAC Caching using local user role and for that we had configured the redirection URL on the CX switch.

Here we'll be configuring the switch and ClearPass to purely use RADIUS attributes to send the ACL and roles to the switch. Here is the enforcement profile that we need.

Enforcement Profiles - Wired-CX-Guest VSA2-CaptivePortal

Summary | Profile | Attributes

Profile:

Name:	Wired-CX-Guest VSA2-CaptivePortal
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-NAS-Filter-Rule	=	permit in udp from any to any 67
2.	Radius:Aruba	Aruba-NAS-Filter-Rule	=	permit in udp from any to any 53
3.	Radius:Aruba	Aruba-NAS-Filter-Rule	=	permit in tcp from any to 192.168.1.95 80
4.	Radius:Aruba	Aruba-NAS-Filter-Rule	=	permit in tcp from any to 192.168.1.95 443
5.	Radius:Aruba	Aruba-Captive-Portal-URL	=	https://192.168.1.95/guest/wired_guest.php
6.	Radius:Aruba	Aruba-NAS-Filter-Rule	=	cp-redirect in tcp from any to any 443
7.	Radius:Aruba	Aruba-NAS-Filter-Rule	=	cp-redirect in tcp from any to any 80
8.	Radius:IETF	Session-Timeout	=	300
9.	Radius:IETF	Tunnel-Private-Group-Id	=	13
10.	Radius:IETF	Tunnel-Type	=	VLAN (13)
11.	Radius:IETF	Tunnel-Medium-Type	=	IEEE-802 (6)
12.	Radius:IETF	Termination-Action	=	RADIUS-Request (1)

	Type	Name	Value
1	Radius:Aruba	Aruba-NAS-Filter-Rule	permit in udp from any to any 67
2	Radius:Aruba	Aruba-NAS-Filter-Rule	permit in udp from any to any 53
3	Radius:Aruba	Aruba-NAS-Filter-Rule	permit in tcp from any to 192.168.1.95 80
4	Radius:Aruba	Aruba-NAS-Filter-Rule	permit in tcp from any to 192.168.1.95 443
5	Radius:Aruba	Aruba-Captive-Portal-URL	https://192.168.1.95/guest/wired_guest.php
6	Radius:Aruba	Aruba-NAS-Filter-Rule	cp-redirect in tcp from any to any 443
7	Radius:Aruba	Aruba-NAS-Filter-Rule	cp-redirect in tcp from any to any 80
8	Radius:IETF	Session-Timeout	300
9	Radius:IETF	Tunnel-Type	VLAN (13)
10	Radius:IETF	Tunnel-Private-Group-Id	13
11	Radius:IETF	Tunnel-Medium-Type	IEEE-802 (6)
12	Radius:IETF	Termination-Action	RADIUS-Request (1)

And we are going to reference it from the same enforcement policy that we used previously. We'll be using it in the default profile. This is what we had before.

Services - CX MAC Auth

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	Wired-CX MAC Auth [Modify] Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	Wired-CX-Guest CaptivePortal
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Conflict *EQUALS* true)	Wired-CX-MAC-Spoof-CP
2.	(Tips:Role *EQUALS* School-Asset)	Wired-CX-CorpDev
3.	(Tips:Role *MATCHES_ALL* [MAC Caching] [Guest] [User Authenticated])	Wired-CX-MAC-Auth Guest, CX Return-Endpoint-Username
4.	(Tips:Role *EQUALS* [MAC Caching]) *AND* (Endpoint:Guest Role ID *EQUALS* AD-User)	Wired-CX-AD-Guest, CX Return-Endpoint-Username
5.	(Authorization:[Endpoints Repository]:Device Name *EQUALS* Aruba IAP)	CX Wired Instant-AP

And this is what we have changed it to.

Services - CX MAC Auth

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	Wired-CX MAC Auth [Modify] Add New Enfo

Enforcement Policy Details

Description:	
Default Profile:	Wired-CX-Guest VSA2-CaptivePortal
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Conflict *EQUALS* true)	Wired-CX-MAC-Spoof-CP
2.	(Tips:Role *EQUALS* School-Asset)	Wired-CX-CorpDev
3.	(Tips:Role *MATCHES_ALL* [MAC Caching] [Guest] [User Authenticated])	Wired-CX-MAC-Auth Guest, CX Return-Endpoint-Username
4.	(Tips:Role *EQUALS* [MAC Caching]) *AND* (Endpoint:Guest Role ID *EQUALS* AD-User)	Wired-CX-AD-Guest, CX Return-Endpoint-Username
5.	(Authorization:[Endpoints Repository]:Device Name *EQUALS* Aruba IAP)	CX Wired Instant-AP

Now we'll connect a client and test this service.

#	Server	Source	Username	Service	Login Status	Enforcement Profiles	Request Timestamp
1.	192.168.1.95	RADIUS	cpuser	CX MAC Auth	ACCEPT	Wired-CX-MAC-Auth Guest, CX Return-Endpoint-Username	2023/01/07 10:07:14
2.	192.168.1.95	WEBAUTH	cpuser	CX GuestWebAuth	ACCEPT	CX-GuestMAC-Caching, CX MAC Caching Expire Post Login, [Update Endpoint Known], [AOS-CX - Bounce Switch Port]	2023/01/07 10:06:39
3.	192.168.1.95	RADIUS	28d24452c238	CX MAC Auth	ACCEPT	Wired-CX-Guest VSA2-CaptivePortal	2023/01/07 10:05:00

Starting with Session #3

Summary | Input | Output | Accounting | RADIUS CoA

Login Status:	ACCEPT
Session Identifier:	R00000005-01-63b8a91b
Date and Time:	Jan 07, 2023 10:05:00 AEDT
End-Host Identifier:	28-D2-44-52-C2-38 (Computer / Windows / Windows 10)
Username:	28d24452c238
Access Device IP/Port:	192.168.1.25:1 (CX-SW1 / Aruba)
Access Device Name:	6200-Lab
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	CX MAC Auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]
Roles:	[Other], [User Authenticated]

Summary | Input | Output | Accounting | RADIUS CoA

Enforcement Profiles:	Wired-CX-Guest VSA2-CaptivePortal
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-Captive-Portal-URL	https://192.168.1.95/guest/wired_guest.php
Radius:Aruba:Aruba-NAS-Filter-Rule	cp-redirect in tcp from any to any 443
Radius:Aruba:Aruba-NAS-Filter-Rule	cp-redirect in tcp from any to any 80
Radius:Aruba:Aruba-NAS-Filter-Rule	permit in tcp from any to 192.168.1.95 443
Radius:Aruba:Aruba-NAS-Filter-Rule	permit in tcp from any to 192.168.1.95 80
Radius:Aruba:Aruba-NAS-Filter-Rule	permit in udp from any to any 53
Radius:Aruba:Aruba-NAS-Filter-Rule	permit in udp from any to any 67
Radius:IETF:Session-Timeout	300
Radius:IETF:Termination-Action	1
Radius:IETF:Tunnel-Medium-Type	6
Radius:IETF:Tunnel-Private-Group-Id	13

```
6200-Lab# sh port-access clients

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

------------------------------------------------------------------------------------
  Port     MAC-Address        Onboarding     Status               Role
Device Type
                              Method
------------------------------------------------------------------------------------
c 1/1/1    28:d2:44:52:c2:38                 In-Progress

6200-Lab# sh port-access clients

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

------------------------------------------------------------------------------------
```

```
  Port     MAC-Address       Onboarding     Status               Role
Device Type
                             Method
-------------------------------------------------------------------------------------
c 1/1/1    28:d2:44:52:c2:38 mac-auth       Success              RADIUS_1500294024

6200-Lab# sh client ip

 MAC Address               Interface        VLAN             IP Address
 ------------------------------------------------------------------------------
 28:d2:44:52:c2:38         1/1/1            13               172.16.13.28

6200-Lab#
```

```
6200-Lab# sh port-access clients detail

Port Access Client Status Details:

Client 28:d2:44:52:c2:38, 28d24452c238
======================================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 39s
    IPv4 Address : 172.16.13.28
    IPv6 Address :
    Device Type  :

  VLAN Details
  ------------
    VLAN Group Name :
    VLANs Assigned  : 13
      Access          : 13
      Native Untagged :
      Allowed Trunk   :

  Authentication Details
  ----------------------
    Status          : mac-auth Authenticated
    Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
    Auth History    : mac-auth - Authenticated, 28s ago
                      dot1x - Unauthenticated, Supplicant-Timeout, 28s ago

  Authorization Details
  ---------------------
    Role   : RADIUS_1500294024
    Status : Applied


Role Information:

Name  : RADIUS_1500294024
Type  : radius
-----------------------------------------------
    Reauthentication Period             : 300 secs
    Cached Reauthentication Period      :
    Authentication Mode                 :
    Session Timeout                     :
    Client Inactivity Timeout           :
    Description                         :
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         : 13
    Native VLAN                         :
```

```
    Allowed Trunk VLANs                  :
    Access VLAN Name                     :
    Native VLAN Name                     :
    Allowed Trunk VLAN Names             :
    VLAN Group Name                      :
    MTU                                  :
    QOS Trust Mode                       :
    STP Administrative Edge Port         :
    PoE Priority                         :
    PVLAN Port Type                      :
    Captive Portal Profile               : RADIUS_1500294024
    Policy                               : RADIUS_101364289
    Device Type                          :


Captive Portal Profile Configuration

    Name                              : RADIUS_1500294024
    Type                              : radius
    URL                               : https://192.168.1.95/guest/wired_guest.php


Access Policy Details:

Policy Name   : RADIUS_101364289
Policy Type   : Radius
Policy Status : Applied

SEQUENCE    CLASS                          TYPE ACTION
----------- ------------------------------ ---- ----------------------------------
10          RADIUS_101364289_2348833312  ipv4 permit
20          RADIUS_101364289_2174631534  ipv6 permit
30          RADIUS_101364289_861005094   ipv4 permit
40          RADIUS_101364289_4142458329  ipv4 redirect captive-portal
50          RADIUS_101364289_3577529593  ipv6 redirect captive-portal


Class Details:

class ip RADIUS_101364289_2348833312
    10 match udp any any eq dhcp-server
    20 match udp any any eq dns
class ipv6 RADIUS_101364289_2174631534
    10 match udp any any eq dhcp-server
    20 match udp any any eq dns
class ip RADIUS_101364289_861005094
    10 match tcp any 192.168.1.95 eq http
    20 match tcp any 192.168.1.95 eq https
class ip RADIUS_101364289_4142458329
    10 match tcp any any eq https
    20 match tcp any any eq http
class ipv6 RADIUS_101364289_3577529593
    10 match tcp any any eq https
    20 match tcp any any eq http

6200-Lab#
```

Now once the user logs with credentials of cpuser, we'll see a WEBAUTH followed by another MAC auth. Herer is the final MAC auth that will provide MAC caching (Session #1)

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000006-01-63b8a9a2
Date and Time:	Jan 07, 2023 10:07:14 AEDT
End-Host Identifier:	28-D2-44-52-C2-38 (Computer / Windows / Windows 10)
Username:	cpuser
Access Device IP/Port:	192.168.1.25:1 (CX-SW1 / Aruba)
Access Device Name:	6200-Lab
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	CX MAC Auth
Authentication Method:	MAC-AUTH
Authentication Source:	Local:localhost
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]
Roles:	[Guest], [MAC Caching], [User Authenticated]

Summary | Input | Output | Accounting

Enforcement Profiles:	Wired-CX-MAC-Auth Guest, CX Return-Endpoint-Username
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role	Guest
Radius:IETF:Session-Timeout	28800
Radius:IETF:User-Name	cpuser

```
6200-Lab# sh port-access clients

Port Access Clients
Status Codes: d device-mode, c client-mode, m multi-domain

--------------------------------------------------------------------------------
  Port     MAC-Address       Onboarding     Status               Role
Device Type
                             Method
--------------------------------------------------------------------------------
c 1/1/1    28:d2:44:52:c2:38 mac-auth       Success              Guest

6200-Lab#
```

```
6200-Lab# sh port-access clients detail

Port Access Client Status Details:

Client 28:d2:44:52:c2:38, cpuser
================================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 396s
    IPv4 Address : 172.16.14.28
    IPv6 Address :
    Device Type  :

  VLAN Details
  ------------
    VLAN Group Name :
    VLANs Assigned  : 14
```

```
      Access          : 14
      Native Untagged :
      Allowed Trunk   :

  Authentication Details
  ----------------------
    Status          : mac-auth Authenticated
    Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
    Auth History    : mac-auth - Authenticated, 384s ago
                      dot1x - Unauthenticated, Supplicant-Timeout, 384s ago

  Authorization Details
  ----------------------
    Role   : Guest
    Status : Applied

Role Information:

Name  : Guest
Type  : local
---------------------------------------------
    Reauthentication Period             : 3000 secs
    Cached Reauthentication Period      :
    Authentication Mode                 : client-mode
    Session Timeout                     :
    Client Inactivity Timeout           : 400 secs
    Description                         : LUR-for-Guest
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         : 14
    Native VLAN                         :
    Allowed Trunk VLANs                 :
    Access VLAN Name                    :
    Native VLAN Name                    :
    Allowed Trunk VLAN Names            :
    VLAN Group Name                     :
    MTU                                 :
    QOS Trust Mode                      :
    STP Administrative Edge Port        :
    PoE Priority                        :
    PVLAN Port Type                     :
    Captive Portal Profile              :
    Policy                              : Guest-Pol
    Device Type                         :

Access Policy Details:

Policy Name   : Guest-Pol
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                        TYPE ACTION
----------- ---------------------------- ---- ----------------------------------
10          IP-Any-Any                   ipv4 permit

Class Details:

class ip IP-Any-Any
    10 match any any any

6200-Lab#
```

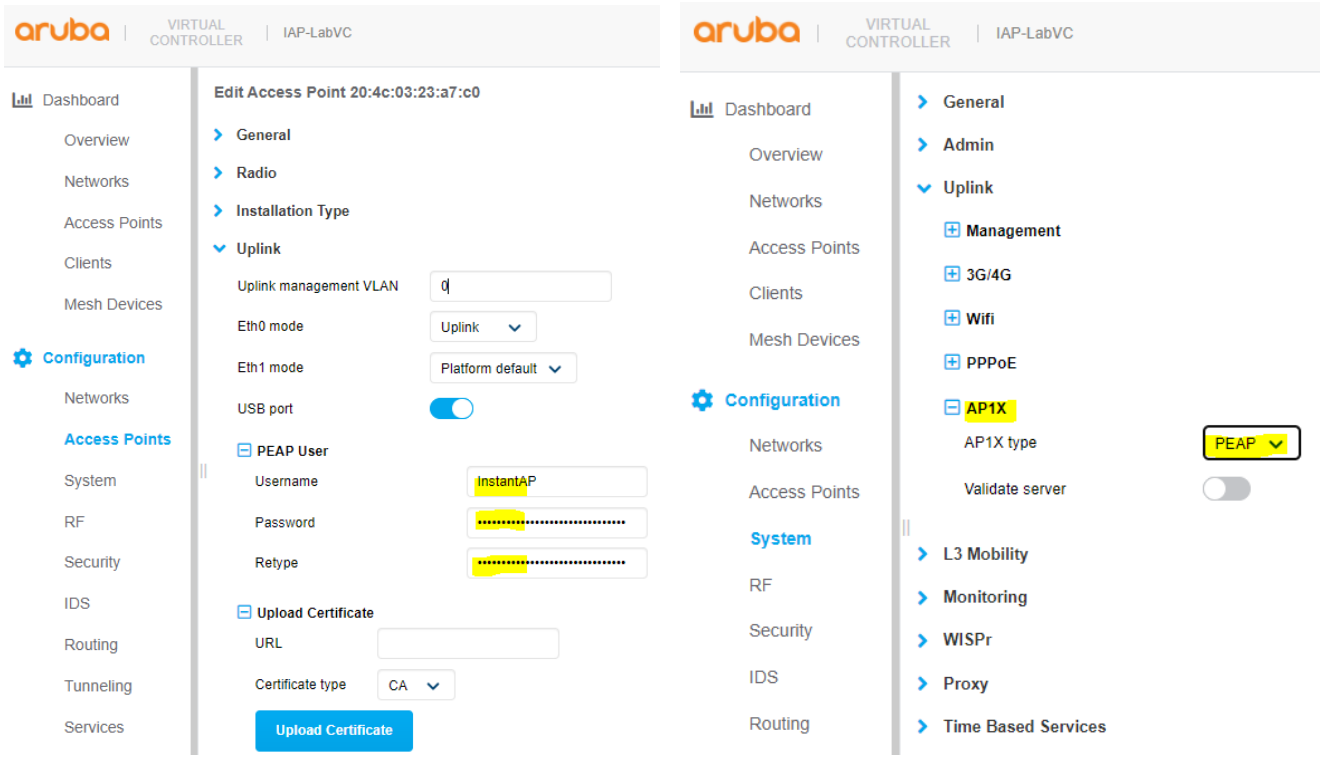
4 Wired Enforcement for Instant APs Dot1x - LUR

We are going to extend the concept of colourless port to the switch ports for Instant APs (IAP) as well.

The aim here is to do enable dot1x to authenticate the IAPs and then place the IAPs in their own user-roles with relevant untagged/tagged VLANs while allowing the wireless users connected to the IAPs to go through as per the authentication on the Wireless LAN configuration of the IAPs.

4.1 Instant AP Configuration

Here we enable the IAP for dot1x authentication. For simplicity we are going to use PEAP user InstantAP as the username



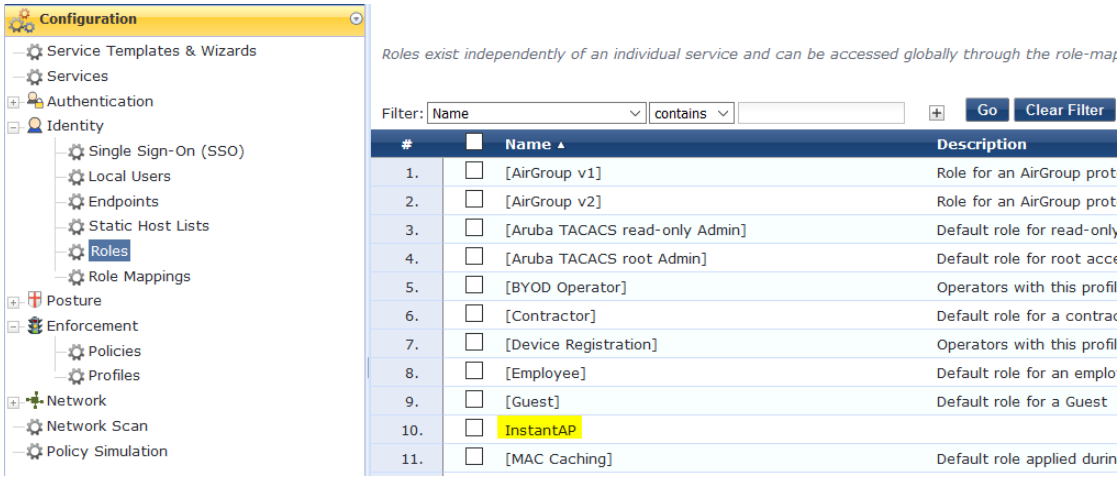
Once you have made the above changes, you need to reboot the IAP.

To verify the above configuration, use these commands

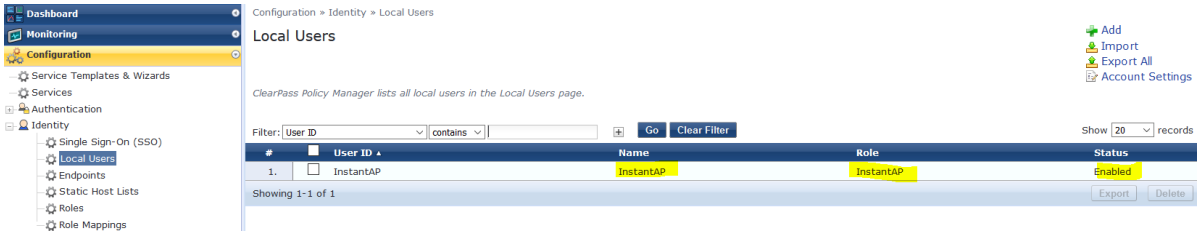
```
20:4c:03:23:a7:c0# sh ap1x config
#generated by rcS.fatap
ctrl_interface=/var/run/wpa_supplicant
ap_scan=0
eapol_version=1
fast_reauth=1
network={
    scan_ssid=0
    key_mgmt=IEEE8021X
  eap=PEAP
  eapol_flags=0
  identity="InstantAP"
  password="xxxxxxxxx"
  phase1="crypto_binding=0"
  phase2="peaplabel=1"
  phase2="auth=MSCHAPV2"
  priority=1
}

20:4c:03:23:a7:98
```

4.2 Wired Dot1x Service Policy

For our demo, we first create a Role in ClearPass



Then add a user to the local database with the same credential that we specified in Instant AP configuration.



We then create an enforcement profile for it to send a specific user role back to the switch.

Enforcement Profiles - CX dot1x Wired Instant-AP

Summary | Profile | Attributes

Profile:

Name:	CX dot1x Wired Instant-AP
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	IAP-1x

And finally modify the previous wired dot1x service policy by adding a rule to the enforcement policy.

Services - CX dot1x Wired

Summary | Service | Authentication | Roles | Enforcement

Use Cached Results:	Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	CX 802.1X Wired Enforcement Policy Modify — Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	[Deny Access Profile]
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:Lab-AD:memberOf *CONTAINS* Staff)	CX dot1x Wired Staff, CX Update Endpoint sec-access
2.	(Authorization:Lab-AD:memberOf *CONTAINS* Student)	CX dot1x Wired Student, CX Update Endpoint sec-access
3.	(Tips:Role *EQUALS* InstantAP)	CX dot1x Wired Instant-AP

4.3 LAN Switch Configuration

Here we need the new user role and its associated policies. The rest of the configuration is exactly the same as shown before.

```
vlan 15
    name Mgmt-vlan
!
interface vlan 15
    ip address 172.16.15.1/24
!
dhcp-server vrf default
    pool Mgmt-15
        range 172.16.15.20 172.16.15.29
        default-router 172.16.15.1
        dns-server 192.168.1.130
        lease 00:01:00
        exit
!
interface 1/1/1
    no shutdown
    no routing
    vlan trunk native 1
    vlan trunk allowed all
!
port-access policy InstantAP-Pol
    10 class ip IP-Any-Any
!
port-access role IAP-1x
    description LUR-for-IAPs
    associate policy InstantAP-Pol
    poe-priority critical
    auth-mode device-mode
    trust-mode dscp
    vlan trunk native 15
!
```

Using auth-mode as device-mode provides the ability when the first client authenticating on the port defines that access for all clients on that port. So, if there are additional clients on the same port, they 'piggyback' on the access of the first device.

In our case, if we authenticate the Instant AP, we don't want the switch to authenticate the wireless clients that are connecting through the AP because the AP already authenticated them.

4.4 Testing

Now is the time to test the setup which starts by the rebooting of the IAP. Here is the console connection of the IAP.

```
<showing only the relevant parts>

Terminal access enabled...
Valid SSID detected...
touching file /tmp/ip_mode_0
do ethtool autoneg on for eth0
init usb modem ...
[   60.675275] SCSI subsystem initialized
No USB Plugged in
error in reading source file
apdot1x authentication type is peap
Mesh is DISABLED on this device.
extended ssid is activated on the platform ...
copying bootuplog ...
[   89.999326] uol_init_driver:434 HW offload not applicable, AP will use cutting
through path!
```

```
allow PAPI
set device anul0 mtu to 2000
notify asap_mod 3g no present...
Starting update SBL1 ...
SBL1 was updated already
Done.
trigger wpa_supplicant with configure file /aruba/ap1x/wpa.conf
checking the authenticaiton result and will time out at most 1 min
ap1x authentication succeeded
Starting DHCP
```

And from the CLI of IAP you can also get the following

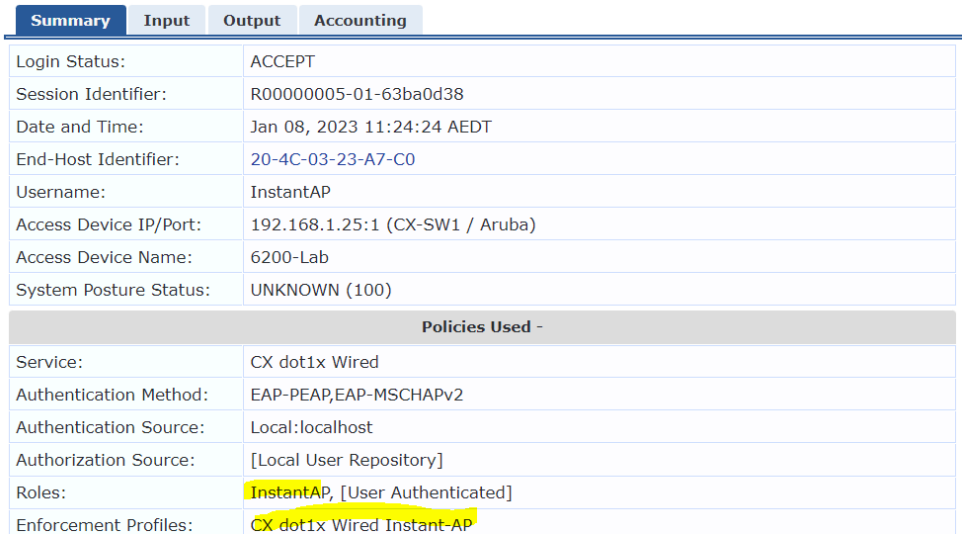
```
LabAP# sh ap1x status

ap1x:peap
ap1x auth result:succeed

LabAP#
```

```
LabAP# sh ap1x config
ap1x-timeout:not configured

#generated by rcS.fatap
ctrl_interface=/var/run/wpa_supplicant
ap_scan=0
eapol_version=1
fast_reauth=1
openssl_ciphers=ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-
ECDSA-AES256-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-
AES128-SHA256:ECDHE-RSA-AES256-SHA:ECDHE-RSA-AES128-SHA
network={
   scan_ssid=0
   key_mgmt=IEEE8021X
  eap=PEAP
  eapol_flags=0
  identity="InstantAP"
  password="********"
  phase1="tls_disable_time_checks=1 tls_suiteb=1 tls_disable_tlsv1_0=1"
  phase2="peaplabel=1 auth=MSCHAPV2"
  fragment_size=1024
  priority=1
}
LabAP#
```

```
LabAP#
LabAP# sh ap1x debug-logs
1970-01-01 00:01:02:apdot1x authentication type is peap
1970-01-01 00:01:03:trigger wpa_supplicant with configure file /aruba/ap1x/wpa.conf
1970-01-01 00:01:03:checking the authenticaiton result and will time out at most 1
min
1970-01-01 00:01:07:ap1x authentication succeeded
LabAP#
```

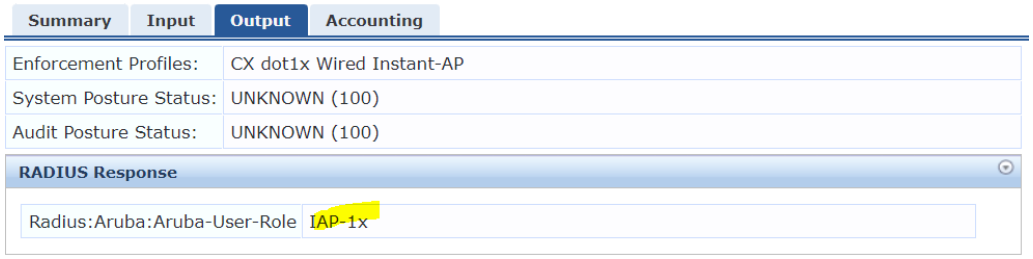
Now from ClearPass Access Tracker we get this.

2.	192.168.1.95	RADIUS	InstantAP	CX dot1x Wired	ACCEPT	CX dot1x Wired Instant-AP	2023/01/08 11:24:24
3.	192.168.1.95	RADIUS	204c0323a7c0	CX MAC Auth	ACCEPT	Wired-CX-Guest VSA2-CaptivePortal	2023/01/08 11:23:56



Summary	Input	Output	Accounting

Login Status:	ACCEPT
Session Identifier:	R00000005-01-63ba0d38
Date and Time:	Jan 08, 2023 11:24:24 AEDT
End-Host Identifier:	20-4C-03-23-A7-C0
Username:	InstantAP
Access Device IP/Port:	192.168.1.25:1 (CX-SW1 / Aruba)
Access Device Name:	6200-Lab
System Posture Status:	UNKNOWN (100)
Policies Used -	
Service:	CX dot1x Wired
Authentication Method:	EAP-PEAP,EAP-MSCHAPv2
Authentication Source:	Local:localhost
Authorization Source:	[Local User Repository]
Roles:	InstantAP, [User Authenticated]
Enforcement Profiles:	CX dot1x Wired Instant-AP



Summary	Input	Output	Accounting

Enforcement Profiles:	CX dot1x Wired Instant-AP
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-User-Role	IAP-1x

And now from LAN switch CLI we see that

```
6200-Lab# sh port-access clients

Port Access Clients
Status Codes: d device-mode, c client-mode, m multi-domain

------------------------------------------------------------------------------
  Port     MAC-Address       Onboarding     Status               Role
Device Type
                             Method
------------------------------------------------------------------------------
d 1/1/1    20:4c:03:23:a7:c0 dot1x          Success              IAP-1x

6200-Lab#
```

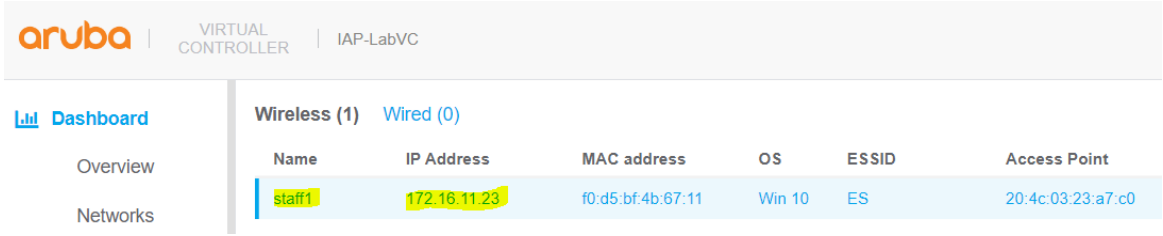
```
6200-Lab# sh port-access clients detail

Port Access Client Status Details:

Client 20:4c:03:23:a7:c0, InstantAP
==================================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 71s
    IPv4 Address :
    IPv6 Address :
    Device Type  :

  VLAN Details
  ------------
    VLAN Group Name :
    VLANs Assigned  : 15
```

```
      Access          :
      Native Untagged : 15
      Allowed Trunk   :

  Authentication Details
  ----------------------
    Status          : dot1x Authenticated
    Auth Precedence : dot1x - Authenticated, mac-auth - Not attempted
    Auth History    : dot1x - Authenticated, 32s ago
                      mac-auth - Authenticated, 60s ago
                      dot1x - Unauthenticated, Supplicant-Timeout, 60s ago

  Authorization Details
  ---------------------
    Role   : IAP-1x
    Status : Applied

Role Information:

Name  : IAP-1x
Type  : local
-------------------------------------------
    Reauthentication Period             :
    Cached Reauthentication Period      :
    Authentication Mode                 : device-mode
    Session Timeout                     :
    Client Inactivity Timeout           :
    Description                         : LUR-for-IAPs
    Gateway Zone                        :
    UBT Gateway Role                    :
    UBT Gateway Clearpass Role          :
    Access VLAN                         :
    Native VLAN                         : 15
    Allowed Trunk VLANs                 :
    Access VLAN Name                    :
    Native VLAN Name                    :
    Allowed Trunk VLAN Names            :
    VLAN Group Name                     :
    MTU                                 :
    QOS Trust Mode                      : dscp
    STP Administrative Edge Port        :
    PoE Priority                        : critical
    PVLAN Port Type                     :
    Captive Portal Profile              :
    Policy                              : InstantAP-Pol
    Device Type                         :

Access Policy Details:

Policy Name   : InstantAP-Pol
Policy Type   : Local
Policy Status : Applied

SEQUENCE    CLASS                         TYPE ACTION
----------- ----------------------------- ---- ----------------------------------
10          IP-Any-Any                    ipv4 permit

Class Details:

class ip IP-Any-Any
    10 match any any any

6200-Lab#
```

```
6200-Lab# sh mac-address-table
```

```
MAC age-time             : 300 seconds
Number of MAC addresses : 1

MAC Address           VLAN     Type                          Port
------------------------------------------------------------
20:4c:03:23:a7:c0     15       port-access-security          1/1/1

6200-Lab#
```

We also have a “ES” SSID that uses dot1x authentication configured on Instant AP that will get some clients to connect to.



As you can see, we have Staff1 connected and getting a VLAN 11.

The CX switch still shows one user-role for interface 1/1/21 however we see the new MAC address for these wireless clients in the MAC table.

```
6200-Lab# sh port-access clients

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

-------------------------------------------------------------------------------
  Port     MAC-Address       Onboarding     Status               Role
Device Type
                             Method
-------------------------------------------------------------------------------
d 1/1/1    20:4c:03:23:a7:c0 dot1x          Success              IAP-1x

6200-Lab#
```

```
6200-Lab# sh mac-address-table
MAC age-time             : 300 seconds
Number of MAC addresses : 2

MAC Address           VLAN     Type                          Port
------------------------------------------------------------
f0:d5:bf:4b:67:11     11       port-access-security          1/1/1
20:4c:03:23:a7:c0     15       port-access-security          1/1/1

6200-Lab#
```

Now from the ClearPass access tracker we can verify that there is no additional request from the LAN switch.

Note that we are also using the same ClearPass for wireless dot1x authentication.

#	Server	Source	Username	Service	Login Status	Enforcement Profiles
1.	192.168.1.95	RADIUS	radius-tracking-user	Aruba switch RADIUS-Tracking	ACCEPT	[Allow Access Profile]
2.	192.168.1.95	RADIUS	radius-tracking-user	Aruba switch RADIUS-Tracking	ACCEPT	[Allow Access Profile]
3.	192.168.1.95	RADIUS	staff1	School 802.1X WiFi	ACCEPT	[Update Endpoint Known], school 1xWiFi DUR Staff

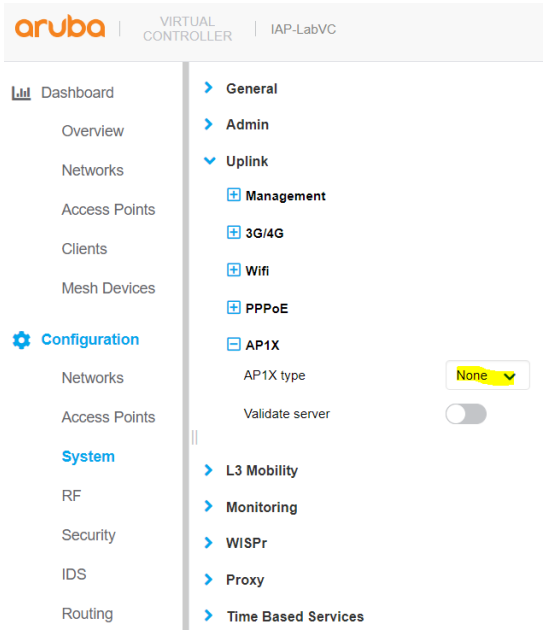
5 Wired Enforcement for Instant APs MAC Auth - LUR

Here instead of using dot1x to authenticate the IAP we'll be using MAC Auth with ClearPass Profiling.

Exactly same as last section except we'll be using ClearPass profiling mechanism by using "ip-helper" to send the DHCP request to ClearPass.

5.1 Instant AP Configuration

Just ensure you have removed the AP1x setting and reboot the IAP.



5.2 Wired MAC Auth Service Policy

The workflow will be as follows:

- when a new Instant AP connects to the wired network, the switch sends the MAC auth followed by DHCP request (using ip-helper command) to ClearPass.
- ClearPass will allow all the MAC authentication and checks the MAC vendor OUI and puts it in the Captive-portal user role.
- While in this user-role which is quite restrictive, the AP will do a DHCP request which ClearPass can see and then profiles it to be Instant AP along with AP name, etc.
- Now because we have enabled "profile endpoints" for this service, we have added a rule in the profile tab that if there is any change in the initial endpoint classification, use CoA to bounce the switch port.
- Now once ClearPass profiles the Instant AP, it'll update the endpoint category which then bounce the switch port.
- There will be a new MAC auth and this time because Instant AP has been profiles, we can match it with any attribute of the endpoint repository like device name which will be "Aruba IAP"

We basically modify the previous "CX MAC Auth" service by adding couple of rules to the enforcement policy.

1. We need to enable profiling and to check for MAC spoofing, the first rule does that.

Services - CX MAC Auth

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Name:	CX MAC Auth
Description:	MAC-based Authentication Service
Type:	MAC Authentication
Status:	Enabled
Monitor Mode:	☐ Enable to monitor network access without enforcement
More Options:	☑ Authorization ☐ Audit End-hosts ☑ Profile Endpoints ☐ Accounting Proxy

Service Rule

Matches ○ ANY or ◉ ALL of the following conditions:

	Type	Name	Operator	Value
1.	Radius:IETF	NAS-Port-Type	BELONGS_TO	Ethernet (15), Wireless-802.11 (19)
2.	Radius:IETF	Service-Type	BELONGS_TO	Login-User (1), Call-Check (10)
3.	Connection	Client-Mac-Address	EQUALS	%{Radius:IETF:User-Name}

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Use Cached Results:	☐ Use cached Roles and Posture attributes from previous sessions
Enforcement Policy:	Wired-CX MAC Auth [Modify] Add New Enforcement Policy

Enforcement Policy Details

Description:	
Default Profile:	Wired-CX-Guest VSA2-CaptivePortal
Rules Evaluation Algorithm:	first-applicable

	Conditions	Enforcement Profiles
1.	(Authorization:[Endpoints Repository]:Conflict *EQUALS* true)	Wired-CX-MAC-Spoof-CP
2.	(Tips:Role *EQUALS* School-Asset)	Wired-CX-CorpDev
3.	(Tips:Role *MATCHES_ALL* [MAC Caching] [Guest] [User Authenticated])	Wired-CX-MAC-Auth Guest, CX Return-Endpoint-Username
4.	(Tips:Role *EQUALS* [MAC Caching]) *AND* (Endpoint:Guest Role ID *EQUALS* AD-User)	Wired-CX-AD-Guest, CX Return-Endpoint-Username
5.	(Authorization:[Endpoints Repository]:Device Name *EQUALS* Aruba IAP)	CX Wired Instant-AP

Summary | Service | Authentication | Authorization | Roles | Enforcement | Profiler

Endpoint Classification:	Select the classification(s) after which an action must be triggered - Any Category / OS Family / Name [Remove] -- Select --
RADIUS CoA Action:	[AOS-CX - Bounce Switch Port] [View Details] [Modify]

When the Instant AP first connects, it should match the default enforcement profile, then once it gets profiled it should match the 5th rule.

Here are the enforcement profiles.

Enforcement Profiles - Wired-CX-MAC-Spoof-CP

Summary | Profile | Attributes

Profile:

Name:	Wired-CX-MAC-Spoof-CP
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	Captive-Portal-Spoof
2.	Radius:Aruba	Aruba-Captive-Portal-URL	=	https://192.168.1.95/guest/wired_mac_spoof.php
3.	Radius:IETF	Session-Timeout	=	600

Enforcement Profiles - CX Wired Instant-AP

Summary | Profile | Attributes

Profile:

Name:	CX Wired Instant-AP
Description:	
Type:	RADIUS
Action:	Accept
Device Group List:	-

Attributes:

	Type	Name		Value
1.	Radius:Aruba	Aruba-User-Role	=	InstantAP

5.3 LAN Switch Configuration

The only thing we are adding is the ip-helper command for VLAN15 which is out mgmt. VLAN

The rest are just shown for completeness.

```
port-access policy InstantAP-Pol
    10 class ip IP-Any-Any

port-access role InstantAP
    description LUR-for-IAPs
    associate policy InstantAP-Pol
    auth-mode device-mode
    poe-priority critical
    trust-mode dscp
    vlan trunk native 15
    vlan trunk allowed 11-12

interface vlan 13
    ip address 172.16.13.1/24
    ip helper-address 192.168.1.95

interface vlan 15
    ip address 172.16.15.1/24
    ip helper-address 192.168.1.95
```

We have added the IP helper address so that ClearPass get to see the DHCP requests from the IAPs.

5.4 Testing

Now is the time to test the setup which starts by the rebooting of the IAP and ensuring the endpoint database is cleared. Now from ClearPass Access Tracker we get this.

Filter: Request ID contains Go Clear Filter

#	Server	Source	Username	Service	Login Status	Enforcement Profiles
1.	192.168.1.95	RADIUS	204c0323a7c0	CX MAC Auth	ACCEPT	CX Wired Instant-AP
2.	192.168.1.95	RADIUS	204c0323a7c0	CX MAC Auth	ACCEPT	Wired-CX-Guest VSA2-CaptivePortal

Checking the request #2.

Summary	Input	Output	Accounting	RADIUS CoA	Alerts

Login Status:	ACCEPT
Session Identifier:	R00000015-01-63ba1bcf
Date and Time:	Jan 08, 2023 12:26:39 AEDT
End-Host Identifier:	20-4C-03-23-A7-C0 (Access Points / Aruba / Aruba IAP)
Username:	204c0323a7c0
Access Device IP/Port:	192.168.1.25:1 (CX-SW1 / Aruba)
Access Device Name:	6200-Lab
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	CX MAC Auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]
Roles:	[Other], [User Authenticated]

Summary	Input	Output	Accounting	RADIUS CoA	Alerts

Enforcement Profiles:	Wired-CX-Guest VSA2-CaptivePortal
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

Radius:Aruba:Aruba-Captive-Portal-URL	https://192.168.1.95/guest/wired_guest.php
Radius:Aruba:Aruba-NAS-Filter-Rule	cp-redirect in tcp from any to any 443
Radius:Aruba:Aruba-NAS-Filter-Rule	cp-redirect in tcp from any to any 80
Radius:Aruba:Aruba-NAS-Filter-Rule	permit in tcp from any to 192.168.1.95 443
Radius:Aruba:Aruba-NAS-Filter-Rule	permit in tcp from any to 192.168.1.95 80
Radius:Aruba:Aruba-NAS-Filter-Rule	permit in udp from any to any 53
Radius:Aruba:Aruba-NAS-Filter-Rule	permit in udp from any to any 67
Radius:IETF:Session-Timeout	300
Radius:IETF:Termination-Action	1
Radius:IETF:Tunnel-Medium-Type	6
Radius:IETF:Tunnel-Private-Group-Id	13

```
6200-Lab# sh port-access clients

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

--------------------------------------------------------------------------------
  Port      MAC-Address       Onboarding     Status               Role
Device Type
                              Method
--------------------------------------------------------------------------------
c 1/1/1     20:4c:03:23:a7:c0 mac-auth       Success              RADIUS_1500294024

6200-Lab#
```

Checking the next request, at this point the IAP does the DHCP request then ClearPass would profile it and adds the profiling info to the Endpoint database, the category update in the endpoint repository will trigger a port bounce and the IAP is put into the correct VLAN and user role.

Summary | Input | Output | Accounting

Login Status:	ACCEPT
Session Identifier:	R00000016-01-63ba1c11
Date and Time:	Jan 08, 2023 12:27:45 AEDT
End-Host Identifier:	20-4C-03-23-A7-C0 (Access Points / Aruba / Aruba IAP)
Username:	204c0323a7c0
Access Device IP/Port:	192.168.1.25:1 (CX-SW1 / Aruba)
Access Device Name:	6200-Lab
System Posture Status:	UNKNOWN (100)

Policies Used -

Service:	CX MAC Auth
Authentication Method:	MAC-AUTH
Authentication Source:	None
Authorization Source:	[Guest User Repository], [Guest Device Repository], [Endpoints Repository], [Insight Repository], [Time Source]
Roles:	[Other], [User Authenticated]

Summary | Input | Output | Accounting

Username:	204c0323a7c0
End-Host Identifier:	20-4C-03-23-A7-C0 (Access Points / Aruba / Aruba IAP)
Access Device IP/Port:	192.168.1.25:1 (CX-SW1 / Aruba)

RADIUS Request

Authorization Attributes

Computed Attributes

Endpoint Attributes

MAC Vendor	Aruba, a Hewlett Packard Enterprise Company
Added by	Policy Manager
Status	Unknown
Device Category	Access Points
Device OS Family	Aruba
Device Name	Aruba IAP
MAC Address	204c0323a7c0

Summary | Input | Output | Accounting

Enforcement Profiles:	CX Wired Instant-AP
System Posture Status:	UNKNOWN (100)
Audit Posture Status:	UNKNOWN (100)

RADIUS Response

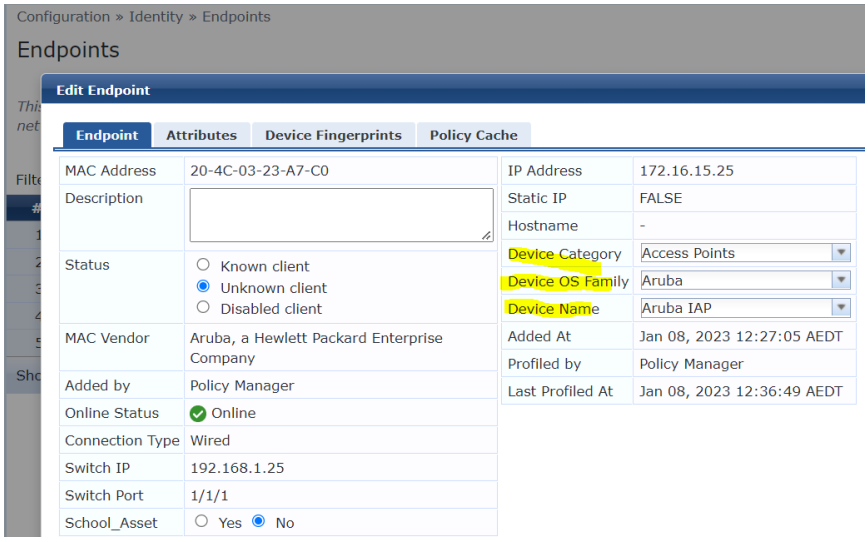
Radius:Aruba:Aruba-User-Role	InstantAP

Here is the port-access info from the CX switch.

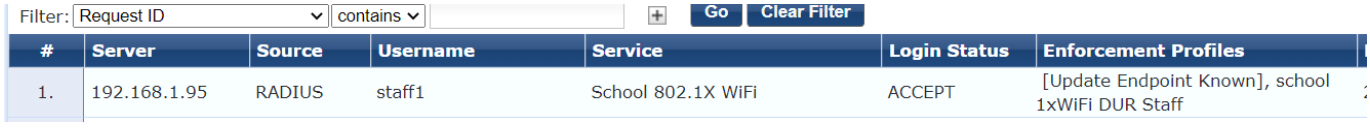
```
6200-Lab# sh port-access clients

Port Access Clients
Status Codes: d device-mode, c client-mode, m multi-domain

--------------------------------------------------------------------------------
  Port      MAC-Address       Onboarding     Status               Role
Device Type
                            Method
--------------------------------------------------------------------------------
d 1/1/1     20:4c:03:23:a7:c0 mac-auth       Success              InstantAP

6200-Lab#
```

```
6200-Lab# sh port-access clients detail

Port Access Client Status Details:

Client 20:4c:03:23:a7:c0, 204c0323a7c0
======================================
  Session Details
  ---------------
    Port         : 1/1/1
    Session Time : 198s
    IPv4 Address :
    IPv6 Address :
    Device Type  :

  VLAN Details
  ------------
    VLAN Group Name :
    VLANs Assigned  : 15
      Access          :
      Native Untagged : 15
      Allowed Trunk   :

  Authentication Details
  ----------------------
    Status          : mac-auth Authenticated
    Auth Precedence : dot1x - Unauthenticated, mac-auth - Authenticated
    Auth History    : mac-auth - Authenticated, 188s ago
                      dot1x - Unauthenticated, Supplicant-Timeout, 188s ago

  Authorization Details
  ---------------------
    Role   : InstantAP
    Status : Applied

Role Information:
 -- MORE --, next page: Space, next line: Enter, quit: q
```

Here is the endpoint repository information



Now once again we'll connect a Wireless client to "ES" SSID that uses dot1x authentication configured on Instant AP.



The CX switch still shows one user-role for interface 1/1/24 however we see the new MAC address for these wireless clients in the MAC table.

```
6200-Lab# sh port-access client

Port Access Clients

Status Codes: d device-mode, c client-mode, m multi-domain

--------------------------------------------------------------------------------
  Port     MAC-Address       Onboarding     Status               Role
Device Type
                             Method
--------------------------------------------------------------------------------
d 1/1/1    20:4c:03:23:a7:c0 mac-auth       Success              InstantAP

6200-Lab#
```

```
6200-Lab# sh client ip

 MAC Address               Interface        VLAN             IP Address
 ------------------------------------------------------------------------------
 f0:d5:bf:4b:67:11         1/1/1            11               172.16.11.23

6200-Lab#
```

```
6200-Lab# sh mac-address-table
MAC age-time            : 300 seconds
Number of MAC addresses : 2

MAC Address          VLAN     Type                       Port
-------------------------------------------------------------
f0:d5:bf:4b:67:11    11       port-access-security       1/1/1
20:4c:03:23:a7:c0    15       port-access-security       1/1/1
6200-Lab#
```