

1 Table of Contents

1	Table of Contents.....	1
1.1	Revision History	1
2	Personal Wireless Network with Aruba Central	2
2.1	Things you need.....	2
2.2	Assumptions.....	2
3	CloudAuth and Personal Wireless networks	3
3.1	WLAN MPSK configuration	3
3.2	Admin Managed MPSK	5
4	PWN Testing.....	8

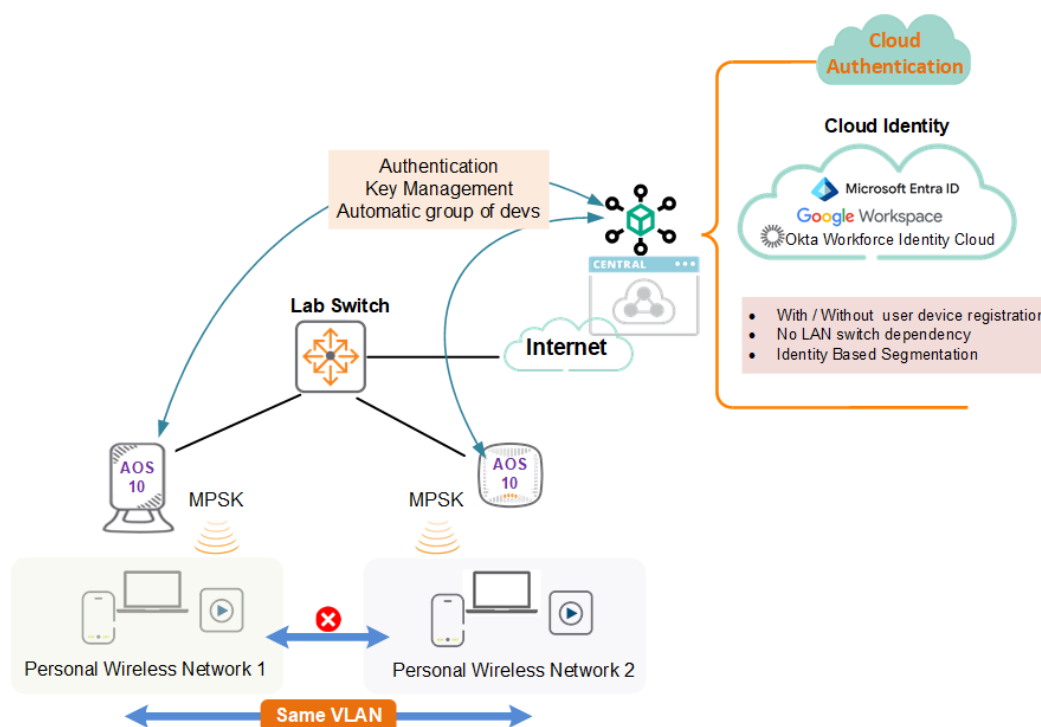
1.1 Revision History

DATE	VERSION	EDITOR	CHANGES
12 Nov 2024	0.1	Ariya Parsamanesh	Initial creation
25 Nov 2024	0.1	Ariya Parsamanesh	Added the pcap

2 Personal Wireless Network with Aruba Central

Personal Wireless Networks (PWN) are groups of user-owned Wi-Fi devices that connect and operate together in a VLAN, enabling communication within that network. It's essential to ensure that only devices within the designated group can interact with one another, along with an added ability for the device owners to permit Multicast DNS (mDNS) and Simple Service Discovery Protocol (SSDP) based services to be shared with their friends.

In this technote I'll be demonstrating PWN solution, using Multi Pre-Shared Key (MPSK) on AOS10 APs and CloudAuth to provide user role-based policies for segmentation without any dependency on an identity store. There are two parts to this solution, one is the automating the operation workflow for user device registration and the second is the access policy part to provide segmentation.



PWN Benefits are

- Self-service portal makes it easy for users like students and faculty to onboard multiple personal devices and there is no need to register each device separately
- You can use this solution with or without the identity stores
- It eliminates IT help desk tickets through a user-driven, SSID-based approach
- There is no dependency on LAN infrastructure

2.1 Things you need

We need the following.

- 2x APs (I am using AP-515 and AP-605H) running Aruba AOS10 10.7.x.x or later
- Aruba Central account and a few wireless clients

2.2 Assumptions

- Aruba AP is added to the Aruba Central account and has a valid subscription.
- Aruba AP is visible and online in Aruba Central.
- Deny Intra VLAN Traffic is not enabled as it is mutually exclusive with PWN

3 CloudAuth and Personal Wireless networks

PWN with Aruba Central is a solution that uses several features to provide the outcome and those features include

- MPSK with AOS10 APs
- Cloud Auth
- AirGroup
- User roles-based policies for North-south traffic
- VXLAN and Group Based Policy (GBP) for East-West Traffic

First you need to configure MPSK to be the authentication mode for a WLAN. Note that MPSK and MAC authentication are mutually exclusive and AOS 10.4 and above is needed to support the MPSK feature.

The unique PSKs are assigned based on two methods

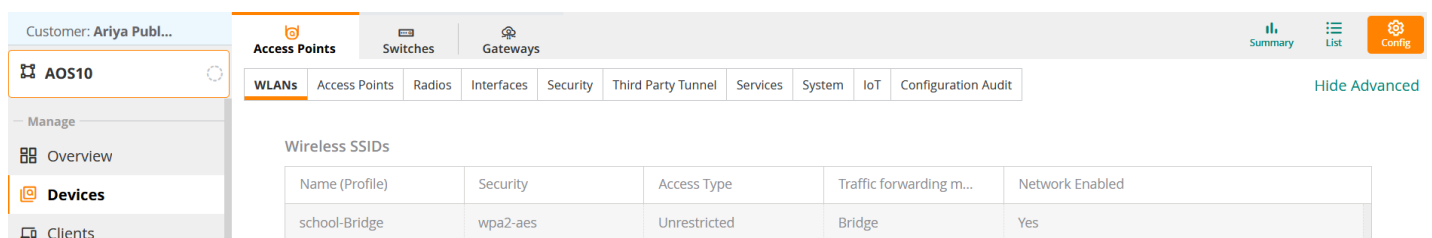
1. Admin Managed MPSK - This is also known as Named MPSK, in which PSKs are auto-generated when the administrator creates a named MPSK entry that can be shared with one or more users or use it to configure multiple devices without dependency on identity store. This is for the use cases where devices that may need to connect to MPSK network do not have any user identity associated
2. User Managed MPSK - These PSKs are specific to the user in the identity store and are auto-generated when the user signs in to the MPSK portal with their credentials. Then the users can connect multiple devices with this MPSK. So, there is a dependency on identity store.

Note that an identity provider should be configured before using the user-managed MPSK. Only the admin-managed MPSK (named MPSK) will work without configuring the identity provider.

We'll be covering Admin Managed MPSK here.

3.1 WLAN MPSK configuration

Here we'll configure "test-mpsk" WLAN that will use for our demonstration.



The screenshot shows the Aruba Central configuration interface. On the left, there's a sidebar with 'Customer: Ariya Publ...' and a list of items including 'AOS10', 'Manage', 'Overview', 'Devices', and 'Clients'. The main area has tabs for 'Access Points', 'Switches', and 'Gateways'. Under 'Access Points', there's a sub-tab 'WLANs'. Below this, there's a table titled 'Wireless SSIDs' with columns: Name (Profile), Security, Access Type, Traffic forwarding m..., and Network Enabled. The table contains one entry: 'school-Bridge' with security 'wpa2-aes', access type 'Unrestricted', traffic forwarding 'Bridge', and network enabled 'Yes'. There are also buttons for 'Summary', 'List', and 'Config' in the top right, and a 'Hide Advanced' link.

Name (Profile)	Security	Access Type	Traffic forwarding m...	Network Enabled
school-Bridge	wpa2-aes	Unrestricted	Bridge	Yes

Here are the details of WLAN configuration.

Access Points

Switches

Gateways

WLANs
Access Points
Radios
Interfaces
Security
Third Party Tunnel
Services
System
IoT
Configuration Audit

Networks > Configuration - test-mpsk

General VLANs Security Access Summary

ESSID:

test-mpsk

Band:

☒ 2.4 GHz
☒ 5 GHz
☐ 6 GHz

[> Advanced Settings](#)

General VLANs Security Access Summary

Traffic forwarding mode:

Bridge

Client VLAN Assignment:

☒ Static
☐ Dynamic

VLAN ID:

1

×

▼

Multiple VLAN IDs or single named VLAN allowed.

[> Show Named VLANs](#)

General VLANs Security Access Summary

Security Level:

Enterprise

Personal

Visitors

Open

Key Management:

MPSK AES ▼

Server Group:

Primary and backup only ▼

Primary Server:

Cloud Auth ▼

+

ⓘ MPSK-AES with Cloudauth requires AOS version 10.4 or above

Personal Wireless Network:

☒

The important thing here is that we have selected MPSK AES and Personal Wireless Network (PWN). By selecting PWN Aruba Central's Cloud auth will auto generate a Personal Area Network id (PAN-id) for each user community and shares it with the APs. Then devices with the same PAN-id can communicate together while devices with different PAN-id cannot have any access to one another. This is how the micro segmentation is achieved.

Using PWN, user's devices can roam from one AP to another while maintaining access to their devices with no risk of access of their devices to other end users. This is done using a PAN ID that is embedded into network traffic and restricts traffic to flow only between devices that belong to the same user.

General
VLANs
Security
Access
Summary

Access rules

Role Based
Network Based
Unrestricted

⚠ Unrestricted option allows full access to the network. This may lead to potential security issues.

Now that it is saved, we have our MPSK WLAN as shown below.

Customer: Ariya Publ...

AOS10

Manage

Overview

Devices

Clients

Guests

Applications

Access Points
Switches
Gateways

WLANs
Access Points
Radios
Interfaces
Security
Third Party Tunnel
Services
System
IoT
Configuration Audit

test-mpsk
mpsk-aes
Unrestricted
Bridge
Yes

Add SSID

Network Summary

General

ESSID
test-mpsk

Security

Security Level
Personal

Summary
List
Config

Hide Advanced

Next, we'll also configure a new user-role "Student-MPSK" that we'll be using for our PWN based MPSK wireless network.

Customer: Ariya Publ...

AOS10

Manage

Overview

Devices

Clients

Guests

Applications

Access Points
Switches
Gateways

WLANs
Access Points
Radios
Interfaces
Security
Third Party Tunnel
Services
System
IoT
Configuration Audit

Roles

Roles

Role

Student-MPSK

Tguest

Access Rules For Selected Roles

Assign to VLAN: 22

Deny Adult and Pornography (Web Category)

Deny Gambling (Web Category)

Allow any to all destinations

Summary
List
Config

Hide Advanced

3.2 Admin Managed MPSK

In this section we'll configure the MPSKs for two students that will create their own two device communities.

Customer: Ariya Publ...

RAPIDS
Authentication & Policy
Gateway IDS/IPS
Firewall

Global

Manage

Overview

Devices

Clients

Guests

Applications

Security

Policies

User Access Policy

Use an organization identity store to authenticate clients and control their access to the network.

Manage MPSK

Edit
Reset

Client Access Policy

Authenticate clients in the network based on their MAC addresses and control their access based on their profiling.

Allow all MAC addresses is enabled

Manage MAC Registration

Edit
Reset

Summary
List
Config

Customer: Ariya Publ...

Global

Manage

Overview

Devices

Clients

Guests

Applications

Security

Network Services

Analyze

Alerts & Events

Audit Trail

Tools

RAPIDS

Authentication & Policy

Gateway IDS/IPS

Firewall

Summary

List

Config

←

MPSK Management

Users and Administrators can create unique Wi-Fi passwords to connect clients to the network. Users can generate passwords via the Password Portal. Administrators can generate passwords by configuring Named MPSK for the network.

MPSK Usage

1 of 5000 MPSKs allocated

MPSK Networks

+ New configuration

WLAN

test-mpsk

Password Portal

Open

Copy URL

From the drop down select the options.

Customer: Ariya Publ...

Global

Manage

Overview

Devices

Clients

Guests

RAPIDS

Authentication & Policy

Gateway IDS/IPS

Firewall

Summary

List

Config

←

test-mpsk MPSK Configuration

MPSK Type

Passphrase

Passphrase

Random Password

Customer: Ariya Publ...

Global

Manage

Overview

Devices

Clients

Guests

Applications

Security

Network Services

RAPIDS

Authentication & Policy

Gateway IDS/IPS

Firewall

Summary

List

Config

←

test-mpsk MPSK Configuration

MPSK Type

Passphrase

Named MPSK (1)

Name

student-1@test.com

Client Role

Student-MPSK

Status

enabled

CANCEL

SAVE

Here we have used student-1@test.com and chosen the Student-MPSK client role that we had previously created in our AOS10 group.

Customer: Ariya Publ...

Global

Manage

Overview

Devices

Clients

Guests

Applications

Security

Network Services

RAPIDS

Authentication & Policy

Gateway IDS/IPS

Firewall

Summary

List

Config

←

test-mpsk MPSK Configuration

MPSK Type

Passphrase

Named MPSK (1)

Name

MPSK

Client Role

Status

student-1@test.com

Student-MPSK

Enabled

Copy to Clipboard

Reveal/Hide

Reset

We'll create the second user "student-2@test.com" as well.

Customer: Ariya Publ...

RAPIDS

Authentication & Policy

Gateway IDS/IPS

Firewall

Summary

List

Config

Global

Manage

Overview

Devices

Clients

Guests

Applications

Security

Network Services

test-mpsk MPSK Configuration

MPSK Type ⓘ

Passphrase

Named MPSK (2)
MPSKs for managed clients allowed to access network.

Name	MPSK		Client Role	Status
student-1@test.com	*****	...	Student-MPSK	Enabled
student-2@test.com	*****	...	Student-MPSK	Enabled

Note that you can use CSV files to upload bulk info and export the named MPSK info as well. As clients connect to the PWN based MPSK their authentication sessions are listed here.

Customer: Ariya Publ...

RAPIDS

Authentication & Policy

Gateway IDS/IPS

Firewall

3 hours

Summary

List

Config

Global

Manage

Overview

Devices

Clients

Guests

Applications

Security

Network Services

Analyze

Access Requests

Success 3

Failed 2

Sessions 3

Access Requests

Username	Status	Client Role	Access Device Name	Date & Time
student-2@test.com	Accepted	Student-MPSK	AP-605H-5d:6b	October 14, 2024 1:00:15 pm (AEDT)
student-1@test.com	Accepted	Student-MPSK	AP-605H-5d:6b	October 14, 2024 12:05:05 pm (AEDT)
student-1@test.com	Accepted	Student-MPSK	AP-605H-5d:6b	October 14, 2024 12:01:48 pm (AEDT)
2c1f23d02f48	Rejected		AP-605H-5d:6b	October 14, 2024 11:57:50 am (AEDT)
2c1f23d02f48	Rejected		AP-605H-5d:6b	October 14, 2024 11:56:51 am (AEDT)

So now we have 3x clients connected that are all from student-1@test.com and student-2@test.com as shown above.

4 PWN Testing

We have connected two APs in the AOS10 group that are configured with PWN.

Customer: Ariya Publ...	Access Points	Switches	Gateways	Summary	List	Config
AOS10	Access Points	Online 2	Offline 0	Radios 4		
Manage	Access Points (2)					
Overview	Device Name	Status	IP Ad...	M...	Serial	Firmware Version
Devices	AP-515-2b:30	Online	10.10.10.27	AP-515	CNH7KD5275	10.7.0.0_90579
Clients	AP-605H-5d:6b	Online	10.10.10.29	AP-605H	CNR5LHJ13Y	10.7.0.0_90579
				Clients	MAC Addr...	Config Status
				1	9c:8c:d8:c9:2b:30	Synchronized
				1	f0:1a:a0:2a:5d:6b	Synchronized

We now have 3x connected clients as well, in which 2x devices are from Strunet-1 and 1x device is from student-2. Note that the clients are distributed on both APs.

Customer: Ariya Publ...

AOS10

Manage

Overview

Devices

Clients

Guests

Applications

Security

Clients

3 hours

CLIENTS

ALL

22.78 MB (1.64 M)

All4

Connecting0

Connected3

Failed1

Offline0

Blocked0

Wireless4

Wired0

Remote0

CLIENTS

Client Name	Status	IP Address	VLAN	Connected To	SSID/Port	AP Role	Switch
0e:61:83:05:2c:6e	Failed			AP-515-2b:30	test-mpsk		
student-1@test.com	Connected	10.10.22.31	22	AP-605H-5d:6b	test-mpsk	Student-MPSK	
student-1@test.com	Connected	10.10.22.30	22	AP-515-2b:30	test-mpsk	Student-MPSK	
student-2@test.com	Connected	10.10.22.20	22	AP-605H-5d:6b	test-mpsk	Student-MPSK	

Here is the CLI view of the AP-605H.

```
AP-605H-5d:6b# sh client

Client List
-----
Name                IP Address    MAC Address    OS      ESSID      Access Point
Channel  Type  Role          IPv6 Address  Signal(dB)    Speed  (Mbps)
-----  -
student-2@test.com  10.10.22.20  ce:55:81:30:f8:3c  Win 10  test-mpsk  AP-605H-5d:6b
100E      AC   Student-MPSK  --              43 (good)    780 (good)
student-1@test.com  10.10.22.31  2c:1f:23:d0:2f:48  Apple  test-mpsk  AP-605H-5d:6b
100+     AN   Student-MPSK  --              46 (good)    135 (good)
Number of Clients   :2
Info timestamp      :5959

AP-605H-5d:6b#
```

You can get the PAN-id from these two commands.

```
AP-605H-5d:6b# sh ap association

The phy column shows client's operational capabilities for current association

Flags: H: Hotspot(802.11u) client, K: 802.11K client, M: Mu beam formee, R: 802.11R client, W: WMM client, w:
802.11w client, V: 802.11v BSS trans capable, P: Punctured preamble, U: HE UL Mu-mimo, O: OWE client, S: SAE
client, E: Enterprise client, m: Agile Multiband client, C: Cellular Data Capable - network available, c:
Cellular Data Capable - network unavailable, T: Individual TWT client, t: Broadcast TWT client

PHY Details: HT      : High throughput;      20: 20MHz;   40: 40MHz;  t: turbo-rates (256-QAM)
```

VHT : Very High throughput; 80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz
HE : High Efficiency; 80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz
EHT : Extremely High throughput; 80: 80MHz; 160: 160MHz; 80p80: 80MHz + 80MHz; 320: 320MHz
<n>ss: <n> spatial streams

MLO Bands: Indicates the band of each link. * indicates the band where the association occurred.

Association Table

Name	bssid	mac	auth	assoc	aid	l-int	essid	vlan-id	phy_cap
phy	assoc. time	num assoc	Flags	DataReady	UAC	user-panid	mlo-bands		
----	-----	---	----	-----	----	-----	-----	-----	-----
AP-605H-5d:6b	50:e4:e0:14:0e:51	ce:55:81:30:f8:3c	y	y	2	250	test-mpsk	22	5GHz-VHT-
80sgi-2ss-KV	5GHz-VHT-80sgi-2ss	15m:13s	1	WV	Yes	0.0.0.0	4347809	-	-
AP-605H-5d:6b	50:e4:e0:14:0e:51	2c:1f:23:d0:2f:48	y	y	1	20	test-mpsk	22	5GHz-HT-40sgi-
1ss-R	5GHz-HT-40sgi-1ss	1h:10m:23s	1	WR	Yes	0.0.0.0	13984993	-	-

Num Clients:2

AP-605H-5d:6b#

Here you'll see the mpskcache that Aruba Central sent to the APs.

AP-605H-5d:6b# sh ap mpskcache

PPSK Cache Table

Client MAC	Key	Del	Expiry	Role	VLAN	ESSID
Seqno IP		---	-----	----	----	-----
-----	---					
ce:55:81:30:f8:3c	(6): b2 f6 f4 57 02 c2 ...	No	-	Student-MPSK	22	test-mpsk
2289 10.10.22.20						
2c:1f:23:d0:2f:48	(6): d1 d7 ff a5 ed 78 ...	No	-	Student-MPSK	22	test-mpsk
2288 10.10.22.31						

PPSK Cache Count:2

AP-605H-5d:6b#

AP-605H-5d:6b# sh ap mpskcache 2c:1f:23:d0:2f:48

Station MAC address :2c:1f:23:d0:2f:48
Seq no :2288
Key :(6): d1 d7 ff a5 ed 78
ESSID :test-mpsk
Name :student-1@test.com
Role :Student-MPSK
Server :Not set
VLAN :22
To Del :0
Expire :2m:26s
Vlanhow :254
Rolehow :0
ACL Rule Index :229374
User panid :13984993
Session timeout :28800

AP-605H-5d:6b#

AP-605H-5d:6b# sh ap mpskcache ce:55:81:30:f8:3c

Station MAC address :ce:55:81:30:f8:3c
Seq no :2289
Key :(6): b2 f6 f4 57 02 c2
ESSID :test-mpsk
Name :student-2@test.com
Role :Student-MPSK
Server :Not set
VLAN :22
To Del :0

```

Expire           :6m:19s
Vlanhow          :254
Rolehow          :0
ACL Rule Index   :229374
User panid       :4347809
Session timeout  :28800

AP-605H-5d:6b#

```

Now I'll check the other AP (AP-515) and we see that the PAN id is the same since they are the devices of the same user (student-1@test.com)

```

AP-515-2b:30# sh clients

Client List
-----
Name           IP Address   MAC Address   OS      ESSID      Access Point
Channel  Type  Role      IPv6 Address  Signal (dB)  Speed (Mbps)
-----
-----
student-1@test.com 10.10.22.30 5c:51:4f:e6:a9:83 Win 10  test-mpsk  AP-515-2b:30  149E
AC      Student-MPSK --      49 (good)  702 (good)
Number of Clients :1
Info timestamp    :2602

AP-515-2b:30# sh ap mpskcache 5c:51:4f:e6:a9:83

Station MAC address :5c:51:4f:e6:a9:83
Seq no              :2284
Key                 : (6): d1 d7 ff a5 ed 78
ESSID               :test-mpsk
Name                :student-1@test.com
Role                :Student-MPSK
Server              :Not set
VLAN                :22
To Del              :0
Expire              :0s
Vlanhow             :254
Rolehow             :0
ACL Rule Index      :0
User panid          :13984993
Session timeout     :28800

AP-515-2b:30#

```

The breakdown of the clients are as follows and all are on the same VLAN/IP subnet.

Username	Clients	MAC address	IP address	User Pan id	AP-name
student-1@test.com	Ipod	2c:1f:23:d0:2f:48	10.10.22.31	13984993	AP-605H-5d:6b
	Win10	5c:51:4f:e6:a9:83	10.10.22.30	13984993	AP-515-2b:30
student-2@test.com	Win11	ce:55:81:30:f8:3c	10.10.22.20	4347809	AP-605H-5d:6b

Now we'll ping between the student-1's devices, note that they are associated to different APs and we find that the ping is successful.

Customer: Ariya Publ...

Summary

AI Insights

Location

Sessions

Profile

← student-1@test.c...

SESSIONS

ACCESS POINT

Total sessions: 14

Last refreshed: 1:20:23 PM

Manage

Overview

Applications

Security

Analyze

Live Events

IP Address | 10.10.22.30 (14)

Appli...	Sourc...	Desti...	Proto...	Sourc...	Dest ...	Action	Flags ⓘ	Pack...	St... ▾
Windows Mark...	52.167.163.114	10.10.22.30	TCP	443	49397	Permit	--	9	Active
Internet Contr...	10.10.22.30	10.10.22.31	ICMP	23	2048	Permit	R I F C	1	Active
Internet Contr...	10.10.22.30	10.10.22.31	ICMP	26	2048	Permit	R I F C	1	Active
Internet Contr...	10.10.22.30	10.10.22.31	ICMP	25	2048	Permit	R I F C	1	Active
Internet Contr...	10.10.22.30	10.10.22.31	ICMP	24	2048	Permit	R I F C	1	Active

Because the student-1's devices are on different APs, under the hood, the APs will make a tunnel encapsulation for this traffic.

Here is the datapath session table when we were pinging between 10.10.22.30 and .31

```
AP-605H-5d:6b# sh datapath session | incl 10.10.22.31
```

Datapath Session Table Entries

```

-----
Flags: A - Application Firewall Inspect
      C - client, D - deny, E - Media Deep Inspect
      F - fast age, G - media signal, H - high prio
      I - Deep inspect, L - ALG session, M - mirror, N - dest NAT
      O - Session is programmed through SDN/Openflow controller
      P - set prio, R - redirect, S - src NAT,
      T - set ToS, U - Locally destined, V - VOIP
      X - Http/https redirect for dpi denied session
      Y - no syn
      a - rtp analysis, h - Https redirect error page
      i - in offload flow, m - media mon
      p - Session is marked as permanent
      s - media signal
      d - DPI cache hit
      f - FIB init pending in session
      c - MSCS or SCS session
RAP Flags: 0 - Q0, 1 - Q1, 2 - Q2, r - redirect to conductor
           t - time based, i - in flow, l - local redirect
Flow Offload Denylist Flags: O - Openflow, E - Default, U - User os unknown, T - Tunnel
                             R - L3 route

17.57.145.39    10.10.22.31    6    5223  51581  0    0    0    9    dev30    6d41 9    2a8    i
10.10.22.31    17.57.145.39    6    51581  5223  0    0    0    9    dev30    6d41 a    3d6    Ci
17.57.145.39    10.10.22.31    6    5223  51581  0    0    0    10   dev30    6dc0 9    2a8    i
10.10.22.30    10.10.22.31    1    27    2048  0    0    0    0    tunnel 1    2f    1    3c    FCI
10.10.22.30    10.10.22.31    1    30    2048  0    0    0    0    tunnel 1    10    1    3c    FCI
10.10.22.30    10.10.22.31    1    29    2048  0    0    0    0    tunnel 1    1a    1    3c    FCI
10.10.22.30    10.10.22.31    1    28    2048  0    0    0    0    tunnel 1    25    1    3c    FCI
10.10.22.31    17.57.145.39    6    51581  5223  0    0    0    10   dev30    6dc0 a    3d6    Ci
10.10.22.31    10.10.22.30    1    29    0      0    0    0    0    tunnel 1    1a    1    3c    FRI
10.10.22.31    10.10.22.30    1    28    0      0    0    0    0    tunnel 1    25    1    3c    FRI
10.10.22.31    10.10.22.30    1    30    0      0    0    0    0    tunnel 1    10    1    3c    FRI
10.10.22.31    10.10.22.30    1    27    0      0    0    0    0    tunnel 1    2f    1    3c    FRI
10.10.22.31    10.10.22.30    17   4789  4789  0    0    0    0    dev6     2f    4    1b8   FA
10.10.22.30    10.10.22.31    17   4789  4789  0    0    0    0    dev6     2f    4    1b8   FCA

```

```
AP-605H-5d:6b#
```

Here is the pcap which was done on the switch to see the ICMP ping traffic between the two devices for student-1 that are on different AP. Note that there is, indeed an UDP encapsulation between the two APs the port that is used is VXLAN. Now when looked closer you'll see that the VNI=0 but it also carries group Policy ID that is automatically generated and assigned.

PWN packets.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.10.22.31

No.	Time	Source	Destination	Protocol	Length	Info
→ 13	0.910533945	10.10.22.30	10.10.22.31	ICMP	128	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 14)
← 14	1.374679895	10.10.22.31	10.10.22.30	ICMP	128	Echo (ping) reply id=0x0001, seq=35/8960, ttl=64 (request in 13)
→ 19	1.931189344	10.10.22.30	10.10.22.31	ICMP	128	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 20)
→ 20	1.988414611	10.10.22.31	10.10.22.30	ICMP	128	Echo (ping) reply id=0x0001, seq=36/9216, ttl=64 (request in 19)
→ 22	2.942973146	10.10.22.30	10.10.22.31	ICMP	128	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (reply in 23)
→ 23	3.012412241	10.10.22.31	10.10.22.30	ICMP	128	Echo (ping) reply id=0x0001, seq=37/9472, ttl=64 (request in 22)
→ 26	3.960523639	10.10.22.30	10.10.22.31	ICMP	128	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (reply in 27)
→ 27	4.011549891	10.10.22.31	10.10.22.30	ICMP	128	Echo (ping) reply id=0x0001, seq=38/9728, ttl=64 (request in 26)

<

> Frame 13: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface MirrorRxNet, id 0

> Ethernet II, Src: Intel_e6:a9:83 (5c:51:4f:e6:a9:83), Dst: Apple_d0:2f:48 (2c:1f:23:d0:2f:48)

> 802.1Q Virtual LAN, PRI: 1, DEI: 0, ID: 22

> Internet Protocol Version 4, Src: 10.10.22.30, Dst: 10.10.22.31

> User Datagram Protocol, Src Port: 4789, Dst Port: 4789

> Virtual eXtensible Local Area Network

> Flags: 0x04d5, Don't Learn

> Group Policy ID: 25825

> VXLAN Network Identifier (VNI): 0

> Reserved: 0

> Ethernet II, Src: Intel_e6:a9:83 (5c:51:4f:e6:a9:83), Dst: Apple_d0:2f:48 (2c:1f:23:d0:2f:48)

> Internet Protocol Version 4, Src: 10.10.22.30, Dst: 10.10.22.31

> Internet Control Message Protocol

And this is the return traffic and note that the group policy Id are the same and hence the traffic is allowed.

PWN packets.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

ip.addr==10.10.22.31

No.	Time	Source	Destination	Protocol	Length	Info
→ 13	0.910533945	10.10.22.30	10.10.22.31	ICMP	128	Echo (ping) request id=0x0001, seq=35/8960, ttl=128 (reply in 14)
← 14	1.374679895	10.10.22.31	10.10.22.30	ICMP	128	Echo (ping) reply id=0x0001, seq=35/8960, ttl=64 (request in 13)
→ 19	1.931189344	10.10.22.30	10.10.22.31	ICMP	128	Echo (ping) request id=0x0001, seq=36/9216, ttl=128 (reply in 20)
→ 20	1.988414611	10.10.22.31	10.10.22.30	ICMP	128	Echo (ping) reply id=0x0001, seq=36/9216, ttl=64 (request in 19)
→ 22	2.942973146	10.10.22.30	10.10.22.31	ICMP	128	Echo (ping) request id=0x0001, seq=37/9472, ttl=128 (reply in 23)
→ 23	3.012412241	10.10.22.31	10.10.22.30	ICMP	128	Echo (ping) reply id=0x0001, seq=37/9472, ttl=64 (request in 22)
→ 26	3.960523639	10.10.22.30	10.10.22.31	ICMP	128	Echo (ping) request id=0x0001, seq=38/9728, ttl=128 (reply in 27)
→ 27	4.011549891	10.10.22.31	10.10.22.30	ICMP	128	Echo (ping) reply id=0x0001, seq=38/9728, ttl=64 (request in 26)

<

> Frame 14: 128 bytes on wire (1024 bits), 128 bytes captured (1024 bits) on interface MirrorRxNet, id 0

> Ethernet II, Src: Apple_d0:2f:48 (2c:1f:23:d0:2f:48), Dst: Intel_e6:a9:83 (5c:51:4f:e6:a9:83)

> 802.1Q Virtual LAN, PRI: 0, DEI: 0, ID: 22

> Internet Protocol Version 4, Src: 10.10.22.31, Dst: 10.10.22.30

> User Datagram Protocol, Src Port: 4789, Dst Port: 4789

> Virtual eXtensible Local Area Network

> Flags: 0x04d5, Don't Learn

> Group Policy ID: 25825

> VXLAN Network Identifier (VNI): 0

> Reserved: 0

> Ethernet II, Src: Apple_d0:2f:48 (2c:1f:23:d0:2f:48), Dst: Intel_e6:a9:83 (5c:51:4f:e6:a9:83)

> Internet Protocol Version 4, Src: 10.10.22.31, Dst: 10.10.22.30

> Internet Control Message Protocol

Next, we'll ping between student-1 and student-2's devices that are on the same AP.

Customer: Ariya Publ...

← AP-605H-5d:6b

— Manage

Overview

Device

Clients

Security

Analyze

Clients

AP

512.15 MB

All	Connecting	Connected	Failed	Offline	Blocked	Wireless	Wired	Remote
2	0	2	0	0	0	2	0	0

Client Name	Status	IP Address	VLAN	AP Name	SSID	AP Role
student-2@test.com	Connected	10.10.22.20	22	AP-605H-5d:6b	test-mpsk	Student-MPSK
student-1@test.com	Connected	10.10.22.31	22	AP-605H-5d:6b	test-mpsk	Student-MPSK

And as expected they pings fail as the devices have different PAN-id and drop happens on the destination AP.

Customer: Ariya Publ...

← student-1@test.c...

Manage

Overview

Applications

Security

Analyze

Live Events

Events

Summary

AI Insights

Location

Sessions

Profile

SESSIONS

ACCESS POINT ▾

Total sessions: 6

Last refreshed: 1:25:52 PM ↻

IP Address | 10.10.22.31 (6)

⋮

Appli...	Sourc...	Desti...	Proto...	Sourc...	Dest ...	Action	Flags ⓘ	Pack...	St... ▾
> Secure Socket ...	17.57.145.39	10.10.22.31	TCP	5223	51581	Permit	--	5	Active
> Internet Contr...	10.10.22.20	10.10.22.31	ICMP	14	2048	Deny	D I F C	1	Denied
> Internet Contr...	10.10.22.20	10.10.22.31	ICMP	13	2048	Deny	D I F C	1	Denied
> Secure Socket ...	10.10.22.31	17.57.145.39	TCP	51581	5223	Permit	C	6	Active
> Internet Contr...	10.10.22.31	10.10.22.20	ICMP	13	0	Deny	D I F Y	0	Denied
> Internet Contr...	10.10.22.31	10.10.22.20	ICMP	14	0	Deny	D I F Y	0	Denied

Here we are looking for D flag (indicating drops) between 10.10.22.20 and 10.10.22.31. Note that PAN-id will not change for the users even though one might change the MPSK.

AP-605H-5d:6b# sh datapath session | incl 10.10.22.31

17.57.145.39	10.10.22.31	6	5223	51581	0	0	0	11	dev30	3fb2	5	16e	i
10.10.22.20	10.10.22.31	1	16	2048	0	0	0	0	dev30	2e	1	3c	FDCI
10.10.22.31	17.57.145.39	6	51581	5223	0	0	0	11	dev30	3fb2	6	25c	Ci
10.10.22.31	10.10.22.20	1	16	0	0	0	0	0	dev30	2e	0	0	FDYI
10.10.22.31	224.0.0.22	2	2	2	0	0	48	1	dev30	8c	2	50	FCA

AP-605H-5d:6b#

This is simple yet powerful way to enforce Microsegmentation for this specific use case.