

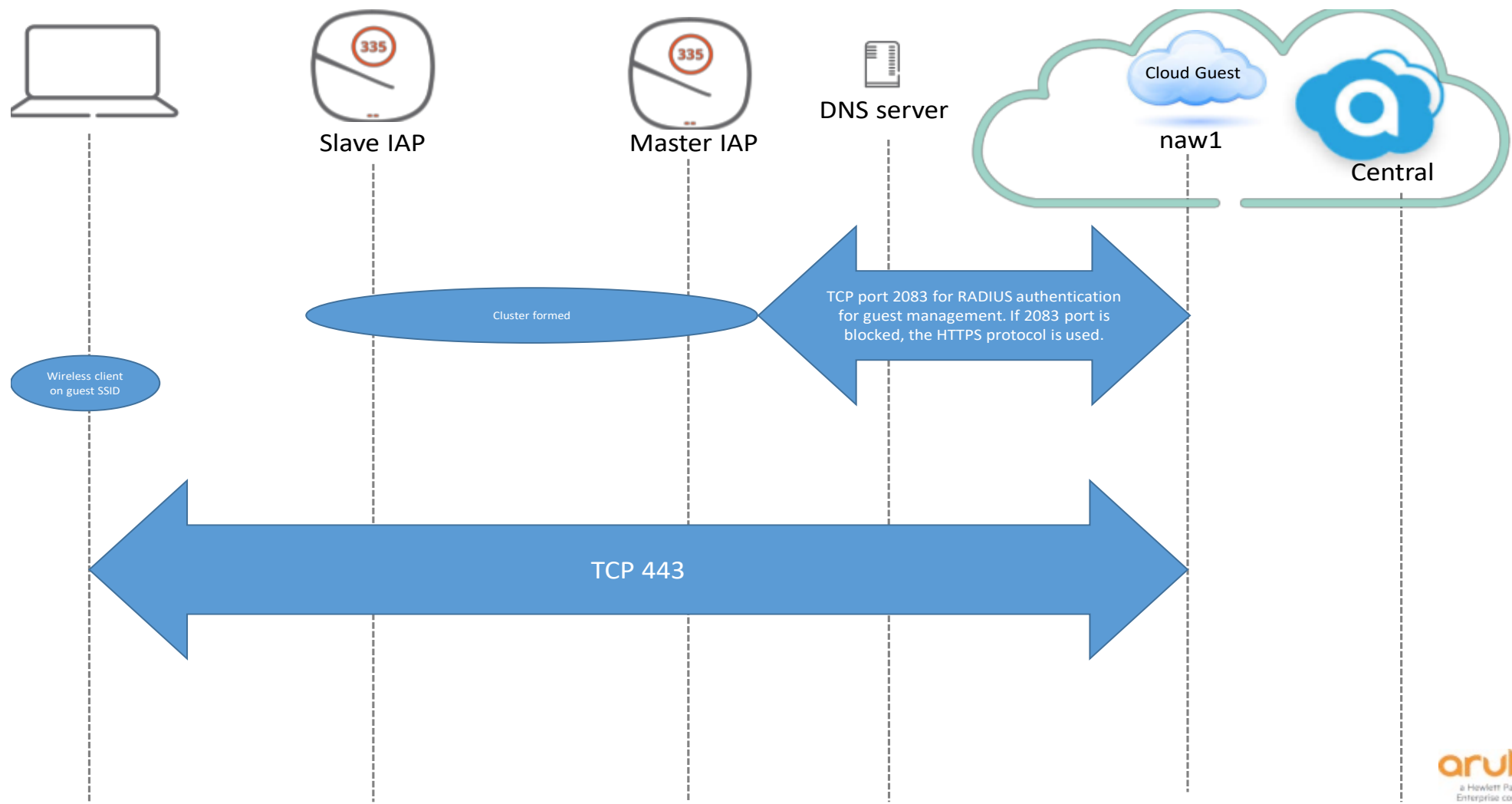
Airheads Tech Talks: Cloud Guest SSID on Aruba Central

Akhil Rajendran

Agenda

- Introduction to Cloud Guest.
- How to configure.
- Debugging on IAP.
- Adding Visitor accounts to Cloud Guest.
- Generating Reports from Central.

Architecture



Cloud Guest Types

- Anonymous
- Authenticated
- Facebook Wifi

Cloud Guest Type - Anonymous

- No credentials required.
- Plain, simple captive portal login.
- Guest password if required can be added to the login.
- MAC Caching – No option to remove the saved mac-address as of now.
- Session limit can be set.
- URL whitelisting.

Config Pushed to Instant AP

```
#show network
-----
Profile Name  ESSID      Clients  Type   Band  Authentication Method  Key Management  IP Assignment  Status  Zone  Coding  Active
-----
Anonymous    Anonymous  0        guest  all   External CP           WPA2-AES       NAT Mode      Enabled -    UTF-8   Yes

#show network Anonymous | in ECP
ECP Profile      :Anonymous_#guest#_

#show external-captive-portal Anonymous_#guest#_
Name              :Anonymous_#guest#_
Server            :ap1.cloudguest.central.arubanetworks.com
Port              :443
Url               :/portal/scope.cust-00bc49df203e4281907cf158062489da/Anonymous/capture
Auth Text         :
Redirect Url      :
Server Fail Throuth :Disable
Disable Auto Whitelist :Disable
Use HTTPs         :Yes
Server Offload    :No
Prevent Frame Overlay :Disable
In Used           :Yes
Redirect Mode     :Yes
Switch IP         :No
```

Debugging on IAP

#show clients

Client List

```
-----
Name      IP Address  MAC Address      OS      ESSID      Access Point      Channel  Type  Role      IPv6 Address
Signal    Speed (mbps)
-----
ak-phone  192.168.1.3  d8:1d:72:7d:75:67 iPhone  Anonymous  f0:5c:19:ca:3c:e8  149E    AC    Anonymous_#guest#_
fe80::1cef:a90:a9aa:5342  35(good)  325(good)
Number of Clients :1
```

Post Authenticating:

#show clients

Client List

```
-----
Name      IP Address  MAC Address      OS      ESSID      Access Point      Channel  Type  Role
IPv6 Address      Signal    Speed (mbps)
-----
ODKsDUXsQVS+qgmftddd+w==.D3TTaA  192.168.1.3  d8:1d:72:7d:75:67 iPhone  Anonymous  f0:5c:19:ca:3c:e8  149E    AC    Anonymous
fe80::1ceaf:a90:a9aa:5342  41(good)  433(good)
Number of Clients :1
```

There are 2 radius servers pushed from Central to Instant AP.

“AS1_#guest#_” uses RADSEC protocol – tcp 2083 to 35.154.164.176.

“AS2_#guest#_” uses https protocol – tcp 443 to 13.126.228.244.

#show radius status

Radius server status

Name	Server IP	Source IP	Server Name		Protocol	Port	NAS IP		
Connected sockets	Status	Last connection	tried at	Next connection at					

AS2_#guest#_	13.126.228.244	192.168.1.12	ap1-elb.cloudguest.central.arubanetworks.com		RADIUS/TLS	443	192.168.1.12	1	
CONNECTED	2019-03-21 14:08:58.184913	Not	Applicable						
AS1_#guest#_	35.154.164.176	192.168.1.12	ap1.cloudguest.central.arubanetworks.com		RADIUS/TLS	2083	192.168.1.12	1	
CONNECTED	2019-03-21 14:08:58.188131	Not	Applicable						

All the radius request would be sent to AS1 as it is first in order.

In any event tcp 2083 is blocked, radius request would be redirected to AS2.

#show radius status

Radius server status

Name	Server IP	Source IP	Server Name	Protocol	Port	NAS IP	
Connected sockets	Status	Last connection tried at	Next connection at				
----	-----	-----	-----	-----	----	-----	-----
AS2_#guest#_	13.126.228.244	192.168.1.12	ap1-elb.cloudguest.central.arubanetworks.com	RADIUS/TLS	443	192.168.1.12	1
CONNECTED	2019-03-21 14:08:58.184913	Not Applicable					
AS1_#guest#_	35.154.164.176	192.168.1.12	ap1.cloudguest.central.arubanetworks.com	RADIUS/TLS	2083	192.168.1.12	0
INIT	2019-03-21 15:12:10.667178	2019-03-21 15:12:20.10667178					

Client's session to the cloudquest URL:

```
# show datapath session | include 35.154.164.176
```

35.154.164.176	192.168.1.3	6	443	62144	0	0	0	1	dev20	6d	F
192.168.1.3	35.154.164.176	6	62144	443	0	0	0	1	dev20	6d	FC

IAP's attempt to contact AS1:

```
# show datapath session | include 35.154.164.176
```

35.154.164.176	192.168.1.12	6	2083	53511	0	0	0	1	local	51	Y
192.168.1.12	35.154.164.176	6	53511	2083	0	0	0	1	local	51	C

IAP communicates with AS2:

```
# show datapath session | include 13.126.228.244
```

13.126.228.244	192.168.1.12	6	443	57852	0	0	0	1	local	49c2	
192.168.1.12	13.126.228.244	6	57852	443	0	0	0	1	local	49c2	C

Security debug logs from IAP:

When radsec establishes:

show log security | in AS1

```
Mar 21 15:28:02 stm[4409]: <124004> <DEBUG> |AP f0:5c:19:ca:3c:e8@192.168.1.12 stm| Starting SSL connection to server
AS1_#guest#_ ip 35.154.164.176 port 2083
Mar 21 15:28:02 stm[4409]: <124004> <DEBUG> |AP f0:5c:19:ca:3c:e8@192.168.1.12 stm| TLS connection succeeded to AS1_#guest#_
Mar 21 15:28:02 stm[4409]: <124004> <DEBUG> |AP f0:5c:19:ca:3c:e8@192.168.1.12 stm| check and send queued requests to server
AS1_#guest#_ on socket 13
Mar 21 15:28:24 stm[4409]: <124004> <DEBUG> |AP f0:5c:19:ca:3c:e8@192.168.1.12 stm| status server processed for server
AS1_#guest#_
```

When radsec fails:

show log security | in AS1

```
Mar 21 15:31:56 stm[4409]: <124004> <DEBUG> |AP f0:5c:19:ca:3c:e8@192.168.1.12 stm| SSL socket not available for server,creating:
AS1_#guest#_
Mar 21 15:31:56 stm[4409]: <124004> <DEBUG> |AP f0:5c:19:ca:3c:e8@192.168.1.12 stm| Resolve DNS for server AS1_#guest#_ with cmd
/aruba/bin/dns_resolv ap1.cloudguest.central.arubanetworks.com
Mar 21 15:31:56 stm[4409]: <124004> <DEBUG> |AP f0:5c:19:ca:3c:e8@192.168.1.12 stm| Starting SSL connection to server
AS1_#guest#_ ip 35.154.164.176 port 2083
Mar 21 15:31:56 stm[4409]: <199802> <ERRS> |AP f0:5c:19:ca:3c:e8@192.168.1.12 stm| rc_rad_tls.c, radsec_resume_connection:1079:
TCP connect to server AS1_#guest#_ failed to establish TLS connection to server AS1_#guest#_. Retry in 320 seconds
```

When both servers are down use the option 'Allow Internet In Failure'.

#show external-captive-portal Anonymous_#guest#_

Name	:Anonymous_#guest#_
Server	:ap1.cloudguest.central.arubanetworks.com
Port	:443
Url	:/portal/scope.cust-00bc49df203e4281907cf158062489da/Anonymous/capture
Auth Text	:
Redirect Url	:
Server Fail Throut	:Disable / Enable
Disable Auto Whitelist	:Disable
Use HTTPs	:Yes
Server Offload	:No
Prevent Frame Overlay	:Disable
In Used	:Yes
Redirect Mode	:Yes
Switch IP	:No

URL Whitelisting:

```
# show access-rule Anonymous_#guest#_
```

```
Access Rules
```

Dest IP	Dest Mask	Eth Type	Dest Match	Protocol (id:sport:eport)	Application	Action	Log	TOS	802.1P	Blacklist
App Throttle (Up:Down)	Mirror	DisScan	ClassifyMedia							
alias	cnn.com	IPv4/6	match	https		permit				
alias	bbc.com	IPv4/6	match	https		permit				

Session Timeout

```
# show ap debug auth-tracebuf
```

```
Mar 22 09:29:19 cp-pap-auth-request -> 68:c4:4d:89:b8:44 f0:5c:19:23:ce:81/AS1_#guest#_ - -
yzTmsIWkQViqzAle2ghwKA==.D3XvFg
Mar 22 09:29:19 cp-pap-auth-success <- 68:c4:4d:89:b8:44 f0:5c:19:23:ce:81/AS1_#guest#_ - - success
Mar 22 09:29:19 rad-acct-start -> 68:c4:4d:89:b8:44 f0:5c:19:23:ce:81 - -
Mar 22 09:29:35 rad-acct-int-update -> 68:c4:4d:89:b8:44 f0:5c:19:23:ce:81 - -
Mar 22 09:31:17 rad-acct-stop -> 68:c4:4d:89:b8:44 f0:5c:19:23:ce:81 - -
```

Cloud Guest Type - Authenticated

- Username/Password along with email and phone based verification.
- Social login – Facebook, Google+, Twitter, LinkedIn

Facebook login

Splash Page > Authenticated

✓ Configuration

Name:

Type: ☒ Anonymous ☒ Authenticated ☐ Facebook Wi-Fi

Username/Password: ☐

Social Login: ☒

Facebook: ☒

Client ID:

Client Secret:

Twitter: ☐

show clients

Client List

Name	Signal	IP Address	MAC Address	OS	ESSID	Access Point	Channel	Type	Role	IPv6
Address		Speed (mbps)								
-----	-----	-----	-----	--	-----	-----	-----	----	----	----
-----	-----	-----								
5U7/JrfqQbqM7WeigqIzOw==.D3VW0A		192.168.1.5	68:c4:4d:89:b8:44	Linux	Facebook	f0:5c:19:ca:3c:e8	6	GN	Facebook	
fe80::6ac4:4dff:fe89:b844	40 (good)	52 (good)								

show access-rule Facebook

Access Rules

Dest IP	Dest Mask	Eth Type	Dest Match	Protocol	(id:sport:eport)	Application	Action	Log	TOS	802.1P	Blacklist	App
Throttle	(Up:Down)	Mirror	DisScan	Classify	Media							
-----	-----	-----	-----	-----	-----	-----	-----	---	---	-----	-----	-----
-----	-----	-----	-----									
any	any	IPv4/6	match	any			permit					



ArubaCG

APP ID: 2146308358796009

ON

Status: Live

[View Analytics](#)[Help](#)Visit [our reference](#) on recent Facebook Login updates.[Dashboard](#)[Settings](#)[Roles](#)[Alerts](#)[App Review](#)PRODUCTS [+](#)[Facebook Login](#)[Settings](#)[Quickstart](#)[Activity Log](#)

Use the Quickstart to add Facebook Login to your app. To get started, select the platform for this app.



iOS



Android



Web

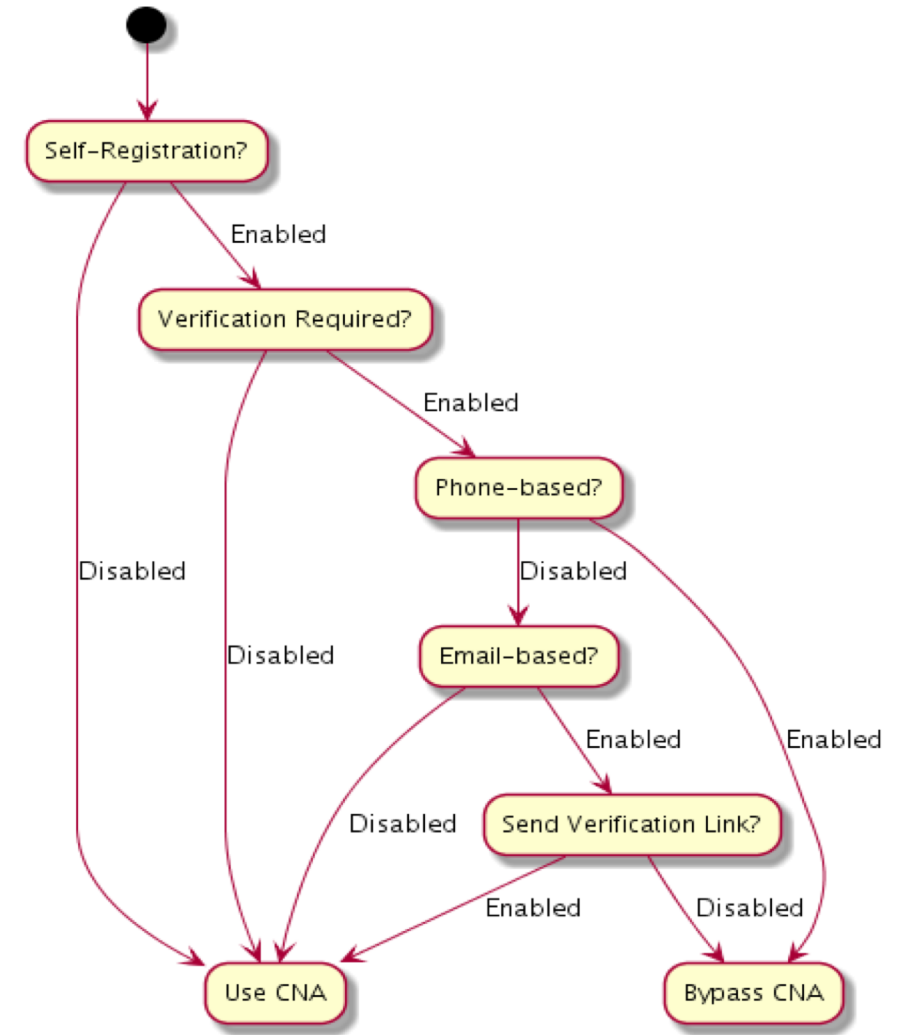


Other

Self Registration Workflow for Apple CNA

Captive portal detection URL's:

- <http://www.apple.com/library/test/success.html>
- <http://captive.apple.com/hotspot-detect.html>



Sponsored Guest:



Allowed Sponsor Domains:

hp.com



[Add domain](#)

Allowed Sponsor Emails (Optional):

**Please specify additional email address to receive approval emails.
They don't have to be in the same domain as sponsored domain.**




Error: 'Sponsor not authorized'

ap1.cloudguest.central.arubanetworks.com

EN

Register

Username

 123456789


Sponsor

Enter the email address of an authorized sponsor who will approve your registration:

Sponsor not authorized

akhil.rajendran@hpe.com

Register

 Back

Session Limit / Data Limit

show ap debug auth-trace-buf

```
Mar 22 13:13:07 cp-pap-auth-request -> d8:1d:72:7d:75:67 f0:5c:19:23:ce:93/AS1_#guest#_ - -
T2jV0x48TAuTCk/7KYNn6g==.D3Yjig
Mar 22 13:13:07 cp-pap-auth-success <- d8:1d:72:7d:75:67 f0:5c:19:23:ce:93/AS1_#guest#_ - - success
Mar 22 13:13:07 rad-acct-start -> d8:1d:72:7d:75:67 f0:5c:19:23:ce:93 - -
Mar 22 13:15:17 rad-acct-int-update -> d8:1d:72:7d:75:67 f0:5c:19:23:ce:93 - -
Mar 22 13:15:25 rad-acct-stop -> d8:1d:72:7d:75:67 f0:5c:19:23:ce:93 - -
```

show clients

Client List

Name	IP Address	MAC Address	OS	ESSID	Access Point	Channel	Type	Role	IPv6
Address	Signal	Speed (mbps)							
-----	-----	-----	--	-----	-----	-----	----	----	-----
-----	-----	-----							
ak-iphone	192.168.1.3	d8:1d:72:7d:75:67		Social	f0:5c:19:ca:3c:e8	52E	AC	Social_#guest#_	
fe80::c77:cc59:6a3f:df9	25 (good)	433 (good)							

Facebook Wifi

The screenshot shows the Aruba Central web interface for configuring a guest access app. The browser address bar shows the URL: `https://app2-ap.central.arubanetworks.com/frontend/#/EDITCAPTIVEPORTAL`. The left sidebar contains navigation links: **aruba Central** (with a '19 days left' badge), **CURRENT APP GUEST ACCESS**, **Search Current App** (Find devices, clients and networks), **Overview** (Guest network overview), **Splash Page** (Create customized splash pages), and **Visitors** (Monitor guest sessions). The main content area is titled **FILTER GUEST ACCESS default** (0 Total Devices | 0 Offline APs | 0 Offline SWITCHES). Below this, the **Splash Page > default** configuration is shown. The **Configuration** section includes:

- Name:** default
- Type:** A slider set to **Facebook Wi-Fi** (between Anonymous and Authenticated).
- Facebook WiFi configuration:** [Configure now...](#)
- Allow Internet In Failure:** Toggle off
- Override Common Name:** Toggle off
- Share This Profile:** Toggle on
- Simultaneous Login Limit:** No Limit
- Whitelist URL:** An empty text box with a trash icon and a '+ Add more URLs' link.

 At the bottom right are **Cancel** and **Save Settings** buttons. A footer message states: 'Due to a change in Google APIs the use of Google+ authentication methods may not be available at this time for the Guest Access App.' The page is labeled '1 of 1'.

Cloud Guest - Visitors

- Generate accounts that can be given to guests.
- Cannot be configured at MSP level.
- Visitor accounts can be created for username/password login.
- Visitor accounts can be modified and new password can be sent via SMS or email.

Guest Access > Visitors

Show visitors for network:

Facebook

▼

Session

Session List (4)

▼ VISITORS	LOGIN TYPE	BROWSER	▼ MAC ADDRESS	DEVICE TYPE	OS NAME	LOGIN TIME	SESSION TIME (SECS)
D8-1D-72-7D-75-67	web		D8-1D-72-7D-75-67	iPhone	iOS	3/22/19 14:26	14

Reports

- Reports can be pulled from Central to have track of various parameters like:
 - Client usage
 - Application usage
 - Client sessions
- Can be automated or ran as and when required.
- Report can be downloaded or sent to any email addresses.

Thank You

Q & A