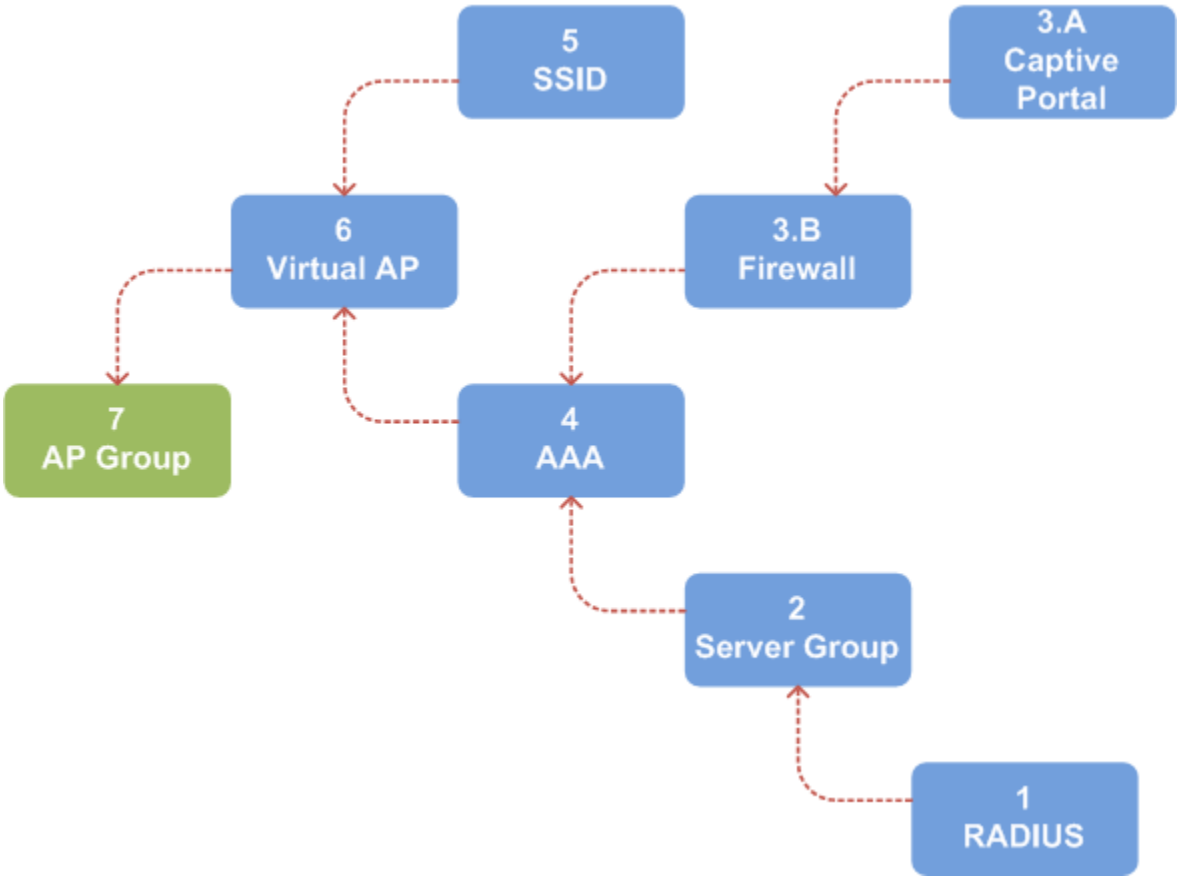
2.2 *Aruba – Guest Configuration*

The easiest way to understand the Aruba configuration is to compartmentalize each element of the configuration. The eduroam service is built up of the following elements which form a Virtual AP (VAP). Multiple VAP's (i.e. eduroam & Guest) can belong to an AP Group to which an AP is provisioned to.



2.2.1 Per-Controller Configuration

IMPORTANT: each Aruba controller stores a locally significant VLAN database. This is not synchronised between Master and Local and must be manually created on each controller.

On each controller select `Configuration` (tab) ▼ `NETWORK` ► `VLANs`. Ensure VLAN ID (tab) is selected and click Add a VLAN.

Under Configuration configure each VLAN as required. On selecting the *Port-Channel ID* the *Port Selection* should automatically refresh to reflect the controller port-channel configuration.

As basic firewall rules are defined for the Captive Portal, a Layer-3 interface is required.

On each controller select `Configuration` (tab) ▼ `NETWORK` ► `IP`. Ensure the `IP Interfaces` (tab) is selected and click `Edit` against the VLAN to be configured. Each Controller is configured with an IP address between [1-4] in the last octet.

2.2.2 *Master Controller Configuration*

1 RADIUS

The backend RADIUS server used for 802.1X authentication of users must be specified.

Select `Configuration` (tab) ▼ `ADVANCED SERVICES` ► `All Profiles`. Expand ⊞ `Wireless LAN` ⊞ `RADIUS Server`. Specify a profile name, which is *{service}.{radius-dns}*. (e.g. guest1.domain.co.uk), for each server.

Name	`guest1.domain.co.uk`	`guest2-backup.domain.co.uk`
Host	`192.168.*.*`	`192.168.*.*`
Key	`<removed>`	`<removed>`
Auth Port	`1645`	`1645`
Acct Port	`1646`	`1646`
Retransmits	`3`	`3`
Timeout	`5`	`5`
NAS ID	`aruba`	`Aruba`
NAS IP	`-`	`-`
Enable IPv6	`Disable`	`Disable`
Source Interface	`VLAN 710`	`VLN 710`
Use MD5	`Disabled`	`Disable`
Use IP address for calling station ID	`Disabled`	`Disable`
Mode	`Enabled`	`Enable`
Lowercase MAC addresses	`Disabled`	`Disable`
MAC address delimiter	`None`	`None`
Service-type of FRAMED-USER	`Disabled`	`Disable`

2 Server Group

Select `Configuration` (tab) ▼ `ADVANCED SERVICES` ► `All Profiles`. Expand ⊞ `Wireless LAN` ⊞ `Server Group`. Select the `Guest.srvrgrp` server group.

On selecting `New`, RADIUS server defined in step 1 can be selected. Add each RADIUS server to the group as required.

No server rules are defined.

3 A - Captive Portal

The Captive Portal profile defines the behaviour of the captive portal. Select `Configuration` (tab) ▼ `ADVANCED SERVICES` ► `All Profiles`. Expand ⊞ `Wireless LAN` ⊞ `Captive Portal Authentication`. The `Guest.captiveportal` profile is configured as follows:

Setting	Value	Notes
Default Role	`Guest`	
Default Guest Role	`Guest`	
Redirect Pause	`0`	
User Login	`Enabled`	
Guest Login	`Disabled`	
Logout popup window	`Disabled`	
Use HTTP for Authentication	`Disabled`	
Login wait minimum wait	`5 (sec)`	
Login wait maximum wait	`10 (sec)`	
Logon wait CPU utilization threshold	`60 (%)`	
Mac Authentication failures	`0`	
Show FQDN	`Disabled`	
Authentication Protocol	`PAP`	Authentication protocol supported by MERU IDM
Login page	`https://guest.domain.co.uk/portal/Guest-Aruba/10.1.0.1?switchip=aruba-a.hor.domain.co.uk`	… where `guest.domain.co.uk` is the SLB VIP 172.18.*.*, *Guest-Aruba* is the Portal configured on the MERU IDM, and `?switchip=aruba-a.domain.co.uk` is the calling station ID. See *Aruba <> MERU IDM Integration Notes* (a) below.
Welcome Page	`None`	
Show Welcome Page	`Disabled`	
Add switch IP address in the redirection ULR	`Disabled`	
Adding user vlan in redirection URL	`Disabled`	
Add a controller interface in the redirection URL	`None`	
Allow onlu one active user session	`Enabled`	
White List	`Null`	
Black List	`Null`	
Show the acceptable use policy page	`Disabled`	
User idle timeout	`Null`	
Redirection URL	`https://www.domain.co.uk/isd/common/wireless/Guest/authenticated`	See *Aruba <> MERU IDM Integration Notes* (b) below.
Bypass Apple Captive Network Assistant	`Enabled`	

Aruba <> MERU IDM Integration Notes
During initial configuration the following was observed:

a. On association to the Guest SSID the captive portal redirection only works if the Login Page is configured as:
`https://guest.domain.co.uk/portal/Guest-Aruba/10.1.0.1?switchip=aruba-a.domain.co.uk.`
This is a hack as the Meru IDM reads the value of `switchip=`, encapsulates it **`https://`**`aruba-a.domain.co.uk`**`/cgi-bin/login`**, and redirects post-authentication. To bypass the somewhat meaningless "User authenticated" page the Redirect URL is configured as::
`https://www.domain.co.uk/isd/common/wireless/Guest/authenticated`.

b. This does introduce resilience issues. The login page value:
`https://guest.domain.co.uk/portal/Guest-Aruba/10.1.0.1?switchip=aruba-a.hor.domain.co.uk`
is propagated from the MASTER to the LOCAL. If the MASTER fails, the MERU IDM will hand off post-authentication to aruba-a.hor.domain.co.uk which has failed, thus the service will fail.

c. A change request so that the *Add switch IP address in the redirection URL* can be toggled between IP and FQDN was submitted on Friday, 27 September 2013 09:05.

3 B - Firewall

It is at this point we need to configure firewall rules. These basically allow access to the following prior to Guest Captive Portal authentication.

- YOURCOMPANY Web Site - www.domain.co.uk (172.18.*.*)
- Guest Captive Portal - guest.domain.co.uk (172.18.*.*)
- Apple IOS Fix-up (www.apple.com) *

* Since Apple IOS 6.01 release, Apple enabled support for the WISPr draft protocol. This is discussed in detail in the Captive Bypassing section of the Cisco Wireless LAN Controller WLAN Configuration Guide, Release 7.4 (http://www.cisco.com/en/US/docs/wireless/controller/7.4/configuration/guides/wlan/config_wlan_chapter_010001.html).

Defining the Captive Portal profile:

a. **Configure Destinations**: Select `Configuration` (tab) ▼ `ADVANCED SERVICES` ▶ `Stateful Firewall` ▶ `Destinations` (tab). Create the following destinations:

IP Version	`IPv4`
Destination Name	`Guest.apple.dst`
Destination Description	`Guest www.apple.com Destination`
Invert	`Disable`
Add	
Rule Type	`Name`
Domain Name	`apple.com`

Add > Apply	

IP Version	IPv4
Destination Name	Guest.domain.co.uk.dst
Destination Description	Guest www.domain.co.uk Destination
Invert	Disable
Add	
Rule Type	Name
Domain Name	domain.co.uk
Add > Apply	

IP Version	IPv4
Destination Name	Guest.idm.dst
Destination Description	Guest Meru IDM Captive Portal Destination
Invert	Disable
Add	
Rule Type	Network
IP Address	172.18.*.*
Netmask/ Range	255.255.255.255
Add > Apply	

b. **Configure Policies:** Select Configuration (tab) ▼ SECURITY ► Access Control ► Policies (tab) and select the Add button. Create the following policies:

Policy Name	Guest.allow.apple.acl
Policy Type	Session
Add	
IP Version	IPv4
Source	Any
Destination	Alias > Guest.apple.dst *(as created in 3a)*
Service	Any
Action	Permit
Log	Disabled
Mirror	Disabled
Queue	Low
Time Range	None
Pause ARM Scanning	Disabled
Black List	Disabled
Classify Media	Disabled
TOS	None
802.1p Priority	None
Add > Done	

Policy Name	Guest.allow.YOURCOMPANY.acl

Policy Type	`Session`
Add	
IP Version	`IPv4`
Source	`Any`
Destination	`Alias > Guest.domain.co.uk.dst` *(as created in 3a)*
Service	`Any`
Action	`Permit`
Log	`Disabled`
Mirror	`Disabled`
Queue	`Low`
Time Range	`None`
Pause ARM Scanning	`Disabled`
Black List	`Disabled`
Classify Media	`Disabled`
TOS	`None`
802.1p Priority	`None`
Add > Done	

Policy Name	`Guest.allow.idm.acl`
Policy Type	`Session`
Add	
IP Version	`IPv4`
Source	`Any`
Destination	`Alias > Guest.idm.dst` *(as created in 3a)*
Service	`Any`
Action	`Permit`
Log	`Disabled`
Mirror	`Disabled`
Queue	`Low`
Time Range	`None`
Pause ARM Scanning	`Disabled`
Black List	`Disabled`
Classify Media	`Disabled`
TOS	`None`
802.1p Priority	`None`
Add > Done	

Click **Apply** to save the changes.

c. **Configure Role:** Select `Configuration` (tab) ▼ `SECURITY` ► `Access Control` ► `User Roles` (tab). Select Add and under ***Misc Configuration*** (right pane) configure as follows:

Role Name	`Guest.fw.rule`
Re-authentication Interval	`0`

Role VLAN ID	790
Bandwidth Contract Upstream	Guest.bw.upstream – Per User
Bandwidth Contract Downstream	Guest.bw.downstream – Per User
VPN Dialer	Not Assigned
L2TP Pool	Not Assigned
PP2T Pool	Not Assigned
Captive Portal Profile	Guest.captiveportal
Max Sessions	0
Stateful NTLM Profile	Not Assigned
Stateful Kerberos Profile	Not Assigned
WISPr Profile	Not Assigned

Within the same window, under ***Firewall Polices*** (left pane) select the Add button and select `logon-control (session)` from the *Choose From Configured Policies* drop-down. In addition, add the policies created in 3b. The final list should look something like:

- logon-control
- Guest.allow.apple.acl
- Guest.allow.YOURCOMPANY.acl
- Guest.allow.idm.acl
- captiveportal (pre-defined)

The order is **important** to avoid 'too many redirects error'! If out of order the ▼▲ arrows can be user to re-position.

4 AAA

Select `Configuration` (tab) ▼ `ADVANCED SERVICES` ► `All Profiles`. Expand ⊞ `Wireless LAN` ⊞ `AAA`. Select the `Guest.aaa` profile.

Initial role	Guest.fw.policy
MAC Authentication Default Role	denyall
802.1X Authentication Default Role	**denyall**
L2 Authentication Fail Through	Disable
User idle timeout	Disable
RADIUS Interim Accounting	Enable
User derivation rules	--NONE--
Wired to Wireless Roaming	Enable
SIP authentication role	--NONE--
Device Type Classification	Enable
Enforce DHCP	Enable

Expand ⊞ `Guest.aaa profile`. The following options should be set to the profiles previously configured.

802.1X Authentication Profile	None
802.1X Authentication Server Group	Guest.srvrgrp

5 SSID

Select `Configuration` (tab) ▼ `ADVANCED SERVICES` ► `All Profiles`. Expand ⊞ `Wireless LAN` ⊞ `SSID`. Select the `eduroam.ssid` profile and ensure the `Basic` tab is selected.

Network	
Network Name (SSID)	`Guest`
802.11 Security	
Network Authentication	`None`

6 Virtual AP

Select `Configuration` (tab) ▼ `ADVANCED SERVICES` ► `All Profiles`. Expand ⊞ `Wireless LAN` ⊞ `Virtual AP`. Select the `Guest.vap` and ensure the `Basic` tab is selected..

General	
Virtual AP enable	`Enabled`
VLAN	`748` (eduroam-ext)
Forward mode	`Tunnel`
RF	
Allowed band	`All`
Band Steering	`Disable`
Steering Mode	`-`
Broadcast/Multicast	
Dynamic Multicast Optimization (DMO)	`Disable`
Drop Broadcast and Multicast	`Disable`
Convert Broadcast ARP requests to unicast	`Enable`

7 AP Group

The AP Group brings together the previously configured profiles and AP's are provisioned to a group.

Prior to configuring the AP Groups, AP System profiles must be defined. Select `Configuration` (tab) ▼ `ADVANCED SERVICES` ► `All Profiles`. Expand ⊞ `AP` ⊞ `AP System`. The following profiles are defined:

Profile	**aruba-a_802.11a**	**aruba-a_802.11g**	**aruba-b_802.11a**	**aruba-b_802.11g**
General				
RF Band	a	g	a	g
RF Band for AM mode scanning	All	All	All	All

Native VLAN ID	1	1	1	1
Corporate DNS Domain				
SNMP sysContact				
LED operating mode (11n/11ac APs only)	normal	normal	normal	normal
SAP MTU				
Spanning Tree	Disable	Disable	Disable	Disable
LMS Settings				
LMS IP *VRRP VIP*	10.1.0.10	10.1.0.10	10.1.0.11	10.1.0.11
Backup LMS IP				
LMS IPv6				
Backup LMS IPv6				
LMS Preemption				
LMS Hold-down Period				
Remote AP {all default settings}				

Select `Configuration` (tab) ▼ `WIRELESS` ► `AP Configuration`. Select the required AP Group and expand ⊞ `Wireless LAN` ⊞ `Virtual AP`. Add the profiles as follows:

Name	AAA Profile	SSID Profile	VLAN	Forward mode	Virtual AP Enabled
`Guest.vap`	`Guest.aaa`	`Guest.ssid`	`790`	`Tunnel`	`Enabled`

When an AP is connected, assuming the Layer-2 and Layer-3 is correctly configured (see 4.4 Access Point) the AP will join the controller. Select `Monitoring` (tab) ▼ `NETWORK` ► `All Access Points`.

To Provision an Access Point, select `Configuration` (tab) ▼ `WIRELESS` ► `AP Installation`. Highlight the AP MAC and select the Provision button. From the drop-down an *AP Group* can be selected and applied.