!!! 6.3.1.3 UPGRADE WARNING !!!

First of all I'd like to warn you guys going to 6.3 not to jump straight to the latest recommended version of 6.3.1.3. I ran into a bug with one of my upgrades that made the controller unable to talk PAPI with the APs and had to rollback.

Workaround: Jump first to 6.3.1.2 then to 6.3.1.3

Solution: It's solved in the upcoming 6.3.1.4 that is scheduled for release on the 14th of March.

Tweaking your controllers in 6.3

Having that said, let's move on to the tutorial! From now on I'll expect you to have your aruba controllers on ArubaOS 6.3.x.I'll be trying to do the configuration and verifying from the web UI as much as I can to make this tutorial usefull to as many as possible.

Except for all the new hardware support and the possibility for deploying 802.11ac there's lots of new/improved features that'll benefit your existing installation and I'll be highlighting some of these features in this tutorial:

Centralized Licensing

Introduced in 6.3 comes the long awaited ability to pool your licenses across multiple controllers. This means that you don't have to buy double amount of licenses for your APs to achieve redundancy and if you're currently using a non-redundant setup the only thing you need to add is hardware and configure centralized licensing.

The two supported models are:

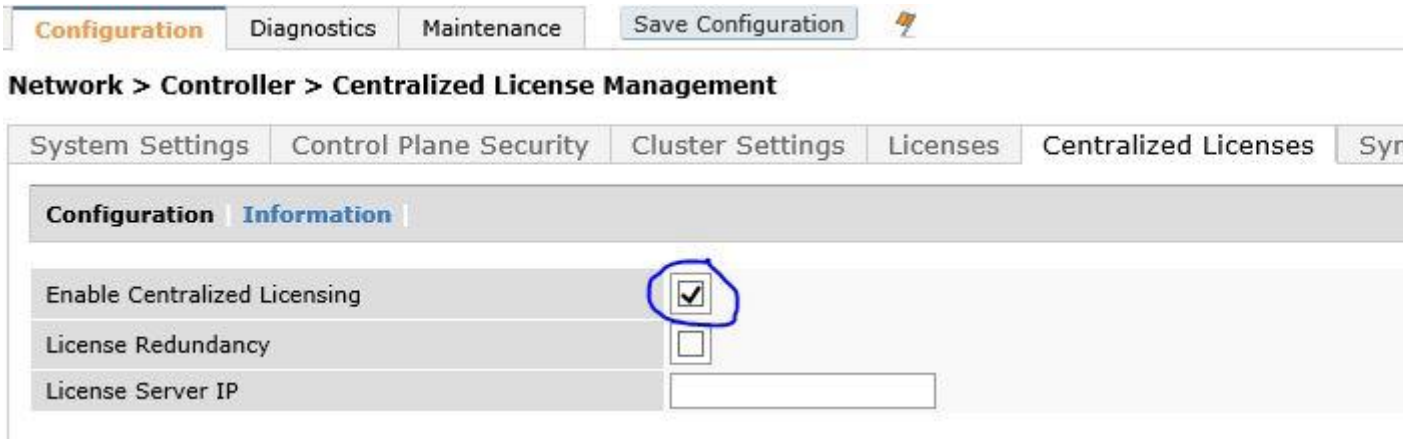
1. Licenses shared over one master-local deployment. (not multiple master-local deployments in the same pool)
2. Licenses shared over an all-master deployment.

Make sure you've got all your controllers on the same Aruba OS version (6.3.x+) then follow the below guides to set it up.

To enable centralized licensing in your Master-Local deployment:

On your active master controller, navigate to Configuration -> Controller -> Centralized Licenses

Check "Enable Centralized Licensing".



Click "apply" and "Save Configuration". That's it, you've got centralized licensing! Your master controller will be your licensing server and if you have a backup master it will be your backup licensing server.

Verify by clicking "information" and you should see your locals as licensing clients, how much licenses they are contributing to the pool with and how much each is using.

To enable centralized licensing in your All-Master deployment:

You'll have to pick one of your controllers to act as a licensing master. Log in to that controller, navigate to: Configuration -> Controller -> Centralized Licenses.

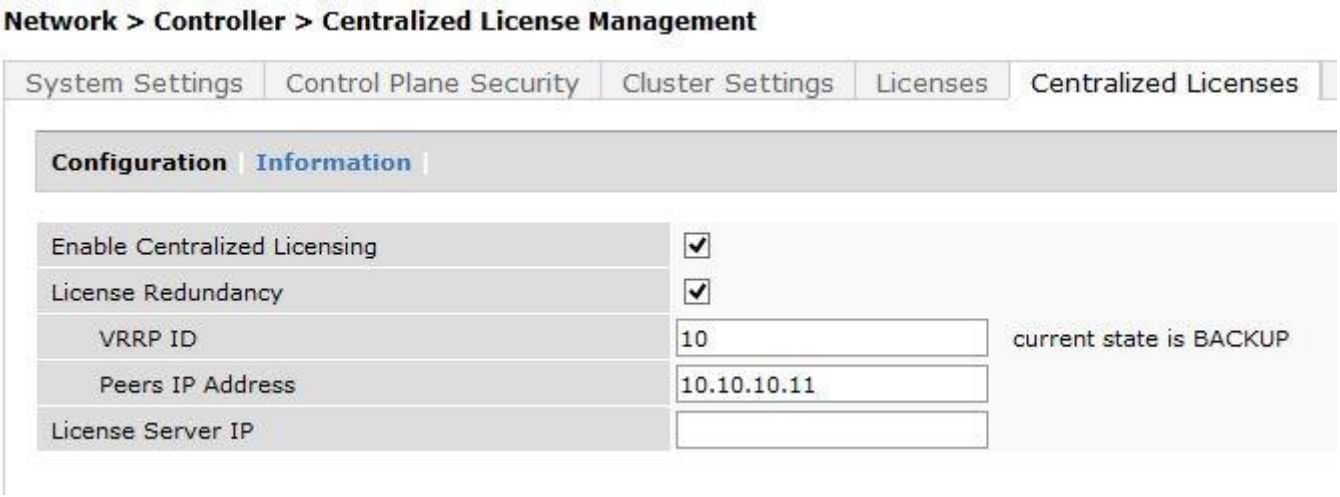
If you just want one licensing server with no backup, look at the above screenshot and just check "Enable Centralized Licensing" accordingly. If you want a backup licensing master you'll need to configure a VRRP between two of your master controllers that will act as the licensing server for the rest of your master controllers.

To create a VRRP, you need two of your controllers to reside on the same layer2 subnet and both have an IP address on that subnet. You'll then pick a third IP to become a virtual IP residing between the controllers which for your preferred licensing master will be active and your backup licensing master will be backup. For details on how to create a VRRP address, please check the section for VRRP in the user guide attached. (Page 529)

In the below example I've shared licenses across three master controllers with Master-01 as primary licensing server, Master-02 as backup licensing server and Master-03 as a licensing client.

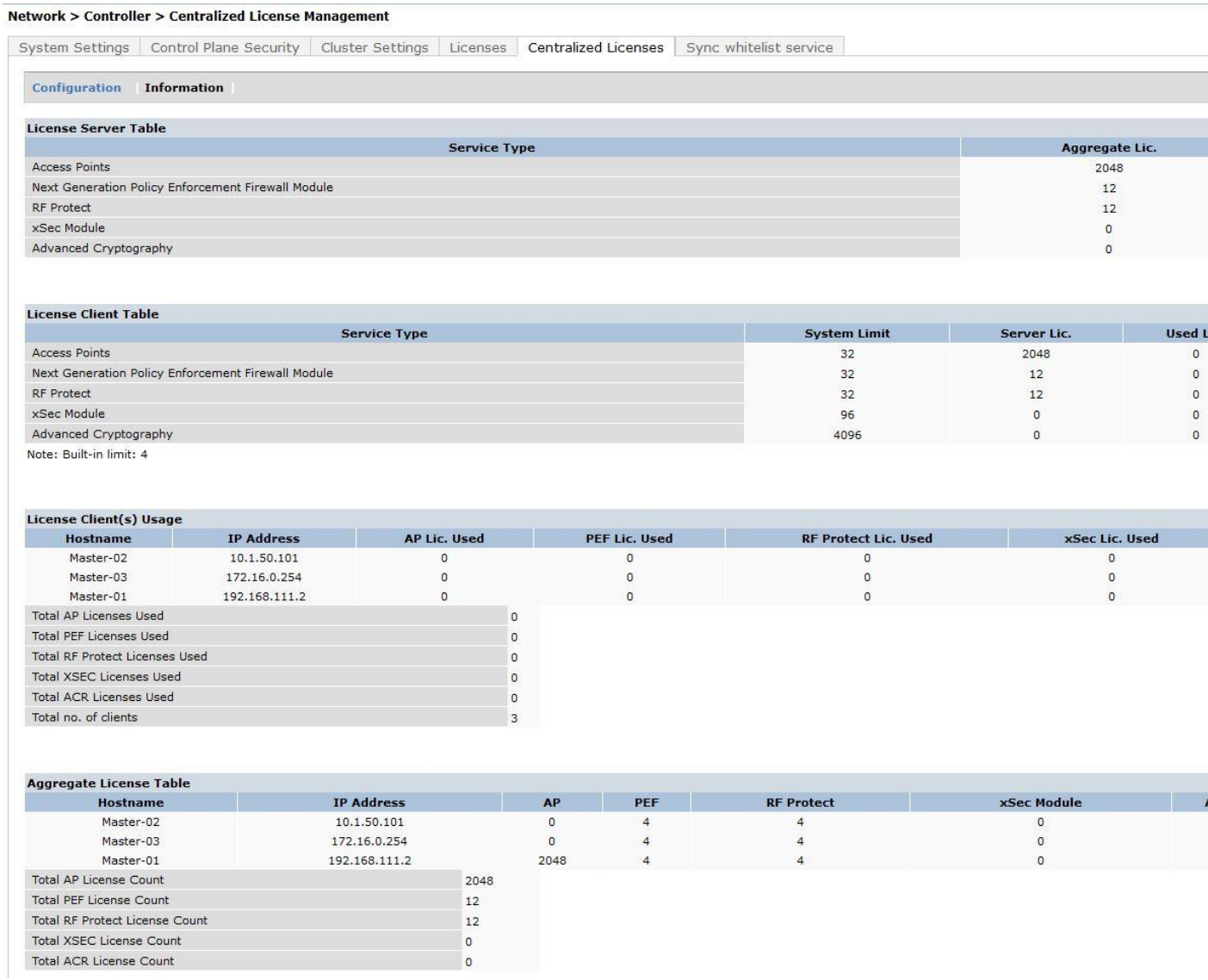
Master-01 configuration:

Master-02 configuration:



Master-03 configuration:

Verify that everything is working by looking in the information section of the tab Centralized licenisng. Here's a screenshot of my Master-01 information section:



Network > Controller > Centralized License Management

System Settings | Control Plane Security | Cluster Settings | Licenses | Centralized Licenses | Sync whitelist service

Configuration | Information

License Server Table

Service Type	Aggregate Lic.
Access Points	2048
Next Generation Policy Enforcement Firewall Module	12
RF Protect	12
xSec Module	0
Advanced Cryptography	0

License Client Table

Service Type	System Limit	Server Lic.	Used L
Access Points	32	2048	0
Next Generation Policy Enforcement Firewall Module	32	12	0
RF Protect	32	12	0
xSec Module	96	0	0
Advanced Cryptography	4096	0	0

Note: Built-in limit: 4

License Client(s) Usage

Hostname	IP Address	AP Lic. Used	PEF Lic. Used	RF Protect Lic. Used	xSec Lic. Used
Master-02	10.1.50.101	0	0	0	0
Master-03	172.16.0.254	0	0	0	0
Master-01	192.168.111.2	0	0	0	0

Total AP Licenses Used	0
Total PEF Licenses Used	0
Total RF Protect Licenses Used	0
Total XSEC Licenses Used	0
Total ACR Licenses Used	0
Total no. of clients	3

Aggregate License Table

Hostname	IP Address	AP	PEF	RF Protect	xSec Module	A
Master-02	10.1.50.101	0	4	4	0	
Master-03	172.16.0.254	0	4	4	0	
Master-01	192.168.111.2	2048	4	4	0	

Total AP License Count	2048
Total PEF License Count	12
Total RF Protect License Count	12
Total XSEC License Count	0
Total ACR License Count	0

You should see all your license clients listed and your total number of licenses contributed by all the clients in your aggregate license table.

Q&A:

Where should I put my licenses in a centralized licenses setup?
Aruba recommends to put all your licenses on the primary licensing server because of the ease of managing your licenses from one point.

What happens if my licensing master(s) becomes unreachable?
If your licensing master becomes unreachable your licensing clients will still keep their

licenses and be able to use them for 30 days. If the licensing server remains down for 30 days straight it will revert back to using its locally installed licenses. If APs are up, they will remain up until they reboot. If they reboot and there's no licenses locally installed, the AP will become unlicensed.

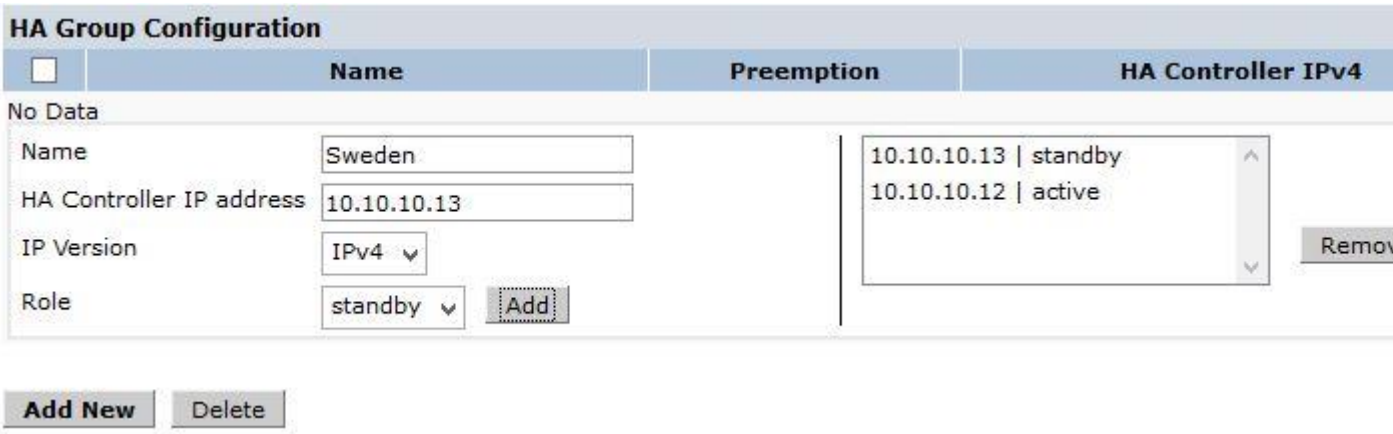
It says in the user guide I need all my masters to be in the same Airwave for this to work, is that true?
I have no idea, it works without it when I test it. If someone knows, please tell us.

Fast Failover

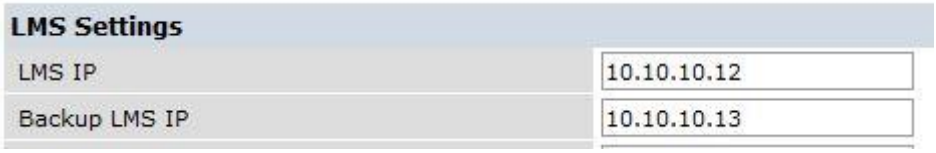
Fast failover is a new high availability feature that you can use for your campus APs in tunnel or decrypt-tunnel mode. It will create a primary tunnel to your preferred controller and a secondary tunnel to the backup controller simultaneously which makes failover times way faster!

This ia achieved by creating something called "HA Groups". On your master controller, navigate to: Configuration -> Redundancy. In this example I've converted my Master-02 and Master-03 to local controllers called Local-01 and Local-02.

On the master, name the HA group and add the controllers participating in it with IP and role. Active for primary and standby for backup. Dual is used for controllers that are both going to be terminating APs and be used as backup for other APs simultaneously. After clicking OK you'll have the option to check "preemption", check it if you want APs to revert back to the preferred controller when it comes back up after a failover. Click apply and save configuration.



On the master also create or modify the AP system profile for the AP-group(s) that will be using fast failover. Put the IP address of the preferred controller in the "LMS IP" field and the IP address of the backup controller in the "Backup LMS IP" field. Like this:



On Local-01 and Local-02 navigate to Configuration -> redundancy and choose to be a member of the configured HA group. If it's not visible, make sure you've saved the configuration in your master controller.

To verify that your AP's are building their redundant tunnels correctly, I log on to the CLI of the master controller. (I can't seem to find this in the GUI anywhere, sorry for that), enter enable mode and issue the command: (Master-01) #show ap database

```
(Master-01) #show ap database

AP Database
-----------
Name   Group   AP Type  IP Address  Status     Flags  Switch IP    Standby IP
----   -----   -------  ----------  ------     -----  ---------    ----------
AP-01  Sweden  105      10.10.10.1  Up 9m:36s  2      10.10.10.12  10.10.10.13
```

You can see the "Switch IP" is the primary controller and the "Standby IP" should be your backup controller.

Q&A:

Won't this work for my RAPs, bridge mode CAPs or Mesh points?
It's not supported, no. I havn't tried it in reality though.

I'm terminating my APs on a VRRP address, is this way better?
I would say this way's better since much of the work is already done when the failover occurs instead of putting all the load on the backup controller first when the primary dies. This way will have faster failovers.

Will this result in a totally seamless failover for my users?
No, this doesn't syncronize user state so your users will need to reauthenticate. There's a feature in ArubaOS 6.4 that will allow totally seamless roaming though!

Client match

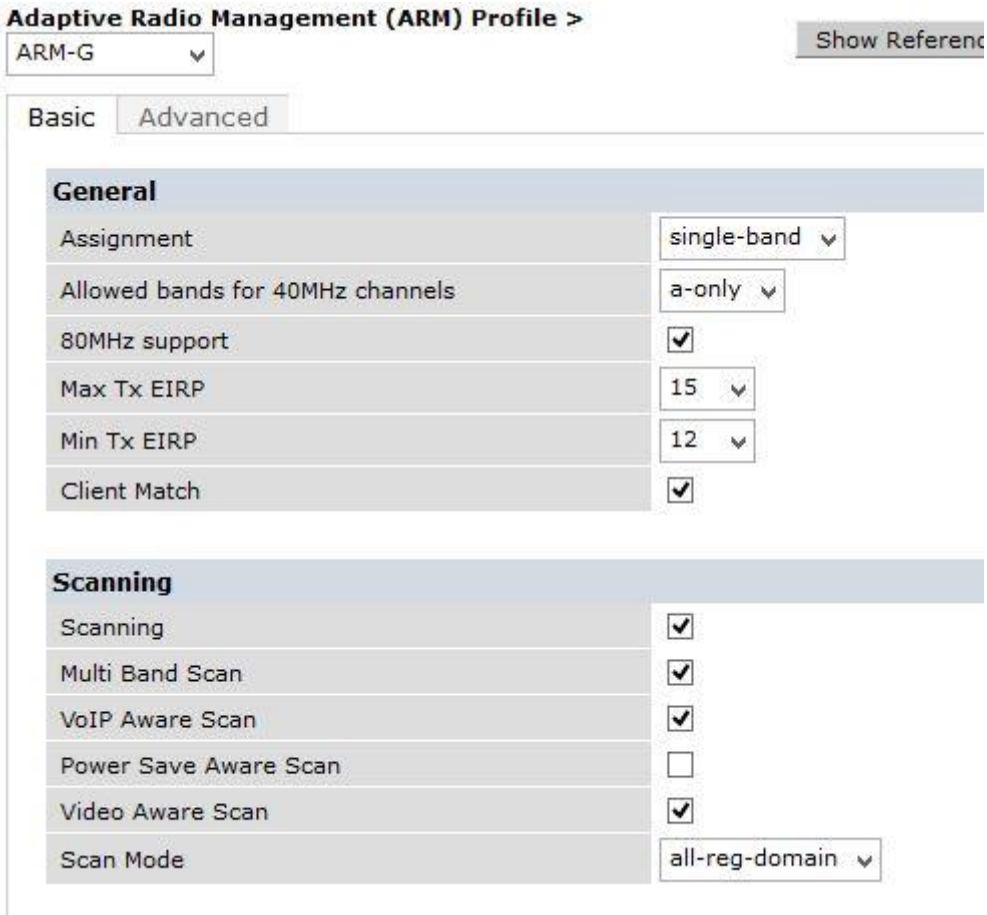
Client match is new since 6.3 and is a feature in ARM that will help your clients make wiser decisions in choosing what AP they'll connect to. It replaces the old band steering and spectrum load balancing features, you could say that client match is a combined and improved version of the two. In my experience this and centralized licensing is the most popular reason to upgrade to 6.3.

I won't dig into detail about this feature but it's on by default after you upgrade and will make your radio life a bit easier. I could write a whole article about how to tweak your radio/ARM settings to fit your needs but that'll be another topic. (let me know if you'd like that though and I'll see what I can do)

What I'll do is to show you where you verify that it's configured and how you verify that it's working for you.

On your master controller, navigate to your ARM profile: Configuration -> AP configuration -> <YOUR AP GROUP> -> RF Management -> 802.11a/g radio

If you click your ARM profile, make sure the checkbox for "Client match" is enabled, like in this screenshot:



Also make sure that it's enabled both for the 2,4ghz radio and the 5ghz radio (the G and the A band). To verify that it's working I'll once again advise you to use the CLI and log on to your controller terminating the access points, enter enable mode and issue the command: show ap arm client-match history

This should show events from your client match feature.

Q&A:

When will client match steer my clients?
When the client tends to stick to the first AP it connected to even though the client has better connection elsewhere.
When the client has the capability of connecting at 5ghz but tries 2,4ghz anyway.
When there's high load on the nearest AP and the neighboring AP has less. etc.

Is there an easier way to see the client match events?
Yes, if you have Airwave you can see the events from there in the GUI.

AMON

I just searched to see what other people have been writing about AMON and I found a perfect guide for it. So I decided that instead of inventing the wheel once again I'll give the credits to cjoseph and link his guide into this thread. (please do not credit me for this guide considering I'm entering the competition and it would not be fair)

Here is his thread:

http://community.arubanetworks.com/t5/Community-Tribal-Knowledge-Base/Why-you-should-always-enable-AMON-on-your-Aruba-Controller-when/ta-p/72104

Q&A:

What Airwave version do I need to supports 6.3 and AMON?
You'll need 7.7x+.

Is there any drawback to using AMON?
Not that I can think of. More and better information more frequently :)