

# Implementation at Murdoch University

## Implementation at Murdoch University

*Notes from presentation 15/11/2007*

### Background

Prior to the university having any involvement with Eduroam, our wireless environment consisted of:

- Approximately fifty Cisco Aironet 1200 access points located over three campuses. No wireless controller / mesh etc.
- Open access network with IPSec VPN connection required to access resources.
- Authentication back end for dialup and VPN was Freeradius:
  - Active Directory user database
  - Freeradius perl modules used for authorisation and some authentication whereby the module interacts with a mysql database. This mechanism provided us with a lot of flexibility.

### Consideration

After Questnet 2005, we were asked to implement Eduroam in our environment:

- We found ourselves well placed to do this due to our pre-existing Freeradius & Cisco infrastructure and the success others had reported with the same setup.
- Implementation was not seen high priority, so the implementation would not be prioritised over other projects.
- We found the documentation available on the Eduroam web site very useful - as a lot of it reflected our environment (Cisco Aironet APs & Freeradius).
- At the end of 2005, we did some preliminary testing with multiple radius servers configured to proxy requests to one another and consulted with Chris Myers from Grangenet to get an idea of what was necessary to proceed.

### Implementation

A project plan with a list of actions required to get Eduroam up and running.

Below is a brief discussion of some of these items.

#### **Investigate the requirements and impact of running WPA/802.1x on our wireless environment**

As we weren't running any WPA / 802.1x, we wanted to verify that:

- Our wireless hardware was able to beacon both our existing MuWLAN SSID and the eduroam SSID concurrently
- There would be no issues trunking multiple vlans to our access points

We found that there were no real issues in running both 802.1x and open networks concurrently on our access points.

The IOS on our AP's needed to be upgraded to beacon multiple SSID's as was required by the eduroam policy. But other than that there were no issues.

The documentation both from Cisco and the Eduroam web site was also very useful.

We were lucky that we weren't utilising dynamic vlan assignment on our existing wireless service, as beaconing multiple SSIDs can break this in a Cisco environment if a wireless controller isn't being utilised.

#### **Investigation of protocols & standards - EAP-PEAP vs EAP-TTLS etc.**

I wasted a bit of time trying to decide which way we should go with this.

Advice from some people locally was that we should use EAP-PEAP as it was more Microsoft friendly and we'd have less hassles with supplicants.

But we decided on EAP-TTLS method as it seemed to be the defacto standard amongst sites in Australia that had already rolled out Eduroam.

#### **802.1x Supplicant Testing**

We tested the SecureW2 client and the native OSX supplicant for Macs without any problems.

I also did some testing on PDA's with varied results - we had success with Dell Axims but couldn't get this working on the O2 (which was prevalently used at Murdoch). We ended up giving up on that one.

#### **IP Allocation & Traffic Policy**

We allocated a new /27 subnet in our public IP range that allowed users to get to many on-net sites, but required them to VPN back to their home institutions to access off-net material.

This was done as we were concerned over the potential abuse by students from other institutions - and considered that this policy could be reviewed in the future.

We also had to prevent this IP range from accessing our proxy servers (we don't run any authentication on these) and consider the licensing implications.

Many resources are licensed for Murdoch staff only, but excluding this range from accessing these resources was relatively simple as we already maintained a database of what IP's were staff, what IP's were students and what IP's were other.

## **Configure pre-production radius server for adherence with policy external proxying with national server**

We tweaked Freeradius via the perl authorisation module so that we could maintain a banned list of mac-addresses and identities. This provided us with the ability to easily kick misbehaving users off our network.

Our testing of the national service was pretty simple and only done with the national server. We weren't entirely confident that everything would work seamlessly with other universities at the time.

In retrospect, we were lucky that our configuration worked and I should have requested assistance with testing from the tech-list.

## **Online Documentation**

This was just a matter of spending a couple of hours writing some web pages and getting our Web services team to publish this at <http://www.its.murdoch.edu.au/eduroam/>

## **Advertise to IT contacts and Pilot**

We piloted this on several Access Points in our Science & Computing Building first and advised the service to our IT staff around the Uni.

We were lucky that some staff travelled to other Eduroam connected institutions during this time and successfully connected.

## **Deployment to all Access Points**

Deployment to all access-points was a matter of modifying our standard AP configuration and co-ordinating the service launch with affected users (service desk etc.)

## **Experience Since**

Our experience with the Eduroam has been positive, but unfortunately the uptake by staff has been limited. Staff that make use of it have reported varying degrees of success at other institutions. Problems reported back by roaming staff are generally

- Some have eduroam deployed on some access points and not others
- Traffic filters haven't always been compatible with our VPN service (TCP 10000)

## **Future Plans**

### **Traffic Policy**

After hearing of other institutions success with on-net/off-net traffic shaping, we have begun investigating a similar setup at Murdoch. Our initial attempts at this involved generating a static ACL based on the published AARNET on-net routes. Unfortunately, the ACL was too large and so a method of doing this based on BGP community tags will be looked at instead.

### **Eduroam SSID available to Murdoch staff & students locally**

It makes a lot of sense to have a single SSID carrying all traffic and to have users assigned to a vlan by our radius server. For this to happen, it will be implemented as part of a larger wireless expansion in the near future.