

# Options for Traffic Peering

## Why Peer?

The close proximity of some participating eduroam organisations to a neighbouring institution and the restriction/requirement that eduroam transit traffic cannot be back charged to another eduroam participant may create the need for transit traffic minimisation.

Other eduroam Australia participants have implemented VPN only access to eduroam to implement transit traffic minimisation - but the use of a security tool to implement a routing protocol causes various problems for eduroam users:

1. Split Tunnel VPN Connections will require a user to reconfigure their VPN to route traffic to their home organisation.
2. Home organisation proxy configuration may auto-select direct connection for VPN ip ranges, thus requiring proxy reconfiguration.
3. The same level of confusion is placed upon visiting academics, staff and students when they access resources and are least able to access their home helpdesk service.
4. eduroam is a world wide effort and connection to it should be as uniform as possible.

If the use of the network by eduroam participants outside of your city/state is projected to be significantly smaller than the use by staff and students of our neighbouring institutions then this document proposes some solutions in peering between institutional networks to make institutions responsible for their own staff/students traffic and network activity.

## Peering Options

There are six options raised in this document:

### 1. VPN Only Traffic to Home Organisation

This is the most commonly deployed option amongst Australian eduroam Participants. It is already available at all eduroam sites in Australia and many have the infrastructure to support it.

#### **Impact: Usability**

Allowing VPN only traffic requires the user to reconfigure their VPN/Proxy connections to allow access to the eduroam network. Use of a network that supports this service is frustrating to the user and it is expected that either the helpdesk will bear the bulk of complaints if this service is adopted - or users will simply not use the service.

### 2. Access to on-net only sites

This option is more liberal in network access than the previous option. But also suffers from usability problems.

#### **Impact: Usability**

The user will be able to reach their "home page" if it is set to their institution - but off-net sights will simply timeout. This will increase the support burden for helpdesk as sights will just not work - as users should revert to using their home organisation VPN for wider network access.

If this option was to be considered in any seriousness a captive portal would be required to provide users with an information page on why they don't have access to a particular site - rather than just have their connection blocked.

### 3. Rate limited VLAN

In addition to the "eduroam" VLAN which is used for all eduroam participants. Either a single VLAN for local eduroam participants or an individual VLAN for each institution would be required.

VLAN Name	Purpose	Ports	IP Addr	Restrictions
eduroam	eduroam users and academic conference use	All	IPv4	
eduroam-slow	Users that have consumed excess network transit but don't warrant being barred access	All - possibly greater port restrictions here?	IPv4	Shared XXXkb/s off-net connection
eduroam-peer	eduroam users from a neighbouring organisation	All	IPv4	Shared XXXkb/s to off-net sites

This option doesn't involve peering but rather shaping of connections from neighbouring institutions. Therefore, it doesn't require technical input from other institutions nor their co-operation. It is relatively easy to implement (in a technical sense) and can be adjusted at any time without liaising with the peering partner.

#### **Impact: Financial**

This option can expose an organisation to a financial burden as eduroam traffic can't be cost recovered to eduroam participants. Based on a 128kb/s shared connection the figures below represent the MAXIMUM transit traffic possible on the connection.

A 128kb/s connection would allow \$6.59 worth of transit to be consumed if the connection was running at full speed for that 24 hour period and if all connectivity was off-net. An authorisation system could be added to the wireless infrastructure to provide access to differing rate limited VLANs in case of abuse by a particular user or realm of users.

kpbs	\$/8hours	\$/24hours	\$/YEAR	24/7/365 Use
32	\$0.55	\$1.65	\$109.86	\$601.50
64	\$1.10	\$3.30	\$219.73	\$1,203.00
128	\$2.20	\$6.59	\$439.45	\$2,406.01
512	\$8.79	\$26.37	\$1,757.81	\$9,624.02
1024	\$17.58	\$52.73	\$3,515.63	\$19,248.05
1536	\$26.37	\$79.10	\$5,273.44	\$28,872.07
2048	\$35.16	\$105.47	\$7,031.25	\$38,496.09
5120	\$87.89	\$263.67	\$17,578.13	\$96,240.23
10240	\$175.78	\$527.34	\$35,156.25	\$192,480.47

*NB: Cost projections are based on AUD\$5/GiB for transit.*

It is expected that the connection would be shared - and therefore would be used by all members of a particular organisation.

While "eduroam" traffic would have a larger bandwidth allocation it is expected that this network would receive less users.

A commitment to a particular dollar figure should be decided and the rate limiting could be adjusted throughout the year to ensure that this figure isn't exceeded if use of the network was higher than expected in any one reporting period.

## 4. VPN/GRE Tunnel

This is the most technically complicated option and would require co-operation between both peering partners. The aim would be to create a tunnel between an allocated VLAN and a network point in the home organisation. All traffic would flow down the tunnel and the home organisation could handle the traffic in any way they feel appropriate. If there is a significant increase in cross city/state institutional eduroam use (particularly in regard to student residences) then this may be the only viable option.

### ***Impact: Technical & Political***

This peering option requires technical input from our neighbouring institutions. The skill level required may not be available - and the structure of their network may not make it technically feasible to make the peering arrangement reciprocal. There would also be administrative barriers to this peering which would need to be overcome.

## 5. IP Block to access Auth Proxy

By providing a static block of addresses for users from neighbouring institutions - their home organisation could allow access to their authenticated proxy. This would required the limited involvement from the visited organisation and give the home organisation full control over the speed at which users could access off-net traffic.

The need for the visited organisation to allow on-net traffic would be negligible - but this option would be best implemented with support from Option #3.

### ***Impact: Security***

By allowing IP ranges from partner institutions to authenticate against University resources could cause a security issue if adequate monitoring of the service wasn't maintained.

## 6. Block entire Realm

This option would deny network access to all staff/students from our neighbour institutions. This can be implemented in technically simple manner and is inline with the aarnet eduroam Policy.

### ***Impact: Anti-Collaborative***

This option would only be considered if no other option was feasible. The impact on the visited organisation implementing this is that it would be highly likely for neighbouring institutions to also block that organisations staff and students. This is not a situation we would enjoy and would harm the collaborative efforts that exist between our organisations.

# Recommendation

Of the options currently explored Option #3 is the: simplest for an organisation to implement; doesn't require co-operation with our intended peers; and the financial impact of such a decision can be varied throughout the year with regular review of bandwidth used, if necessary.

It is hoped that if this option is explored that it could operate in conjunction with Option #5 to provide higher speed access to eduroam users from neighbouring institutions if they choose to allow authenticated proxy requests.