



# Using FreeRADIUS with Eduroam

Glen Turner

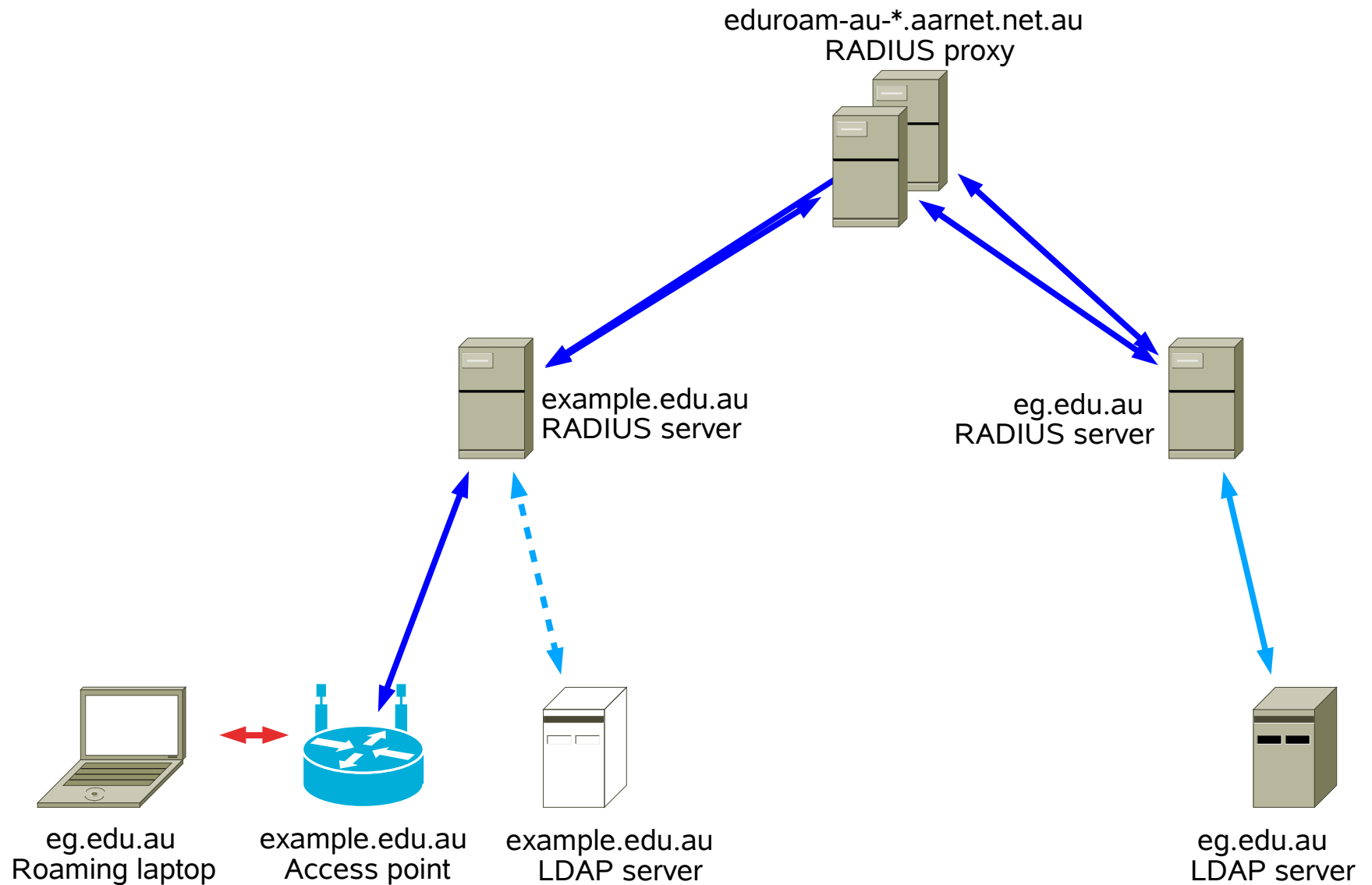
2008-05-29

Eduroam workshop

University of Sydney, Australia

# Eduroam fundamentals

# Chain of authentication



# Visitor

- User uses 802.1X to communicate with access point
  - Gives a user name of fab@eg.edu.au
- This is converted from 802.1X to RADIUS and sent to example.edu.au's RADIUS server
- The RADIUS for server does not have an authentication clause for @eg.edu.au, the default is to proxy to eduroam-au-\*
- eduroam-au-\* proxies to eg.edu.au
- eg.edu.au's RADIUS server gateways to LDAP
- which checks the password

# Local user

- Two choices
  - Prevent local users from using eduroam
    - example.edu.au's RADIUS server can deny access for \*@example.edu.au
  - Map Eduroam users to a different VLAN, within the firewall, applying example.edu.au local user policies
    - example.edu.au's RADIUS server allows access for \*@example.edu.au and sets VLAN
- Second is the more interesting choice
  - Only need “eduroam” SSID
  - Client machines are already set up and tested for roaming

# 802.1X modes

- EAP/PEAP/TTLS/etc

# Beginning

# Installation

- [www.freeradius.org](http://www.freeradius.org)
- Use the package manager
  - Red Hat, Fedora, CentOS
    - # yum install freeradius**
    - Doesn't start by default
      - # chkconfig radiusd on**
      - # /etc/init.d/radiusd start**
  - Debian, Ubuntu
    - # apt-get install freeradius freeradius-ldap**
    - Starts immediately, to stop
      - # update-rc.d -f freeradius remove**
      - # /etc/init.d/freeradius stop**



# Configuration files

- Usual Unix-style configuration file
  - Red Hat  
/etc/raddb
  - Debian  
/etc/freeradius
- Each file collects together related configuration
  - radiusd.conf — Server configuration
  - clients.conf — RADIUS clients
  - proxy.conf — Upstream RADIUS servers
  - snmp.conf — Connection with Net-SNMPand so on

# Log files

- Red Hat  
/var/log/radius/radius.log
- Debian  
/var/log/freeradius/radius.log
- Contains:
  - configuration errors
  - running errors
  - authentication success or failure
- Typical debugging phrase is  

```
# tail -f /var/log/*radius/radius.log &
```

# SELinux

- Type enforcement of programs and their data
  - a simple way to stop zero-day attacks
- Look for audit messages in `/var/log/messages`
- Ask for an explanation
  - `sealert -i ...`
- Look at SELinux configuration options
  - `getsebool -a`
- Modify policy
  - `audit2allow -M local < /var/log/audit/audit.log > local.te`  
`semodule -i local.pp`

# Exercise 1

- Boot CentOS Linux virtual machine
- Record its IP address from DHCP server log
- Install FreeRADIUS
- Start FreeRADIUS
- Examine the log file



# Connect access point

# Configure access point — SSID

- Service-set Identifier is “eduroam”
  - ESSID used to retrieve stored configurations
  - If there are multiple networks operating which provide eduroam then use a riff on the name
    - *eduroam-aarnet*
    - *eduroam-UofA*, *eduroam-adelaide* may have been better
- 32 bytes

The screenshot shows the Linksys configuration interface for a WRT54GSV4 router. The page is titled "Wireless-G Broadband Router with SpeedBooster" and "WRT54GSV4". The "Wireless" tab is selected, and the "Wireless Network" section is active. The "Wireless Network Mode" is set to "Mixed", the "Wireless Network Name (SSID)" is "eduroam", and the "Wireless Channel" is "1 - 2.412GHZ". The "Wireless SSID Broadcast" is set to "Enable". There is a "Reset Security" button and a status indicator for "SES Inactive". A sidebar on the right provides additional information about the "Wireless Network Mode" and "SpeedBooster" settings.

LINKSYS®  
A Division of Cisco Systems, Inc. Firmware Version: v1.06.3

Wireless-G Broadband Router with SpeedBooster WRT54GSV4

Wireless

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Wireless Settings Wireless Security Wireless MAC Filter Advanced Wireless Settings

Wireless Network

Wireless Network Mode: Mixed  
Wireless Network Name (SSID): eduroam  
Wireless Channel: 1 - 2.412GHZ  
Wireless SSID Broadcast:  Enable  Disable

Status: SES Inactive  
Reset Security

Wireless Network Mode : SpeedBooster is enabled automatically on Mixed Mode and G-Only mode. If you wish to exclude Wireless-G clients, choose B-Only Mode. If you would like to disable wireless access, choose Disable. More...

Save Settings Cancel Changes

CISCO

# Configure access point — 802.1X

- Transports Extensible Authentication Protocol from supplicant to access point
- Encrypts session
  - Most supported: WPA Enterprise with TKIP
  - Most secure: WPA2 Enterprise with AES

The screenshot shows the Linksys configuration interface for a WRT54GSV4 router. The page is titled "Wireless Security" and is part of the "Wireless" section. The "Security Mode" is set to "WPA2 Enterprise" and the "WPA Algorithms" are set to "TKIP + AES". The "RADIUS Server Address" is set to "1 . 2 . 3 . 4", the "RADIUS Port" is "1812", the "Shared Key" is "testing", and the "Key Renewal Timeout" is "3600 seconds". A "Security Mode" help box on the right explains that all devices must use the same security mode to communicate. The page includes "Save Settings" and "Cancel Changes" buttons at the bottom.

**LINKSYS**  
A Division of Cisco Systems, Inc.

Firmware Version: v1.06.3

Wireless-G Broadband Router with SpeedBooster WRT54GSV4

**Wireless**

Setup Wireless Security Access Restrictions Applications & Gaming Administration Status

Basic Wireless Settings Wireless Security Wireless MAC Filter Advanced Wireless Settings

**Wireless Security**

Security Mode: WPA2 Enterprise

WPA Algorithms: TKIP + AES

RADIUS Server Address: 1 . 2 . 3 . 4

RADIUS Port: 1812

Shared Key: testing

Key Renewal Timeout: 3600 seconds

**Security Mode:** You may choose from Disable, WEP, WPA Pre-Shared Key, WPA RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate. [More...](#)

Save Settings Cancel Changes

**CISCO**

# Configure access point — RADIUS

- The most common way to transport EAP from the access point across the IP network to the authenticator is RADIUS
- Configure RADIUS
  - Server IP address and ports
    - Well known port: 1812, 1813; used to be 1645, 1646
  - Secret (“shared key”)

The screenshot shows the Linksys configuration interface for a WRT54GSV4 router. The page is titled "Wireless Security" and is part of the "Wireless" section. The configuration fields are as follows:

Security Mode:	WPA2 Enterprise
WPA Algorithms:	TKIP + AES
RADIUS Server Address:	1 . 2 . 3 . 4
RADIUS Port:	1812
Shared Key:	testing
Key Renewal Timeout:	3600 seconds

At the bottom of the page, there are two buttons: "Save Settings" and "Cancel Changes". A sidebar on the right contains a "Security Mode" warning: "Security Mode: You may choose from Disable, WEP, WPA Pre-Shared Key, WPA, RADIUS, or RADIUS. All devices on your network must use the same security mode in order to communicate. More..."



# Configure RADIUS server

- clients.conf contains access points
- Configuration phrase is

```
client 5.6.7.8 {  
    shortname = cbr-c-12  
    secret = testing  
}
```
- The shortname appears in the log file, it has no other significance
  - Some riff on the AP's name seems right

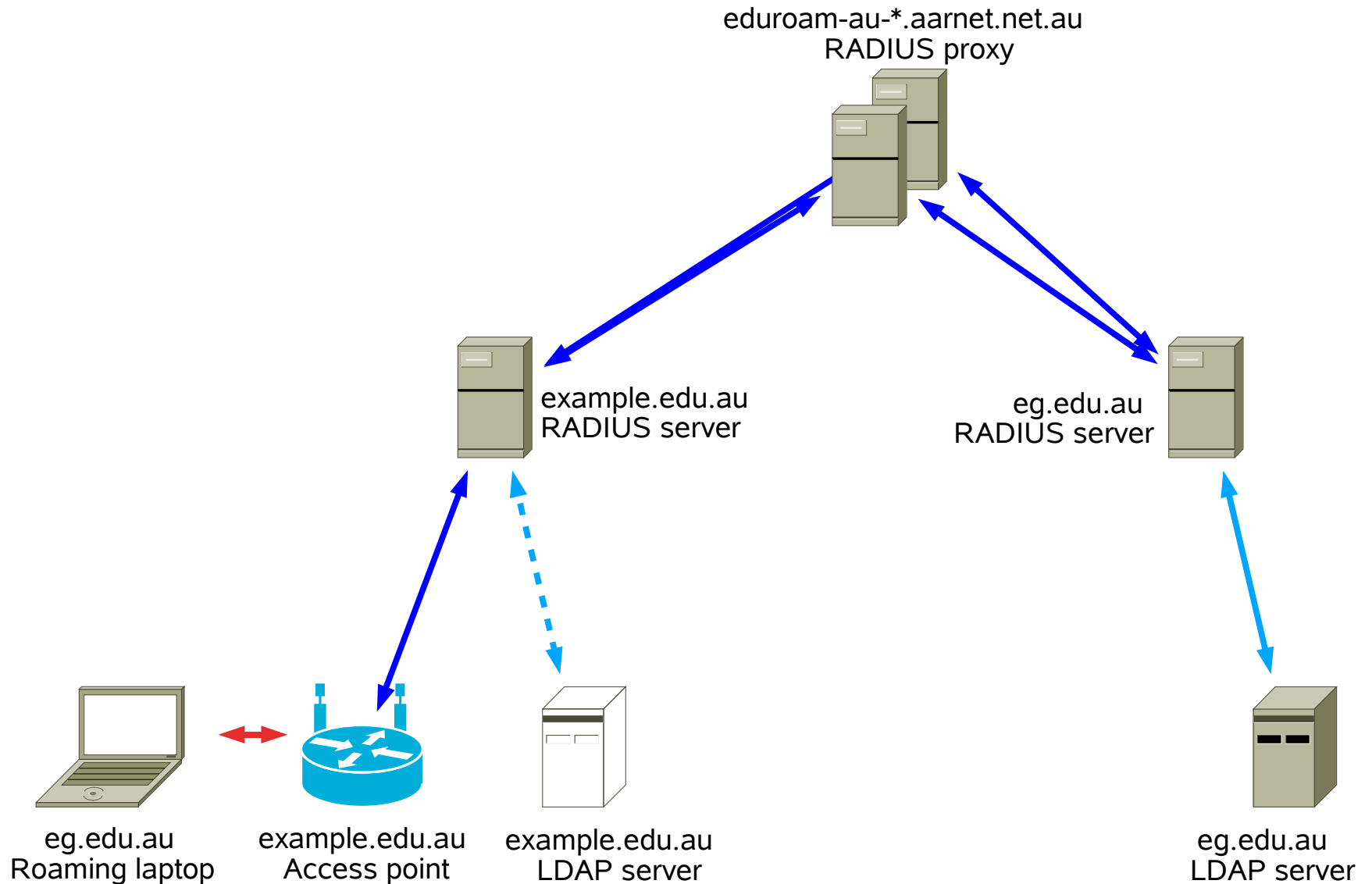
## Exercise 2

- Configure your access point to use
  - DHCP to obtain an IP address
  - Channel 1
  - A unique SSID
  - NAT routing
- Record its IP address from DHCP server log
- Configure 802.1X and RADIUS on access point
- Configure RADIUS server to connect to access point
- Test



# Federate RADIUS server: visitors

# Sending requests to federation



# Sending requests to federation

- Requests which are not handled locally are proxied to the Eduroam federation

- **proxy.conf**

- ```
realm DEFAULT {  
    type = radius  
    authhost = eduroam-au-1.anycast.aarnet.net.au:1812  
    accthost = eduroam-au-1.anycast.aarnet.net.au:1813  
    secret = testing  
    nostrip  
}  
realm DEFAULT {  
    type = radius  
    authhost = eduroam-au-2.anycast.aarnet.net.au:1812  
    accthost = eduroam-au-2.anycast.aarnet.net.au:1813  
    secret = testing  
    nostrip  
}
```

## Exercise 3

- Federate your server with the Australian eduroam server
- Use a test account to check to if your RADIUS server and access point with authenticate a foreign user

# Local users

# Defining a local user

- **users**

```
fred    User-Password == "testing"
```

- **radiusd.conf**

```
authorize {  
    preprocess  
    mschap  
    suffix  
    eap  
    files  
}  
authenticate {  
    Auth-Type MS-CHAP {  
        mschap  
    }  
    eap  
}
```



# MSCHAP

- radiusd.conf

```
mschap {  
    authtype = MS-CHAP  
    use_mppe = yes  
    require_encryption = yes  
    require_strong = yes  
}
```

# EAP

- eap.conf
- eap {  
    default\_eap\_type = ...  
    timer\_expire = 60  
    ignore\_unknown\_eap\_types = no  
    cisco\_accounting\_username\_bug = no
- Now configure TLS, PEAP, TTLS

# TLS

- Transport layer security requires certificates

- eap.conf

```
eap{
  tls {
    private_key_password = abcdefg
    private_key_file = ${raddbdir}/certs/cert-srv.pem
    certificate_file = ${raddbdir}/certs/cert-srv.pem
    CA_file = ${raddbdir}/certs/demoCA/cacert.pem
    dh_file = ${raddbdir}/certs/dh
    random_file = ${raddbdir}/certs/random
    fragment_size = 1024
    include_length = yes
    copy_request_to_tunnel = no
    use_tunneled_reply = no
  }
}
```

# PEAP with MSCHAPv2

- eap.conf

```
eap {
  tls {
    ...
  }
  default_eap_type = peap
  peap {
    default_eap_type = mschapv2
  }
  mschapv2 {
  }
}
```

# TTLS

- eap.conf

```
eap {
  default_eap_type = tls
  tls {
    ""
  }
  ttls {
    copy_request_to_tunnel = no
    use_tunneled_reply = no
  }
}
```

# Exercise 4

- Create a local user
- Configure your wireless supplicant to authenticate against that local user using PEAP +MSCHAPv2 and TTLS
  - You may need to download the Secure W2 client if using Windows
    - [www.securew2.com](http://www.securew2.com)



# Federate RADIUS server: travellers

# The federation makes queries

- Just like access points do

- **clients.conf**

```
client eduroam-au-1.aarnet.net.au {  
    shortname = eduroam-au-1  
    secret = testing  
}  
client eduroam-au-2.aarnet.net.au {  
    shortname = eduroam-au-2  
    secret = testing  
}
```



A bundle of fiber optic cables is shown on the left side of the image, with their tips glowing and creating a bokeh effect of colorful light spots (red, orange, yellow, green, blue) against a dark background.

# Integration with organisational directory

# Connect server with authentication

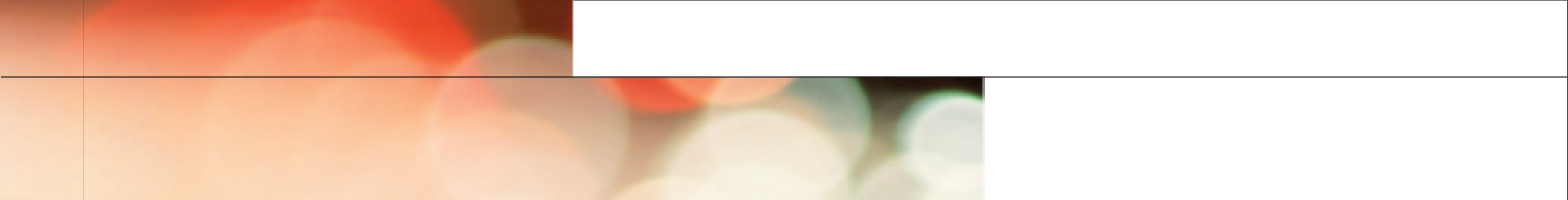
- FreeRADIUS can locally authenticate user IDs and passwords
- FreeRADIUS can proxy the authentication to a database, LDAP, Kerberos and ActiveDirectory
- Authentication servers often provide an LDAP gateway themselves, making LDAP a common ground
  - Oracle Internet Directory
  - Novell eDirectory

# LDAP recipe

- Modern LDAP server schema
  - Very different from what ISO intended
  - Easy interoperation with Internet
- <http://middleware.internet2.edu/dir/docs/ldap-recipe.htm>
- `dn: uid=a12323,ou=people,dc=example,dc=edu,dc=au`  
`uid: a12323`  
`cn: Fred Bloggs`  
`givenName: Fred`  
`sn: Bloggs`  
`eduPersonNickname: Fred`  
`mail: a12323@example.edu.au`  
`mailhost: smtp.srv.example.edu.au`  
`eduPersonAffiliation: staff`  
`eduPersonPrimaryAffiliation: staff`  
`eduPersonPrincipalName: s12323@example.edu.au`

# LDAP and FreeRADIUS

```
• modules {
  ldap {
    server = ldap.srv.example.edu.au
    basedn = "ou=people,dc=example,dc=edu,dc=au"
    filter = "(eduPersonPrincipalName=%{User-Name})"
    dictionary_mapping = ${raddbdir}/ldap.attrmap
    ldap_connections_number = 5
    timeout = 4
    timelimit = 3
    net_timeout = 1
  }
}
authorize {
  ... ldap ...
}
authenticate {
  Auth-Type LDAP {
    ldap
  }
  ...
}
```

- 
- If your LDAP Schema doesn't follow the eduPerson recipe then you can use other attributes, such as email addresses, and add an explicit attribute or LDAP group for use of Eduroam

# OpenLDAP

- `apt-get install slapd`
- `yum install openldap openldap-clients openldap-servers`
- gq is a nice graphical administration tool

# Other directories

- The FreeRADIUS Wiki has configs for Microsoft Active Directory



# Limiting financial exposure



# Strategies

- Blocking
- Rate-limiting
- Blocking with multiple routers
- Rate-limiting with multiple routing tables



# Using FreeRADIUS with Eduroam

[www.gdt.id.au/~gdt/presentations](http://www.gdt.id.au/~gdt/presentations)

Glen Turner

[glen.turner@aarnet.edu.au](mailto:glen.turner@aarnet.edu.au)