RADSEC and IF-MAP trial

Networkshop 39
University of Hertfordshire April 2011

Dr Alan Buxey

[Jon Knight, Scott Armitage, Ramesh Jangama-Baskaran, Colin Morrison]

Loughborough University

Outline of presentation

- Background information on the trial
- RADSEC
  - Background
  - Progress
- IF-MAP
  - Background
  - Progress
- Future

Loughborough University

Background information

- 9 Jun 2010 - Call for Participation

- The trial will investigate the secure use of RADIUS protocol to send authentication requests across insecure networks.
- Furthermore, the project aims to demonstrate how IF-MAP can be extended to provide a measurement & monitoring tool for a potential replacement service.

- 2nd July 2010 deadline for responses

Result of CfP

- Few responses
- Initial ‘Boot-Up’ trial with Loughborough and JANET(UK) as partners
- Looking for other sites to join in when documentation and tools ready

Loughborough University

‘RADSEC’

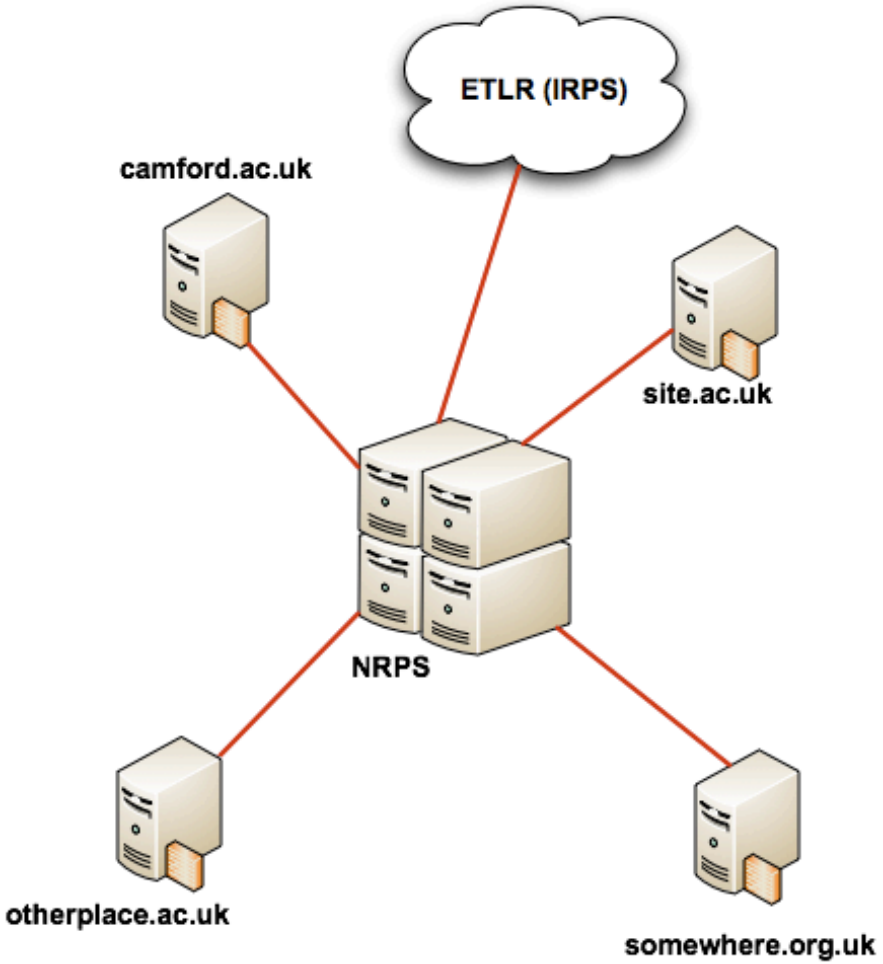
- RadSec is a protocol for transporting RADIUS over TCP and TLS.
- http://tools.ietf.org/html/draft-ietf-radext-radsec-08
- Port for RADIUS over TLS is TCP/2083
- http://tools.ietf.org/html/draft-ietf-radext-tcp-transport-09
- Shared secrets still around:
  - User-Password, Message-Authenticator, Response-Authenticator, MS-MPPE-*
  - ‘mysecret’

Loughborough University

‘RADSEC’ in RADIUS servers

- RADIATOR
  - http://www.open.com.au/radiator/
- RadSecProxy
  - http://software.uninett.no/radsecproxy/
- FreeRADIUS support coming…

Current layout



End sites connect to NRPS (RADIUS)

NRPS connect to IRPS (RADIUS)

UDP

Stats centralized

The rules

- There are two types of server certificates:
- **eduroam SP profile**: for eduroam Service Providers (operators of an eduroam hotspot, or proxy relays for one or more eduroam hotspots)
- **eduroam IdP profile**: for eduroam Identity Providers (operators of an eduroam realm, or proxy relays for one or more eduroam Identity Providers)
- Note: one certificate can carry both profiles at the same time

- Authorisation: make sure that your email address is listed as an eduroam operator. ***eduPKI eduroam RA will only issue certificates with a contact email address that's listed in the eduroam operator database.***
  The profiles you request for your certificate must also match your entry in the database.
  if you are listed as an eduroam IdP only, your certificate will be allowed to carry only the eduroam IdP profile.
- if you are listed as an eduroam SP only, your certificate will be allowed to carry only the eduroam SP profile.
- if you are listed as both, or if you are a proxy or federation operator, the certificate will be allowed to carry both profiles.
- Authentication: we need to perform identity vetting on your certificate request. eduPKI eduroam RA currently supports two ways of identity vetting, you can choose either of the two:
  TCS Personal Certificates: if you are in possession of a TCS Personal Certificate, you can use this in the submission step to send a signed email with the certificate request form.
- **PGP/GPG signature**: if you have a PGP/GPG key, please make sure that the key is signed by your federation operator, and is available on commodity keyservers. You can then use this in the submission step to send a signed email with the certificate request form.

The rules

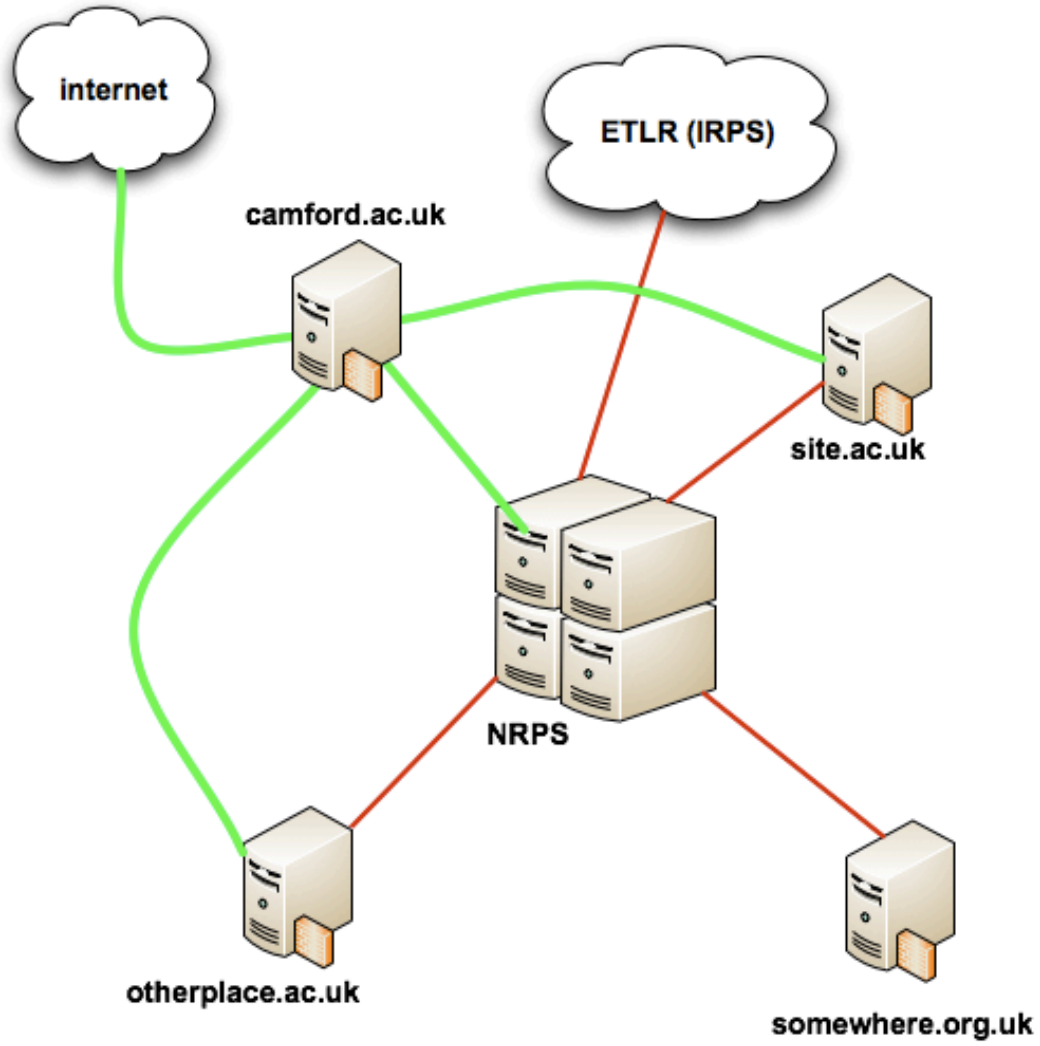
- Certificate request: You use the "eduroam Certificate Request Generator (eduPKI CA)" simply fill out the form. Note that:
- Contact Data: these fields must match the contents of the eduroam Database
- Certificate profile: your selection must be consistent with your entry in the eduroam Database
- Organisation: eduPKI CA only issues certificates to legal entities. If your eduroam installation is only a department of a legal entity, remember to fill in your parent entity's name.
- After submitting the form, you will receive a private key to save locally, and a PDF form. Please send this PDF form via a **signed** email (as per the requirements in step 2) to edupki-ra@eduroam.org. The email signature must be for the email address that is in the certificate request.
- The eduPKI eduroam RA personnel will verify that the request is in order and will issue your certificate as quickly as possible. The verification procedure includes human processing and is not instant, please allow for a few business days.

The config (e.g. RADIATOR)

```
<Handler Realm=/^camford.ac.uk$/I >
<AuthBy RADIUS>
        FailureBackoffTime 10
        RetryTimeout 5
        Retries 1
        UseExtendedIds
        <Host radius.camford.ac.uk>
                Secret t0p-s3cr3t
                AuthPort 1812
                AcctPort 1813
        </Host>
        </AuthBy>
</Handler>
```

```
<Handler Realm=/^camford.ac.uk$/>
      <AuthBy RADSEC>
       NoreplyTimeout 5
       UseTLS
       TLS_CAFile %D/certificates/eduPKI-CA.crt
       TLS_CertificateFile %D/certificates/radsec.camford.ac.uk-eduPKI.pem
       TLS_CertificateType PEM
       TLS_PrivateKeyFile %D/certificates/radsec.camford.ac.uk-key.pem
       TLS_PrivateKeyPassword cert_pass
       TLS_PolicyOID       .1.3.6.1.4.1.25178.3.1.2
                  <Host radsec.camford.ac.uk>
                  Port 2083
                   Protocol radsec
                   Transport tcp
                  UseTLS
                  FailureBackoffTime 10
                  </Host>
    </AuthBy>
</Handler>
```

Proposed future



RADSEC used for direct communication where possible

RADSEC used to talk to NRPS to proxy as RADIUS to sites that don't do RADSEC

Loughborough University

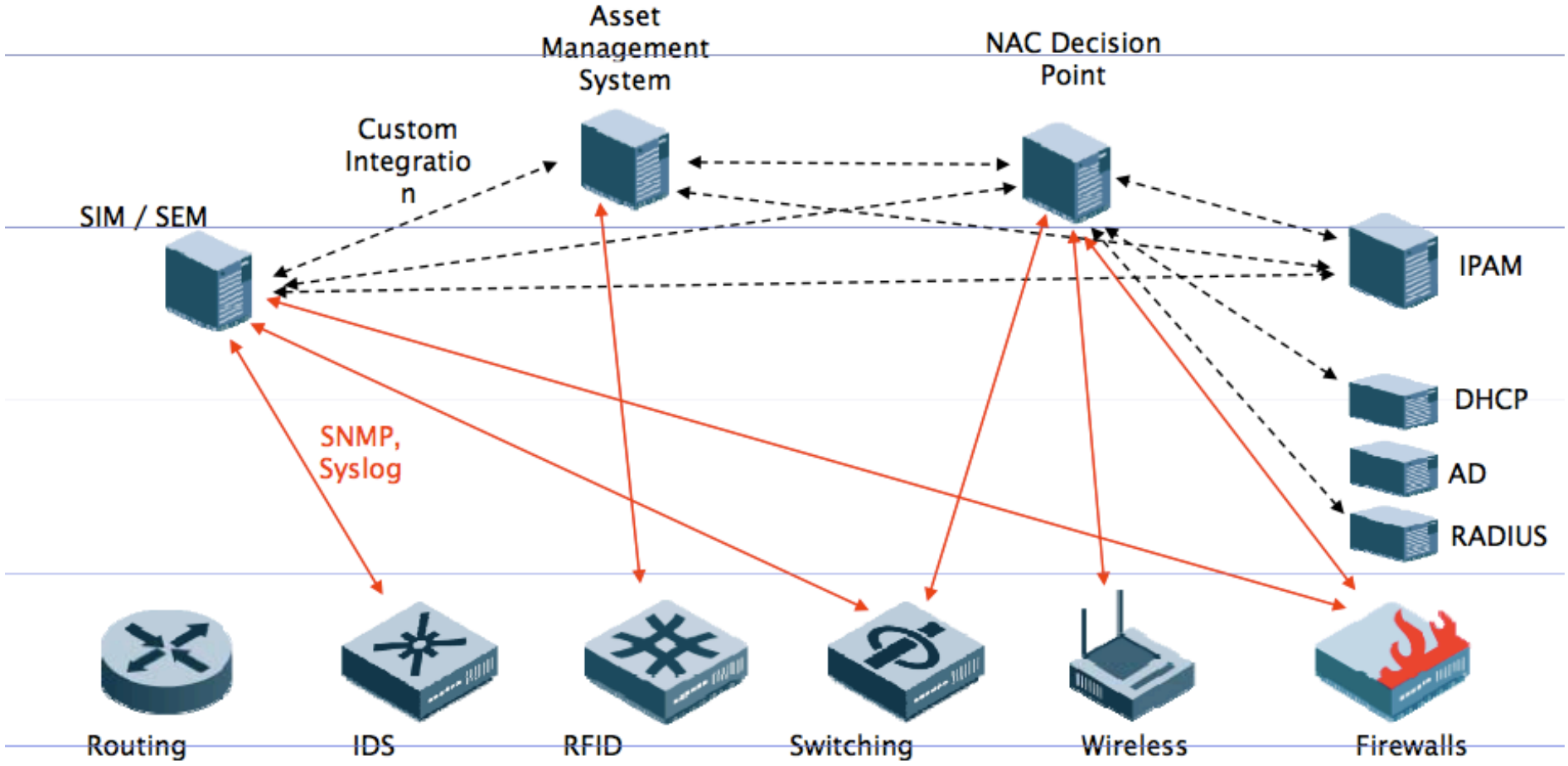
IF-MAP

•difficulty in network security is the collection, correlation, and searchability of bits of information about users of the network
•DHCP, firewall, IDS, RADIUS etc all know bits
•Correlate all of this information together
•IF-MAP describes a database service that contains information (metadata) about systems and users currently connected to a network.
•Can then use all of this information to make a decision policy….at any point or from any point that has subscription to IF-MAP

•E.g. RADIUS can state what is suitable network, or firewall could open a hole.

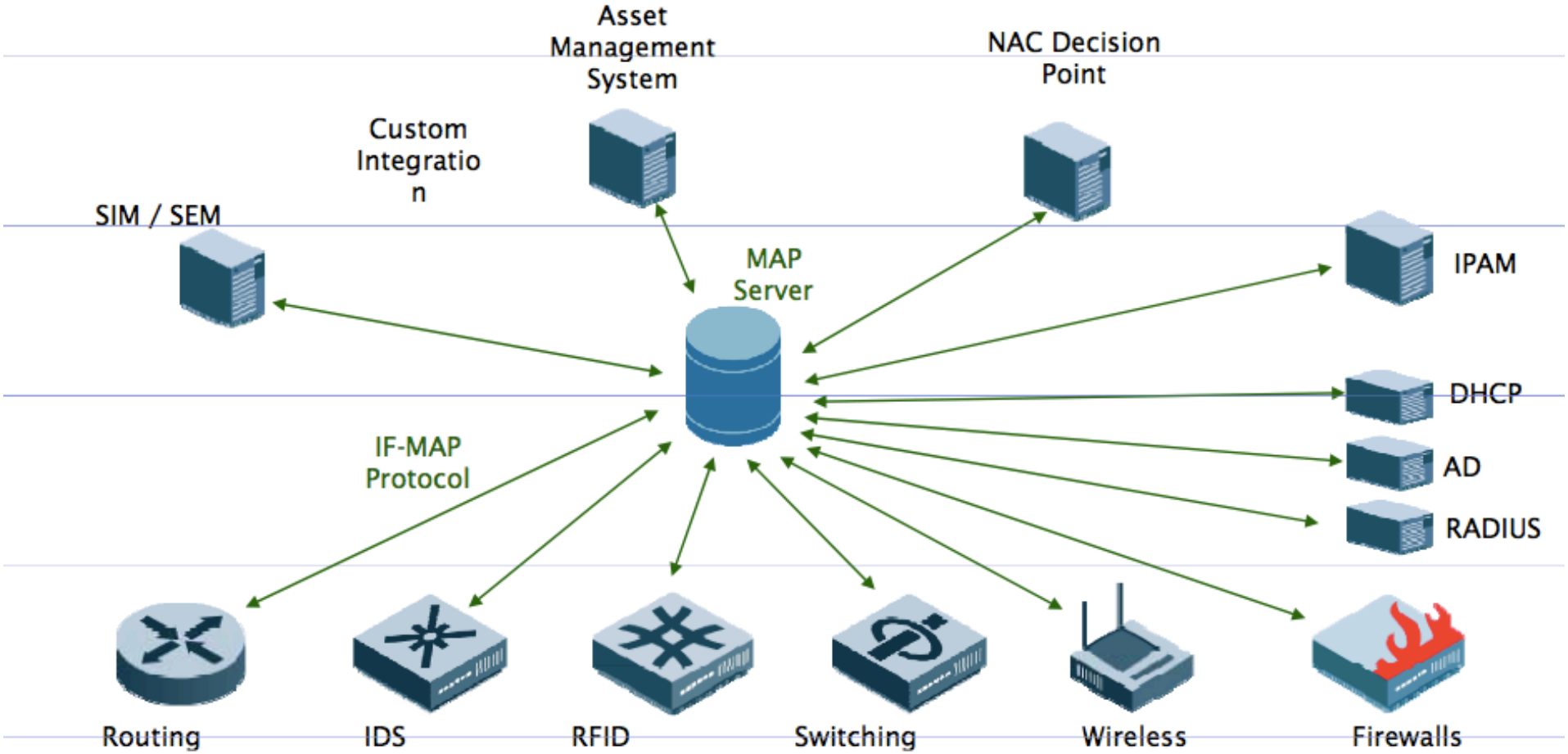
Loughborough University

The current situation



Loughborough University

Proposed IF-MAP integrated solution



Loughborough University

Current situation

- IF-MAP server running on a virtual machine (VMware with Infoblox meta data access point (MAP))
  - http://www.infoblox.com/en/solutions/technology-solutions/orchestration-if-map.html

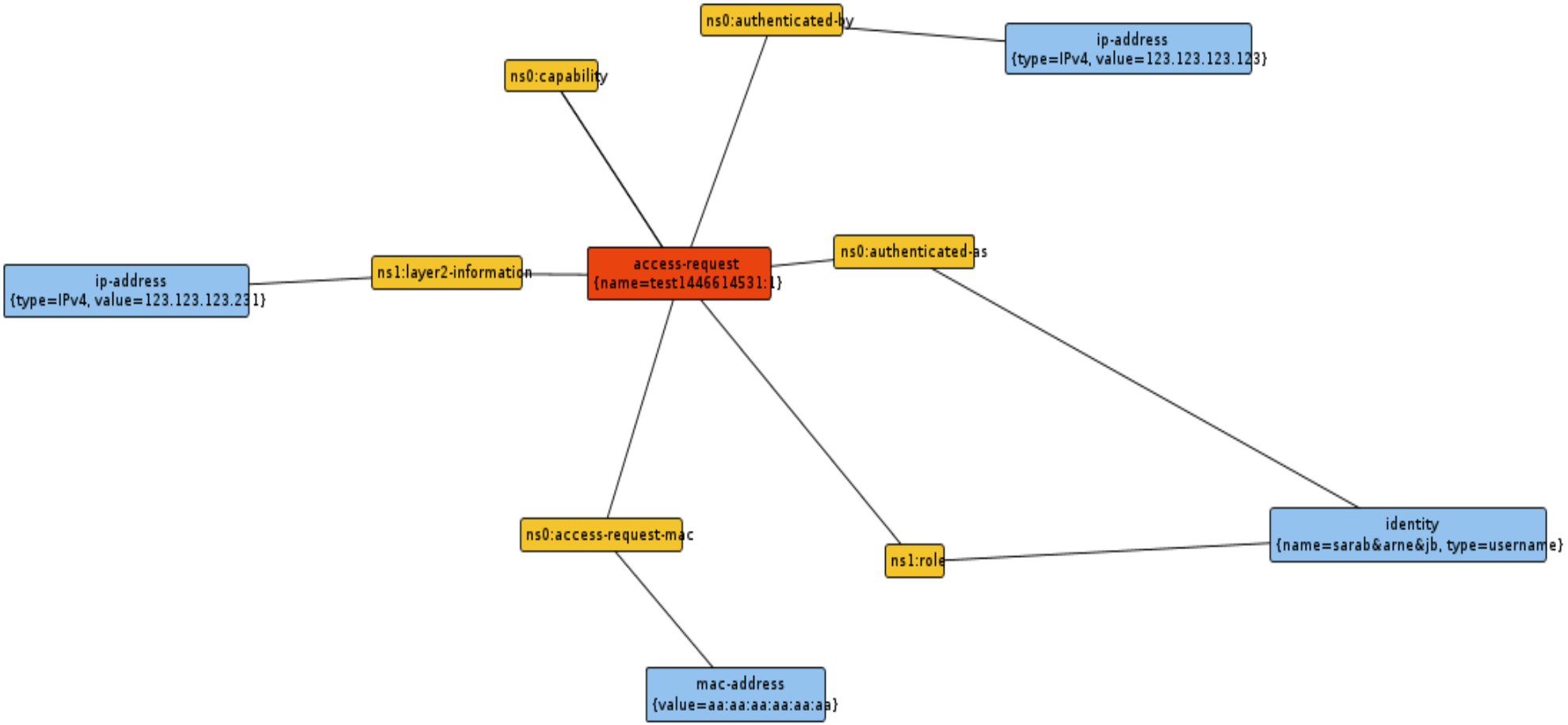
- omapd system
  - omapd is quite basic and naïve right now
  - http://code.google.com/p/omapd/

- irond – Intelligent Reaction on Network Events
  - http://trust.inform.fh-hannover.de/joomla/index.php/projects/iron

- 2 different systems publishing to the IF-MAP server – FreeRADIUS , ISC DHCPD (and test client generator!)

Loughborough University

IRON GUI



FreeRADIUS logging

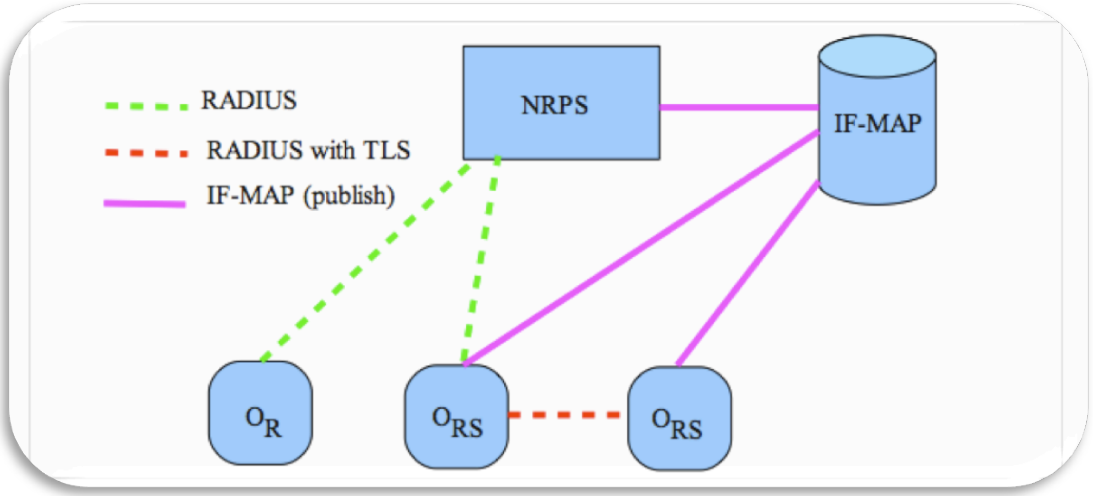
- Currently there is no ‘native’ support for MAP

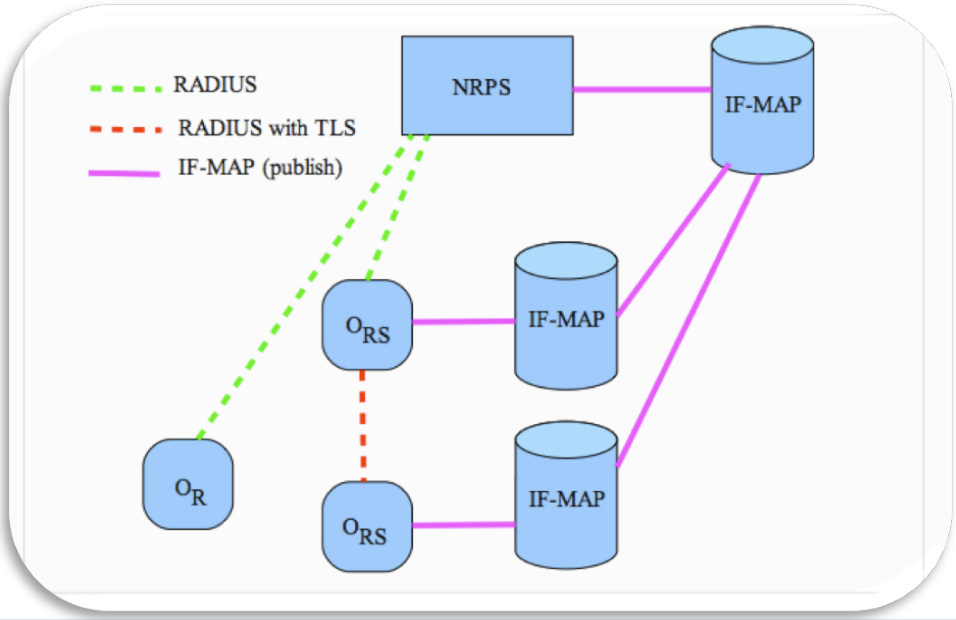
- So, we use log module…..

```
linelog ifmaplog {
        filename = ${logdir}/ifmap_log

        format = "%S,%{%{Packet-Type}:-unknown-method},%{User-
Name},%{%{Operator-Name}:-No_operator},%{%{Calling-Station-
ID}:-00:00:de:ad:be:ef},%{%{NAS-IP-Address}:-0.0.0.0},%{%{NAS-
Port}:-0}”
}
```

Architecture for the system





Loughborough University

Architecture for the system

- Completion of documentation for current work
- PERL code and handler for RADIATOR and RADSECProxy – not inline! (we'd like to see native support and for FreeRADIUS too)
- 'subscriber' and 'query engine'
- De-Duplication?
- F-Ticks integration – publisher and collector

Future…

- Will be looking for other parties to join trial in the 2nd stage

Questions…

- Questions and Comments