Introduction to eduroam

LEARN eduroam Workshop

6th May 2016

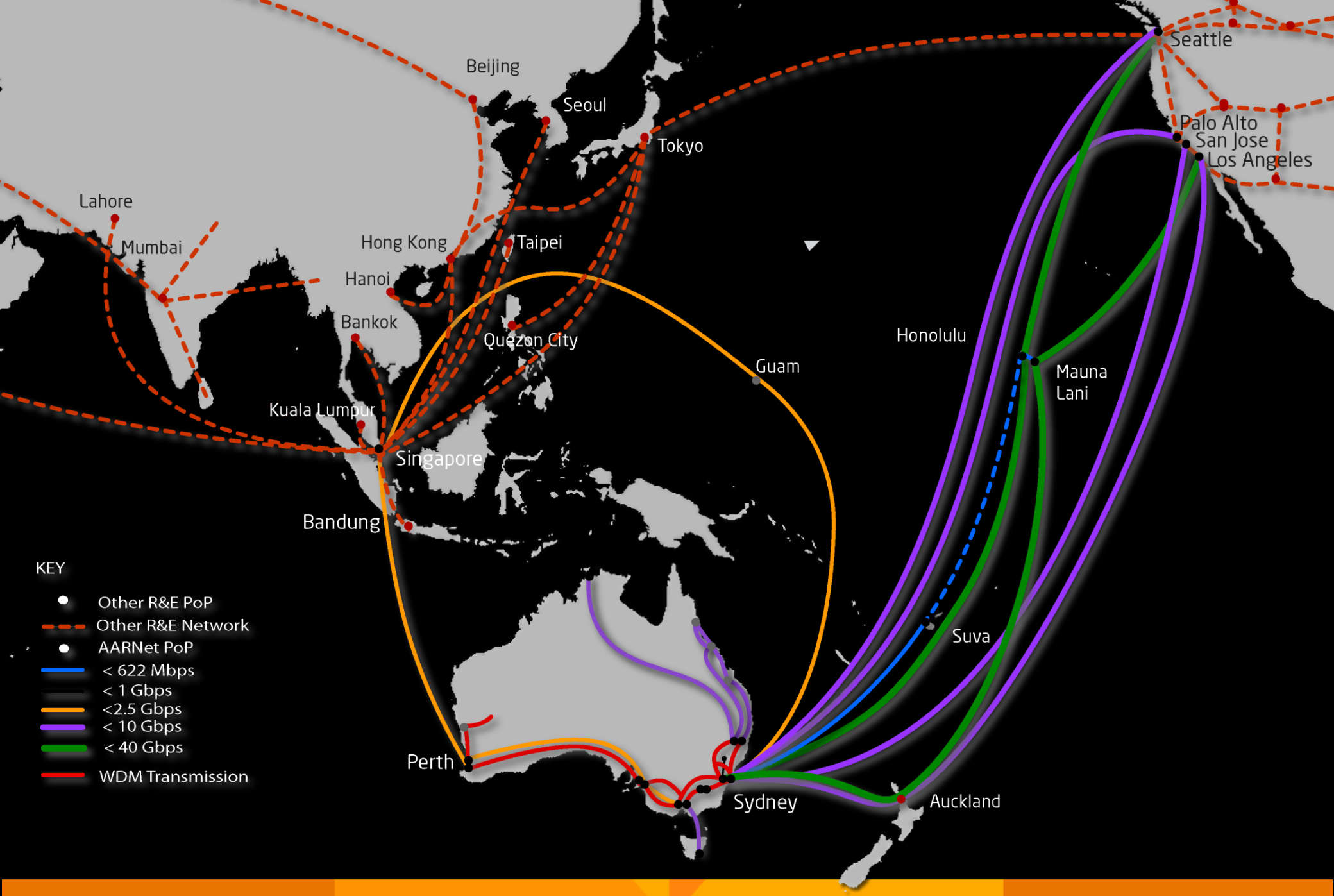
Introduction

- Paul Hii
  - Australia's National Research and Education Network (NREN)
    - UC & Video Service Manager
    - eduroam Service Manager
  - Trans-Eurasia Information Network eduroam Project
    - Project Coordinator

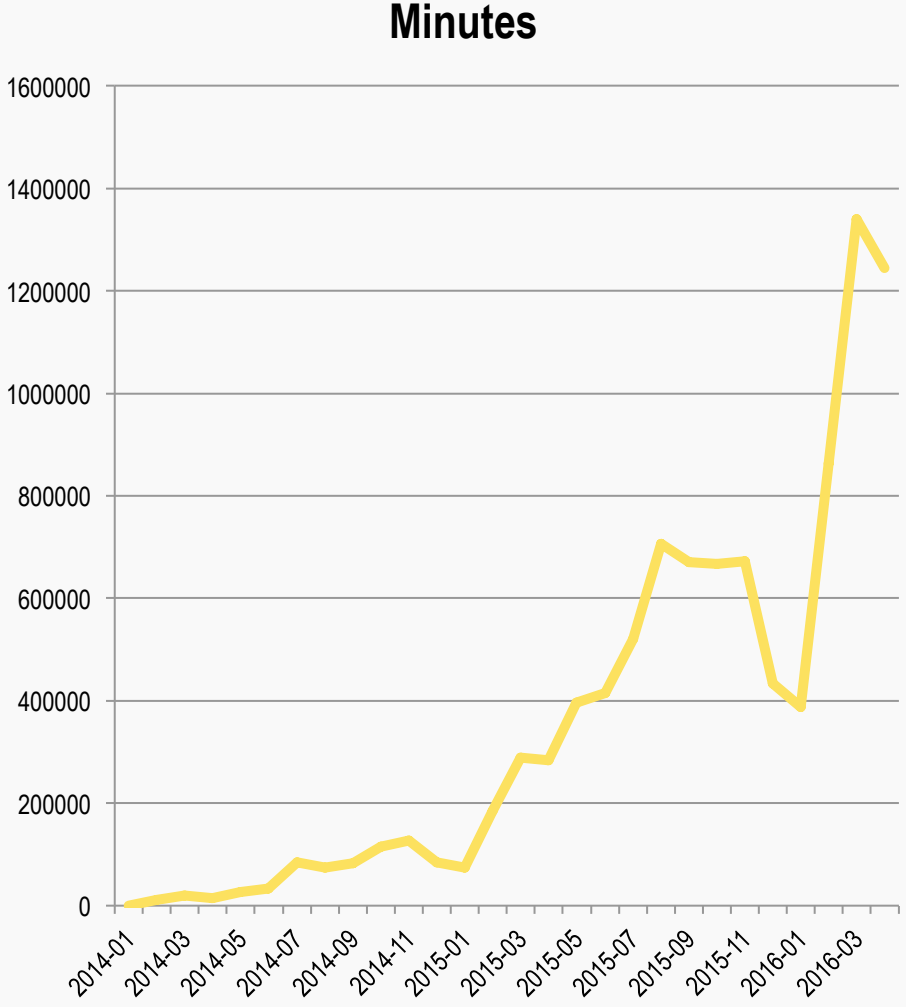
About AARNet

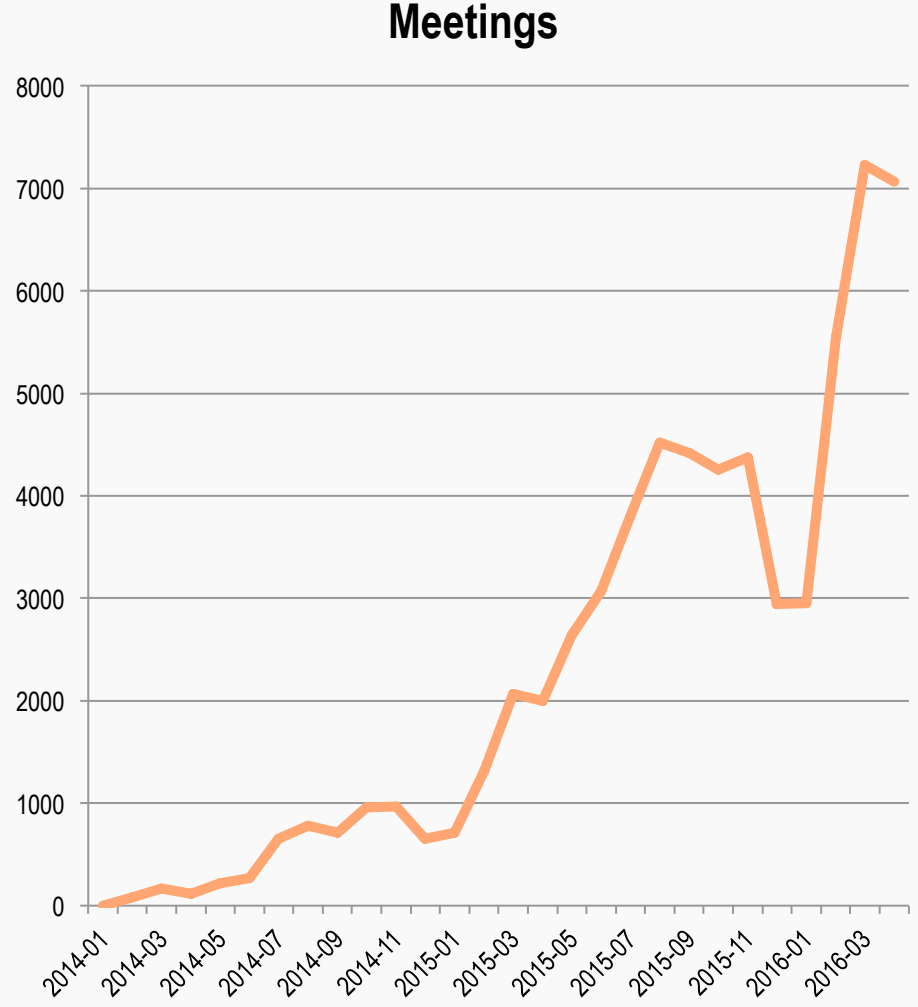
- Australia's National Research and Education Network (NREN)
- A registered carrier under the Australian Telecommunications Act.
- Operate our own dark fibre and optical transmission systems across the country
- High-end network designed specifically for Research and Education
  - Over-engineered to avoid congestion and allow for large data peaks.
  - Fault tolerant design.
  - Uncontended, dedicated connections.
  - Supports direct optical circuits, IPv6, IPv4 multicast, Jumbo frames
- Provide service to any R&E including to schools, TAFE, health and cultural.

- A Not-for-profit Company, owned by the Universities and CSIRO
- Most revenue comes from charges for services to members
- ~80 staff distributed across Australia
- ~120 connected organisations, ~ 1.5 million end-users

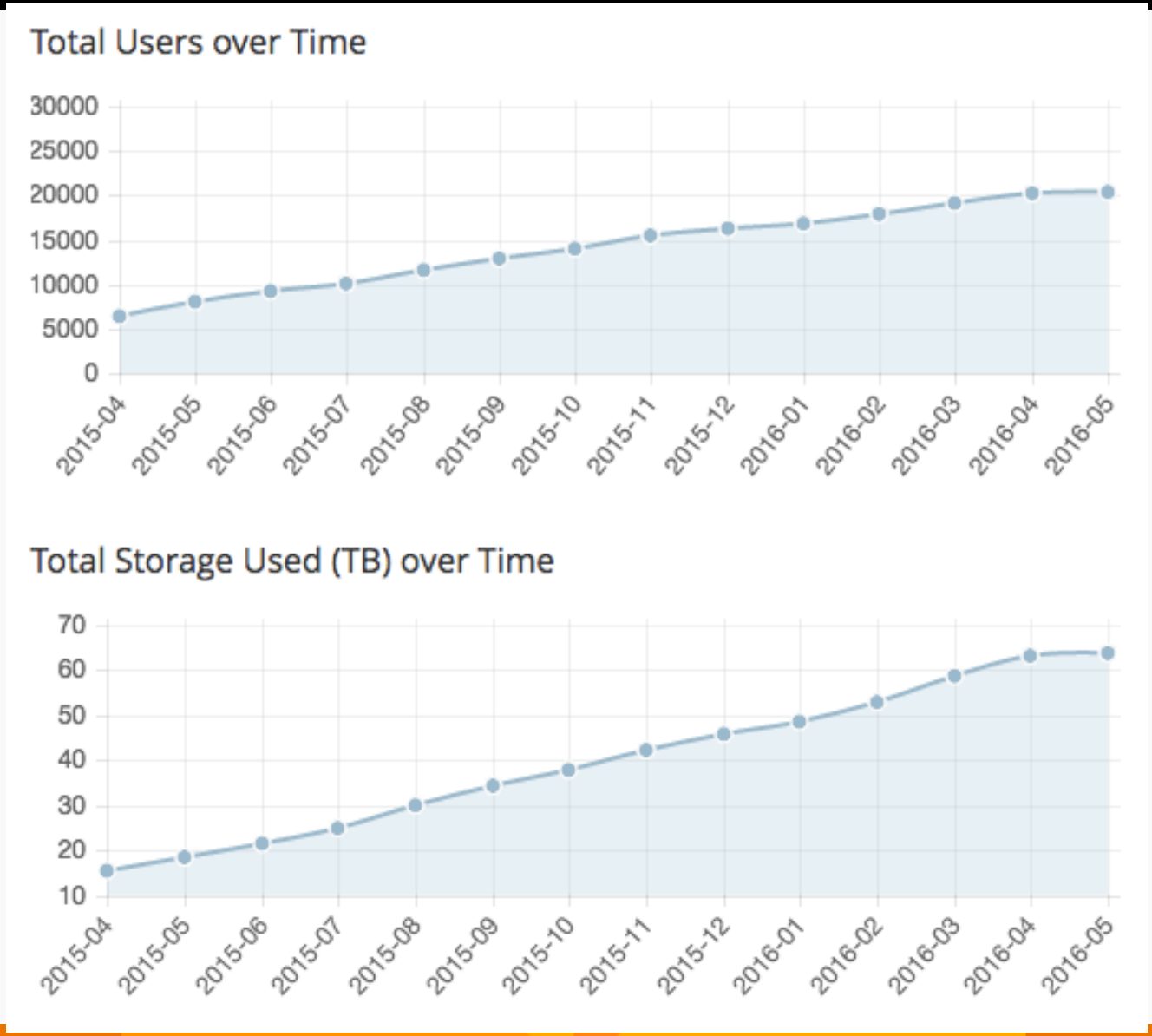

Seattle
Beijing
Seoul
Palo Alto
San Jose
Los Angeles
Tokyo
Lahore
Mumbai
Hong Kong
Taipei
Hanoi
Bankok
Quezon City
Honolulu
Guam
Mauna
Lani
Kuala Lumpur
Singapore
Bandung
Suva
Perth
Sydney
Auckland
KEY
Other R&E PoP
Other R&E Network
AARNet PoP
< 622 Mbps
< 1 Gbps
<2.5 Gbps
< 10 Gbps
< 40 Gbps
WDM Transmission

UC & Video


Minutes
1600000
1400000
1200000
1000000
800000
600000
400000
200000
0
2014-01
2014-03
2014-05
2014-07
2014-09
2014-11
2015-01
2015-03
2015-05
2015-07
2015-09
2015-11
2016-01
2016-03


Meetings
8000
7000
6000
5000
4000
3000
2000
1000
0
2014-01
2014-03
2014-05
2014-07
2014-09
2014-11
2015-01
2015-03
2015-05
2015-07
2015-09
2015-11
2016-01
2016-03

CloudStor


Total Users over Time
30000
25000
20000
15000
10000
5000
0
2015-04
2015-05
2015-06
2015-07
2015-08
2015-09
2015-10
2015-11
2015-12
2016-01
2016-02
2016-03
2016-04
2016-05
Total Storage Used (TB) over Time
70
60
50
40
30
20
10
2015-04
2015-05
2015-06
2015-07
2015-08
2015-09
2015-10
2015-11
2015-12
2016-01
2016-02
2016-03
2016-04
2016-05

XeAP Project

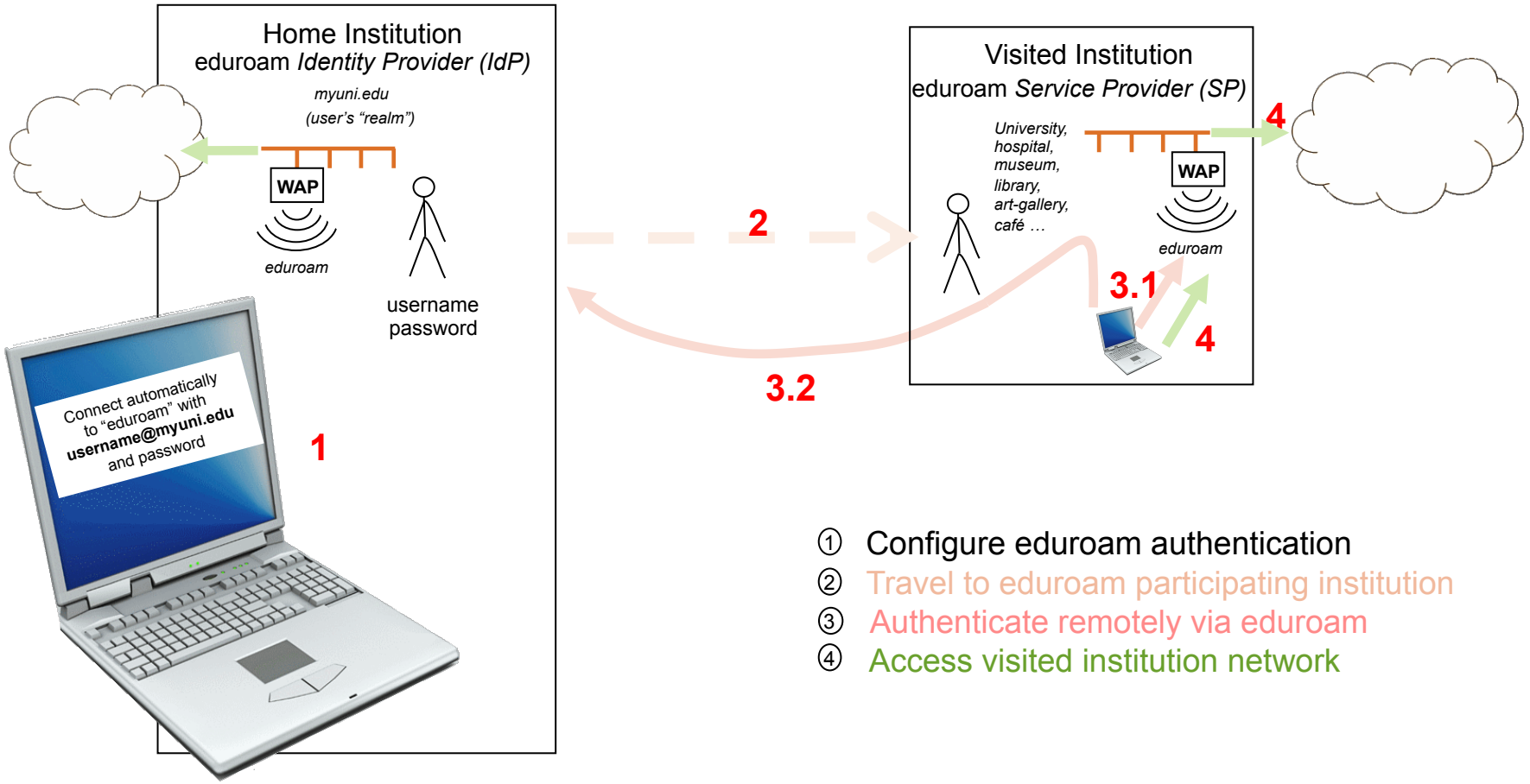
- e**X**tending **e**duroam into **A**sia **P**acific
- Project lead by AARNet and sponsored by TEIN*CC
  - Project Leader: John Batchelder
  - Project Coordinator: Paul Hii
  - Technical Leader: Neil Witheridge
- Funding for TEIN beneficiaries to implement eduroam in selected countries
- 7 countries: Bhutan, Indonesia, Malaysia, Nepal, Pakistan, Sri Lanka, Philippines
- Create resources to be shared with APAC countries.
- Achieve eduroam Compliance.
- More than just deploying RADIUS servers for eduroam.

Introduction

- EDUcation ROAMing
  - Easy network access when visiting other institutions.
- Started in 2002 in Europe
- Over 67 countries
- Global eduroam Governance Committee (GeGC)
- Hierarchy of RADIUS servers and 802.1x
- Defined in RFC7593
- Similar service - GOVROAM

What is eduroam (value proposition)

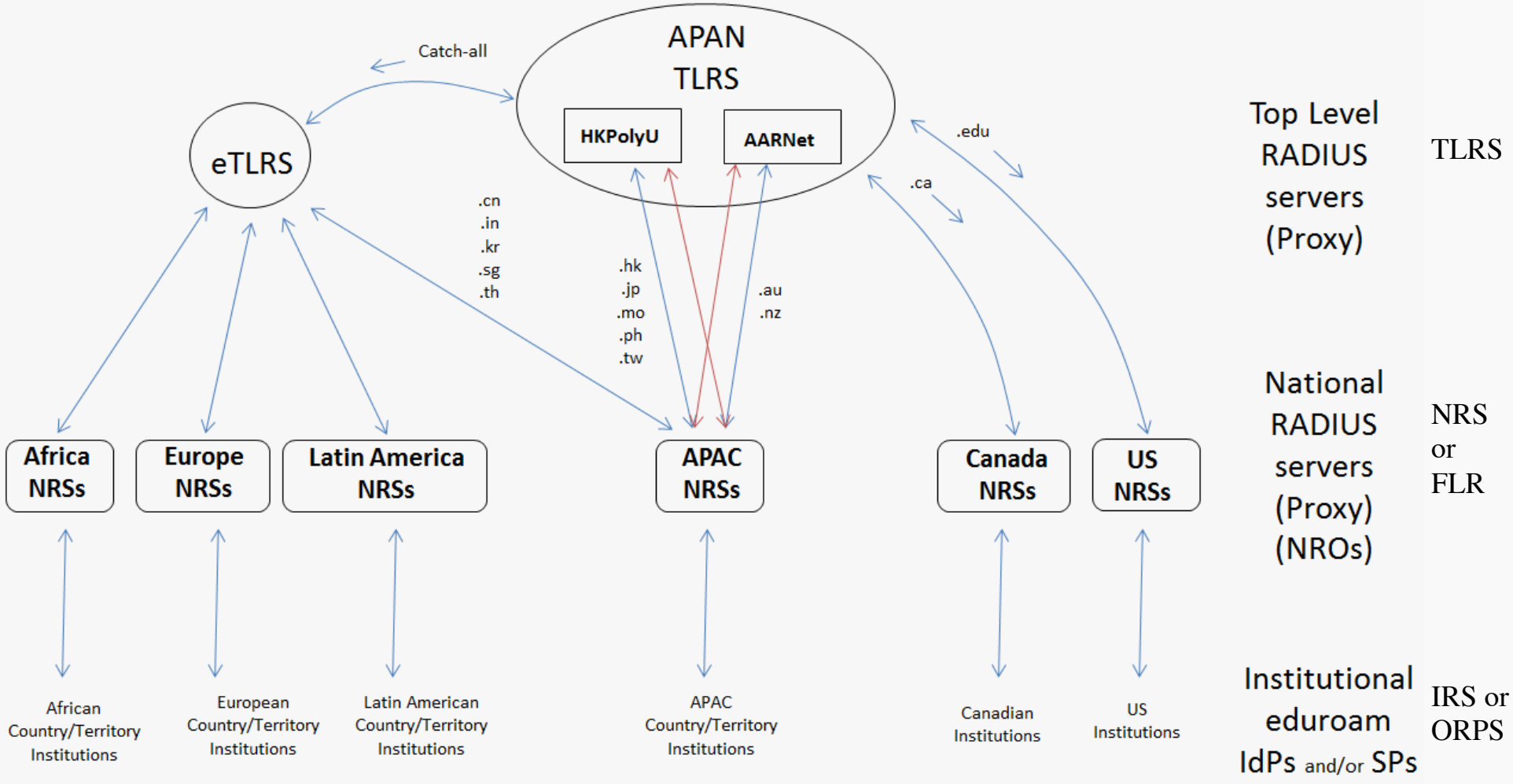
- Eduroam is a global service enabling education and research institution users' 'zero-effort' access to the network of visited eduroam participating institutions, by virtue of their remote authentication at their 'home' institution.



① Configure eduroam authentication
② Travel to eduroam participating institution
③ Authenticate remotely via eduroam
④ Access visited institution network

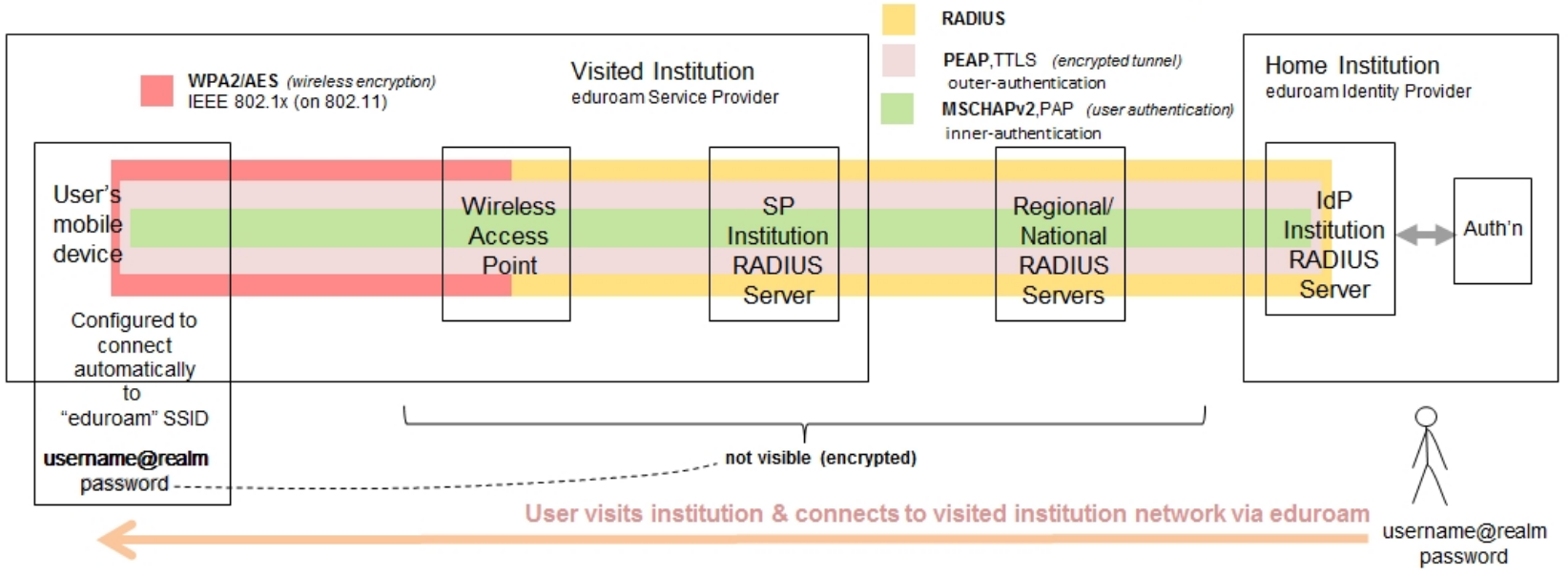
APAC Top-Level RADIUS Servers

- "Classical" eduroam uses hierarchical infrastructure
  - Institutional, National, Regional (Top-Level) RADIUS servers



What is eduroam (technical perspective)

- Infrastructure Components:
  - Supplicant, Network Access Server, RADIUS Servers (Proxy Servers, Authentication Server)
- Protocols: 802.1x (EAP over LAN), RADIUS with tunnelled EAP (TTLS, PEAP)
- Institutions have "Identity Provider" (IdP) (authenticate) and/or "Service Provider" (SP) (proxy for remote auth, grant access) roles



Authentication: RADIUS response "access accept"
Attributes: RADIUS attributes

RADIUS Transaction (wireshark)

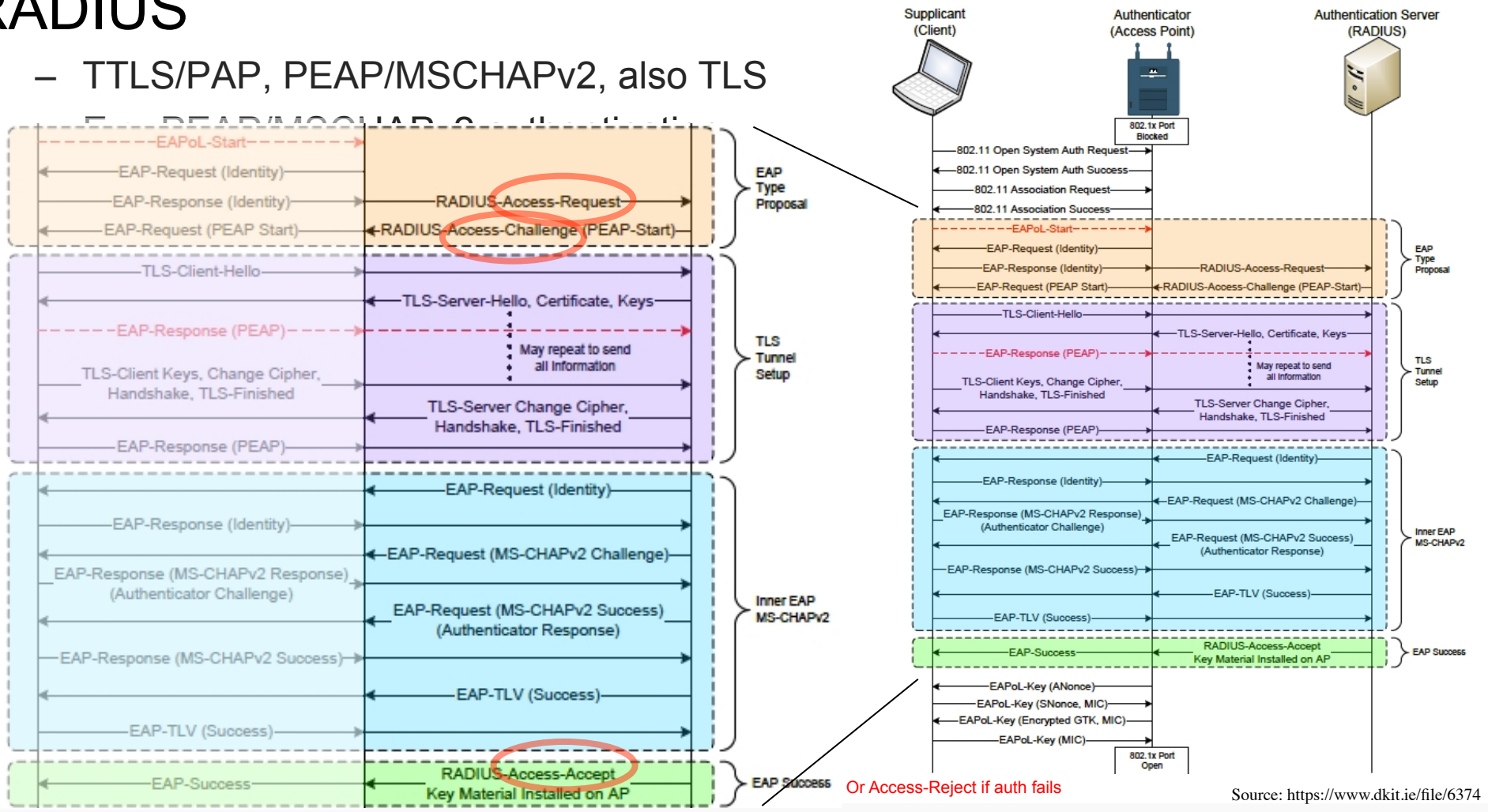
```
⊞ Frame 1: 305 bytes on wire (2440 bits), 305 bytes captured (2440 bits)
⊞ Ethernet II, Src: Supermic_fd:b4:24 (00:30:48:fd:b4:24), Dst: IETF-VRRP-VRID_01 (00:00:5e:00:01:01)
⊞ Internet Protocol Version 4, Src: 202.158.207.10 (202.158.207.10), Dst: 131.181.108.226 (131.181.108.226)
⊞ User Datagram Protocol, Src Port: 34746 (34746), Dst Port: radius (1812)
⊟ Radius Protocol
   Code: Access-Request (1)
   Packet identifier: 0x9a (154)
   Length: 263
   Authenticator: 19fa69641803a8a40213a01552871a6a
 ⊟ Attribute Value Pairs
   ⊞ AVP: l=21  t=User-Name(1): [redacted]@qut.edu.au
   ⊞ AVP: l=3  t=Chargeable-User-Identity(89): \000
   ⊞ AVP: l=6  t=Location-Capable(131): Civix-Location(1)
   ⊞ AVP: l=19  t=Calling-Station-Id(31): f0-db-e2-a1-1a-7b
   ⊞ AVP: l=27  t=Called-Station-Id(30): 0c-d9-96-05-62-60:eduroam
   ⊞ AVP: l=6  t=NAS-Port(5): 13
   ⊞ AVP: l=49  t=Vendor-Specific(26) v=ciscoSystems(9)
   ⊞ AVP: l=6  t=NAS-IP-Address(4): 172.16.192.68
   ⊞ AVP: l=5  t=NAS-Identifier(32): ib1
   ⊞ AVP: l=12  t=Vendor-Specific(26) v=Airespace, Inc (formerly Black Storm Networks)(14179)
   ⊞ AVP: l=6  t=Service-Type(6): Framed(2)
   ⊞ AVP: l=6  t=Framed-MTU(12): 1300
   ⊞ AVP: l=6  t=NAS-Port-Type(61): Wireless-802.11(19)
   ⊞ AVP: l=6  t=Tunnel-Type(64) Tag=0x00: VLAN(13)
   ⊞ AVP: l=6  t=Tunnel-Medium-Type(65) Tag=0x00: IEEE-802(6)
   ⊞ AVP: l=6  t=Tunnel-Private-Group-Id(81): 3900
   ⊞ AVP: l=26  t=EAP-Message(79) Last Segment[1]
   ⊞ AVP: l=18  t=Message-Authenticator(80): 2eb87a203d78f1ef3d17e11375ea7a97
   ⊞ AVP: l=5  t=Proxy-State(33): 323337
   ⊞ AVP: l=4  t=Proxy-State(33): 3132
```

See RFC2865

1	Access-Request
2	Access-Accept
3	Access-Reject
4	Accounting-Request
5	Accounting-Response
11	Access-Challenge
12	Status-Server (experimental)
13	Status-Client (experimental)
255	Reserved

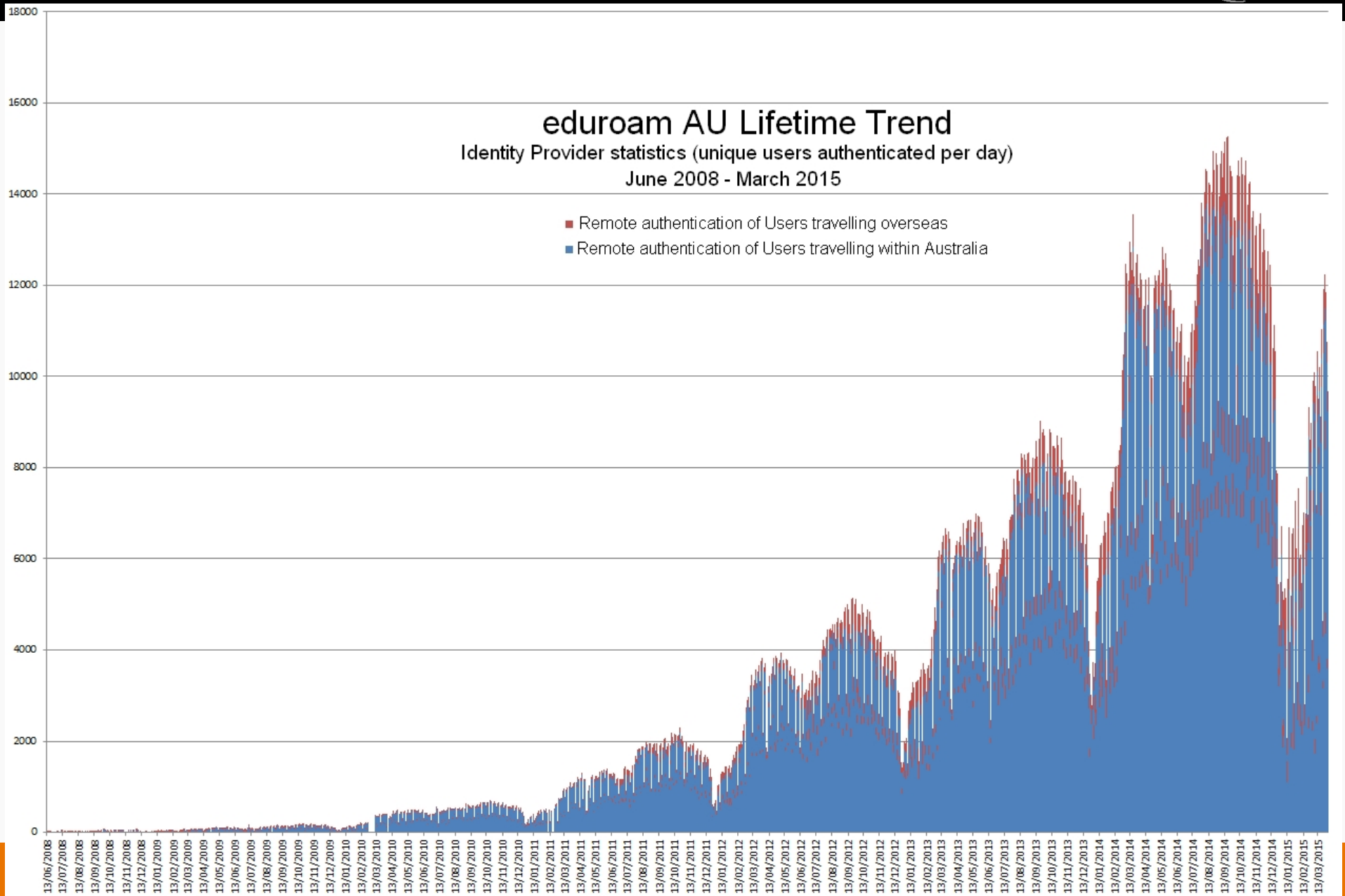
RADIUS Transaction Overview

- NRO admin needs to understand tunneled EAP/ RADIUS
  - TTLS/PAP, PEAP/MSCHAPv2, also TLS

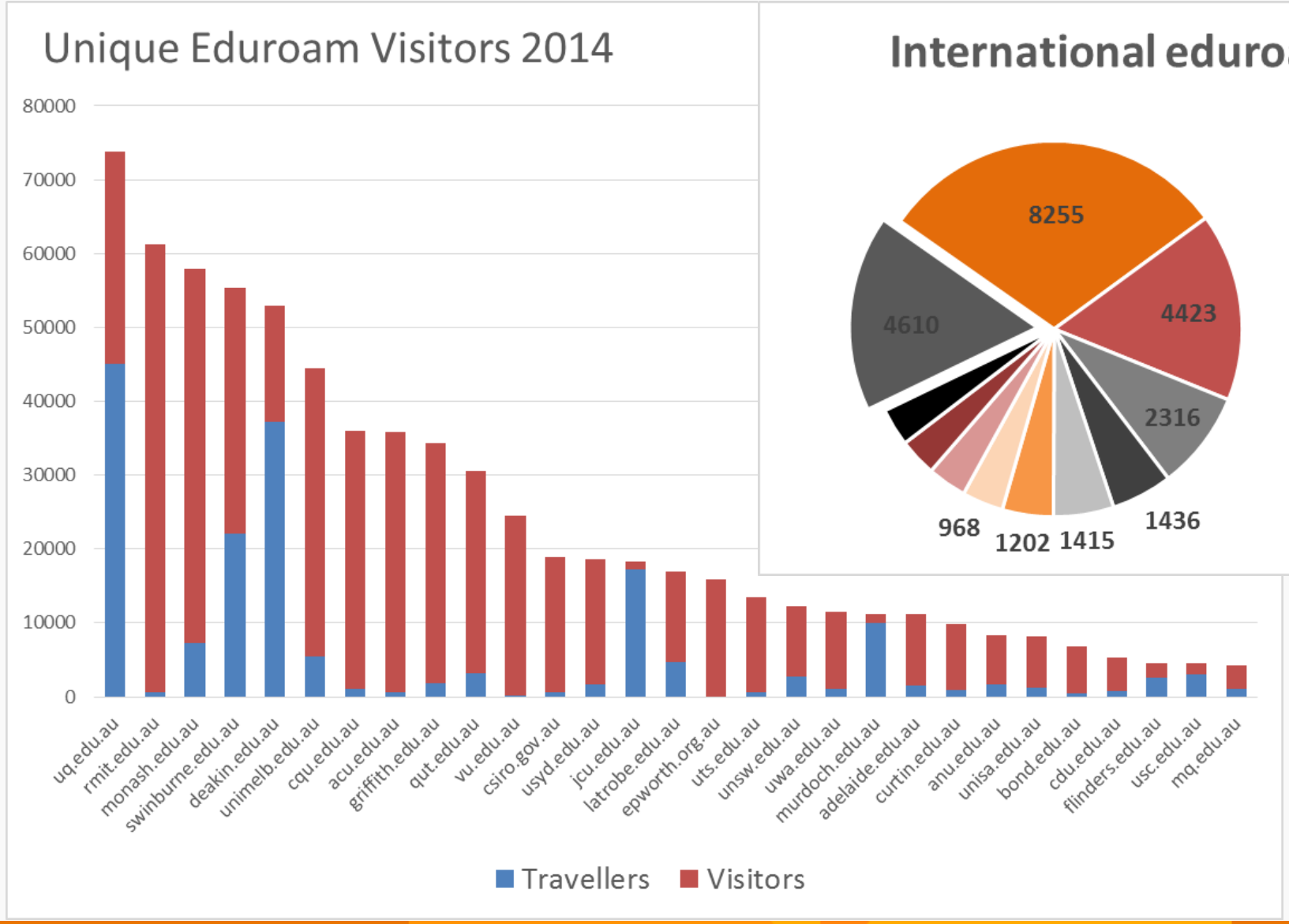


Source: https://www.dkit.ie/file/6374

eduroam AU


eduroam AU Lifetime Trend
Identity Provider statistics (unique users authenticated per day)
June 2008 - March 2015
Remote authentication of Users travelling overseas
Remote authentication of Users travelling within Australia
18000
16000
14000
12000
10000
8000
6000
4000
2000
0

eduroam AU


Unique Eduroam Visitors 2014
80000
70000
60000
50000
40000
30000
20000
10000
0
uq.edu.au
rmit.edu.au
monash.edu.au
swinburne.edu.au
deakin.edu.au
unimelb.edu.au
cqu.edu.au
acu.edu.au
griffith.edu.au
qut.edu.au
vu.edu.au
csiro.gov.au
usyd.edu.au
jcu.edu.au
latrobe.edu.au
epworth.org.au
uts.edu.au
unsw.edu.au
uwa.edu.au
murdoch.edu.au
adelaide.edu.au
curtin.edu.au
anu.edu.au
unisa.edu.au
bond.edu.au
cdu.edu.au
flinders.edu.au
usc.edu.au
mq.edu.au
Travellers
Visitors

International eduroam visitors
8255
4423
2316
1436
1415
1202
968
4610
United Kingdom
Germany
Netherlands
United States
Denmark
Sweden
Hong Kong
Canada
New Zealand
Norway
42 Other Countries

eduroam Service Pre-Requisites

- Trusted protocols, infrastructure and operators
  - Trust model that meets the requirements of the service.
- Technical & administrative capability of NRO
  - eduroam relies on NRO competencies
  - Willingness and ability to devote required resources
- Technical & administrative capability of Institutions
  - eduroam relies on institutional competencies
  - Identity Management at institutions
  - Wireless infrastructure operability
- Business-case for eduroam
  - eduroam relies on institutional & end-user demand
  - Establishment of a business-case justifying cost & effort

Institutional eduroam participation (IdP+SP)

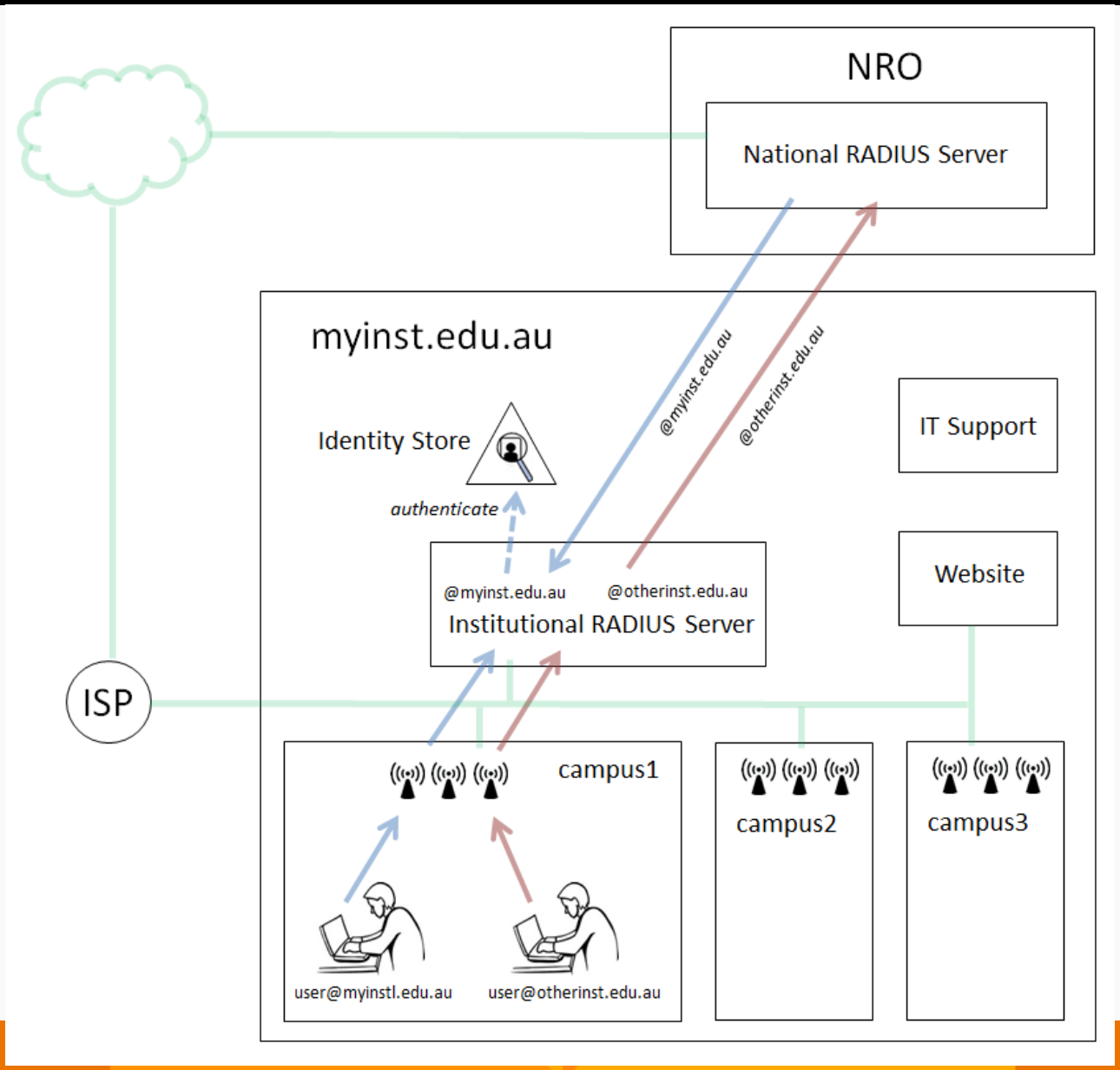
- Pre-requisites for Institution
  - Effective Identity Management
  - Operational wireless infrastructure
  - Institutional network access and Acceptable Use Policy
  - Availability of support for eduroam at the institution
- Global & National eduroam policy agreement
- Planning & Joining Process
  - Planning: Wireless 802.1x, Traffic handling (VLAN, IP addressing, protocols), RADIUS Server deployment (realm, attributes , logging, test user, trust test&monitoring server, certificate), Support, Webpage
  - Institutional deployment info into eduroam AdminTool
  - Institutional deployment of RADIUS server, network access
  - National RADIUS Server configuration
  - Operability Testing & Auditing

Questions?

End of Introduction

INSTITUTIONAL EDUROAM DEPLOYMENT

Typical Institutional Deployment



Institutional eduroam participation (IdP+SP)

- Application to participate in eduroam
  - involving the exchange of institutional and basic eduroam deployment planning information allowing the National Roaming Operator (the NRO) to assess the institution's satisfaction of pre-requisites and ability to operate sustainably as an eduroam participant
- Deployment of eduroam
  - Satisfying technical and administrative requirements
- eduroam Operability Audit
- Commencement of participation
  - NRO announcement of the institution's participation in eduroam to current eduroam national participants, and globally via upload of the institution's eduroam deployment data to the eduroam global database

Institutional Technical Pre-Requisites

(To be assessed during 1st step of institutional joining process)

- Identity Management
  - Directory
  - Realms supported
  - Provide institutional test accounts for testing/monitoring/troubleshooting
- Wireless Infrastructure
  - Coverage
  - IEEE 802.1x
- Network Access
  - ISP, if not NREN
  - Acceptable Use Policy
- IT Support
  - RADIUS/IdP capability, Helpdesk, eduroam webpage

Institutional Wireless Infrastructure

- 802.1x capable
- Broadcast of SSID “eduroam”
  - Issue relating to overlapping hotspots
  - Potential of IEEE 802.11u to alleviate issue
- Wireless coverage across campuses
  - Availability of coverage maps
  - Incidental hotspots
- Encryption support (WPA2-Enterprise required)
- Tunneled EAP Protocol
  - Choice of inner-authentication (depends on identity store)
- Limitations of WiFi Supplicants on various platforms
  - See presentation by GEANT comparing supplicants

Network Access Service

- Successful authentication -> network access for user
- SP role eduroam objectives
  - Provide open network access according to local policy
    - (unconstrained compared with users home environment)
  - See list of recommended network protocols
- Network Characteristics
  - Segregation of eduroam user traffic via VLAN
  - IP Address allocation (DHCP, NAT'ing, range available)
  - Application Proxy (http proxy)
  - Traffic constraints
    - Data rate limiting, data volume quota

Institutional eduroam Implementation

- Institutional RADIUS server must comply with RFC2865
  - FreeRADIUS, Radiator, Cisco ISE, Microsoft NPS (+ RadSecProxy)
  - Others in use: Cisco ACS, Microsoft IAS, Aruba Clearpass
- Deploy RADIUS servers
  - Preferrably public ip address and firewall access provisioned
  - Accurate clock synchronisation
  - Enable trusted client access
- Determine authentication protocols for local realm
  - Supported clients
  - User credentials store
- Acquire server certificate
  - Establish TLS session
  - Same certificate for all RADIUS servers. FQDN but need not DNS name.
  - Provide CA and intermediate certificates if not pre-trusted
- Authentication logging, includes attributes.

Institutional RADIUS Server

- Requirements for proxied RADIUS requests
  - RADIUS Attributes
    - Filtering to release only required attributes
    - Generate Chargeable-User-Identity (CUI) (for IdP role)
    - Include Operator-Name (ON) (for SP role)
  - Terminate (i.e. don't proxy) accounting requests
  - Configure bogus realm black-listing
    - E.g. "*.3gppnetwork.org"
  - Reject request with badly formatted username (e.g. invalid char's)
  - Use Status-Server to handle non-responsive servers
  - Configure trust for NRO Test and Monitoring Server (TMS)

Institutional RADIUS Server (cont'd)

- Deployment considerations
  - Time synchronisation (NTP)
  - Server Redundancy (high-availability deployment)
  - Load-balancing
- RADIUS Request Logging
  - Trust model – ability to trace a network access to a real user
  - Traceability of Users achieved via logging
  - Attributes to be logged
    - DateTimeStamp, User-Name (outer) i.e. realm, Packet Type (Access-Accept, Access-Reject), Chargeable-User-Identifier,
      NAS-IP-Address (IP address of adjacent RADIUS client, i.e. NAS or proxy server),
      Operator-Name (identifier for institution providing network access),
      Calling-Station-ID (MAC address of user device)

RADIUS Attributes

- Set of attributes required (at a minimum) to support eduroam

ref. https://community.jisc.ac.uk/library/janet-services-documentation/faqs-eduroam-system-administrators-and-implementation-techs)

- Below attributes **must NOT** be filtered out of RADIUS messages of type Access-Request, Access-Challenge, Access-Accept, Access-Reject

1. User-Name *username@realm (note username might be anonymous)*
4. NAS-IP-Address *IP address of adjacent NAS or RADIUS proxy from which request received*
18. Reply-Message *Reason, for Access-Reject for example.*
24. State
25. Class
31. Calling-Station-ID *User device MAC address*
33. Proxy-State
79. EAP-Message ← Inner-authentication RADIUS attributes (encrypted)
80. Message-Authenticator
89. Chargeable-User-Identity *Unique, opaque identifier for user*
126. Operator-Name *Identifier for visited institution i.e. where authentication request originated*

Info to be logged

and Microsoft vendor specific attributes: MS-MPPE-Send-Key, MS-MPPE-Recv-Key

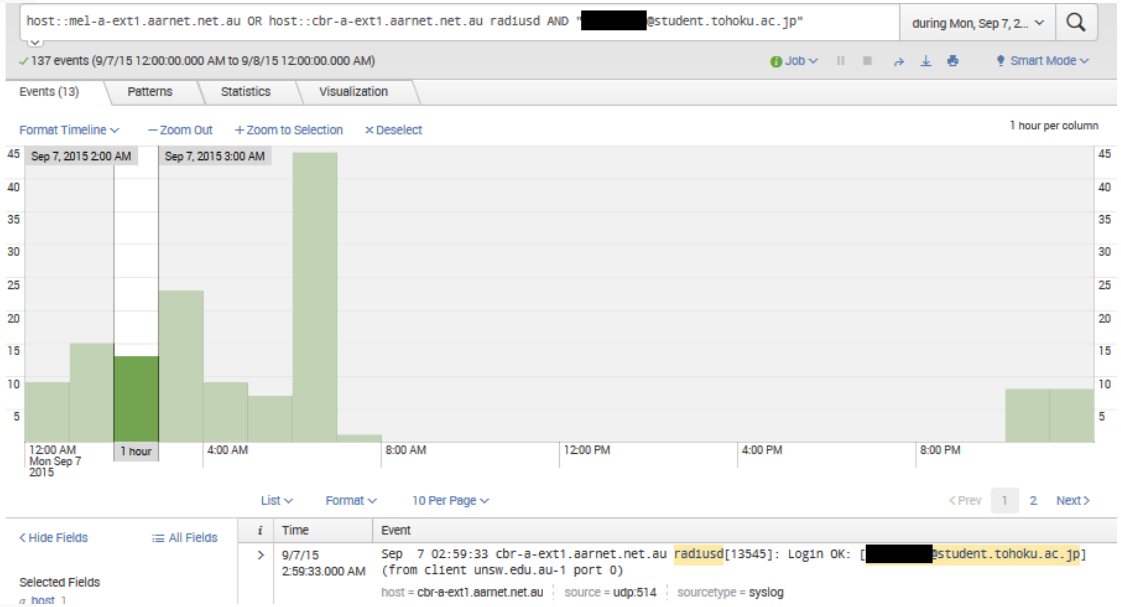
- For RADIUS Accounting Messages

(institutions **should not proxy** local accounting requests, but can't control what comes in)

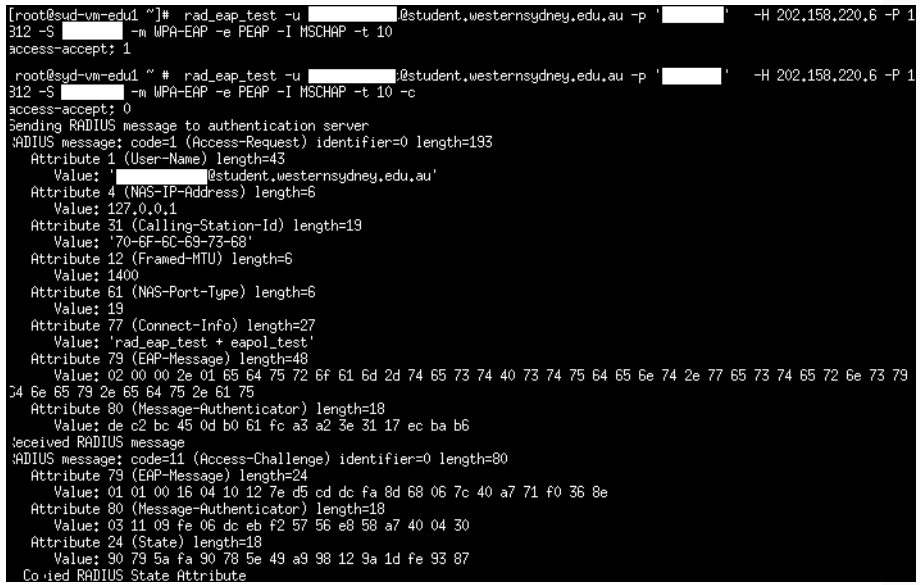
1. User-Name
25. Class
33. Proxy-State
40. Acct-Status-Type
44. Acct-Session-ID

Tools of trade for eduroam

- Troubleshooting tools
  - rad_eap_test RADIUS client (wrapper around WPA supplicant eapol_test)
  - Logs/splunk/ELK
  - Wireshark/tcpdump



Splunk query & output



rad_eap_test request & output

RADIUS Server(s)

Choice of RADIUS Server
Server & CA certificates
IP addressing
RADIUS auth/acct ports
Protocol support
Time synchronisation
Accounting off

Redundancy?
Load-balancing? Fail-over?

Log location & retention period
Use of Syslog

Local Monitoring
Local log analysis (metrics?)
- (e.g. Splunk)

Trust Access Points, secret
Trust NRSs, secret
Trust NRO TMSs, secret

IdP

Decide on local realm(s)
& corresponding identity Store(s)

Auth requests from AP,NRS,TMS

Provide local test account to NRO

Select Authentication methods
(PEAP/MSCHAPv2 and/or
TTLS/MSCHAPv2 or TTLS/PAP)

Release Chargeable-User-Identity

Policy on Anonymous Outer-ID
Support? User recommendation?

Handle local user authentication
i.e. local user connection @home

Capture authentication event logs

SP

Non-local realms proxied to
National RADIUS Server(s) (NRSs)
Configure proxy to NRSs

Auth requests from AP, TMS
NRO TMS test account

Non-responsive server handling
Status-Server

Attribute release (minimal)
Release Calling-Station-ID (MAC)
Release Operator-Name
Request Chargeable-User-Identity

Malformed user-name filtering (reject)
Known bad realm filtering (reject)

Accounting Request handling

Capture network access event logs

AARNet NRS Configuration

Remote test account
Operability testing

Wireless Infrastructure

Broadcast SSID: "eduroam"

Encryption/Access Control:
-> IEEE 802.1X
(WPA2-AES aka WPA2-Enterprise)

Authentication Server(s)
-> Local RADIUS Server(s)

Security requirements i.e. EAP-TLS
or Tunneled EAP Protocol

eduroam Coverage Plan:
- Campuses
-> Campus Information to NRO
- Coverage Map

Special considerations:
- eduroam hotspot overlap?
- Incidental authentications

Network Access

Ports/protocols open
Bandwidth/Performance

VLAN for eduroam users
Local users vs visitors

IP-Addressing
DHCP
NAT'ing
IPv6?

Application Proxies
Transparent?
If not, IP address/port info

Restrictions
Rate limiting (throttling)
Data volume (quotas)

Per campus differences

Institutional Support

School eduroam contacts
Mail-list subscription
NRO monitoring and metrics

Local IT support eduroam training

Local Support role & workflow
Access to logs

Service Request Escalation policy:
IT Support->eduroam admin->NRO

User education, security awareness
Local eduroam promotion
User responsibility
School responsibility to take action
educate userson home configuration

End-user device configuration
Configuration Assistant Tool (CAT)

Eduroam Webpage

Checklist:
Eduroam overview
Policy compliance
Roles (IdP+SP)
User responsibility and local AUP
Links to NRO and global resources

IdP Info:
Authentication Methods
Device Configuration (CAT)
Configure while on campus

SP Info:
SSID
Encryption
Network service characteristics

Logging
Privacy
Support

Handling network abuse

Questions?

Next … lets build an institutional RADIUS for eduroam

Thank-You

Please send feedback/questions to:

Paul.Hii@aarnet.edu.au