



Edward Wincott, JANET(UK)

MRC IT Managers Meeting, March 11th 2010



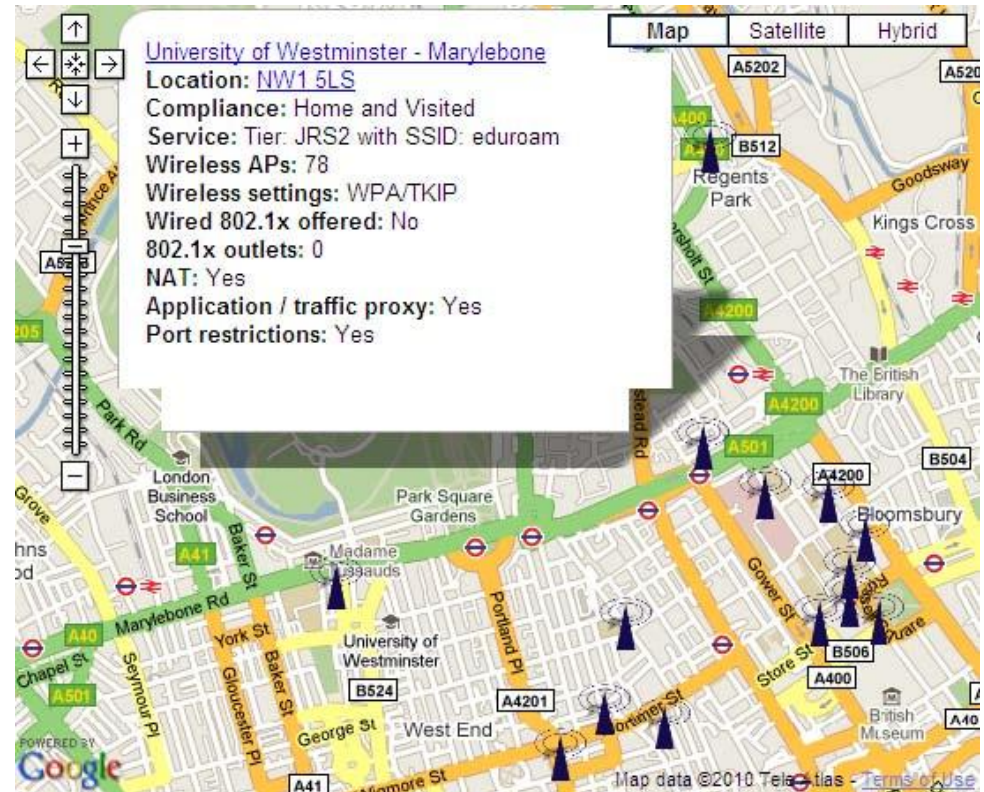
JANET Roaming – eduroam

- JANET Roaming provides eduroam in the UK
- Enables JANET-connected organisations to offer high quality secure network services for visitors
- Without the need for guest account management
- Visitors use their home organisation username and password
- Saving IT Support workload
- Provides easy to use, convenient and secure network service for researchers, staff, students and visitors
- Access to the Internet and home organisation remote access services – e.g. VPN, webmail etc



eduroam – in practice

- Before arriving - visitor checks service available
- One-off configuration of supplicant software
- Uses 802.1X
- Set wireless ciphers for eduroam SSID to (e.g.) WPA/TKIP
- Set username and password





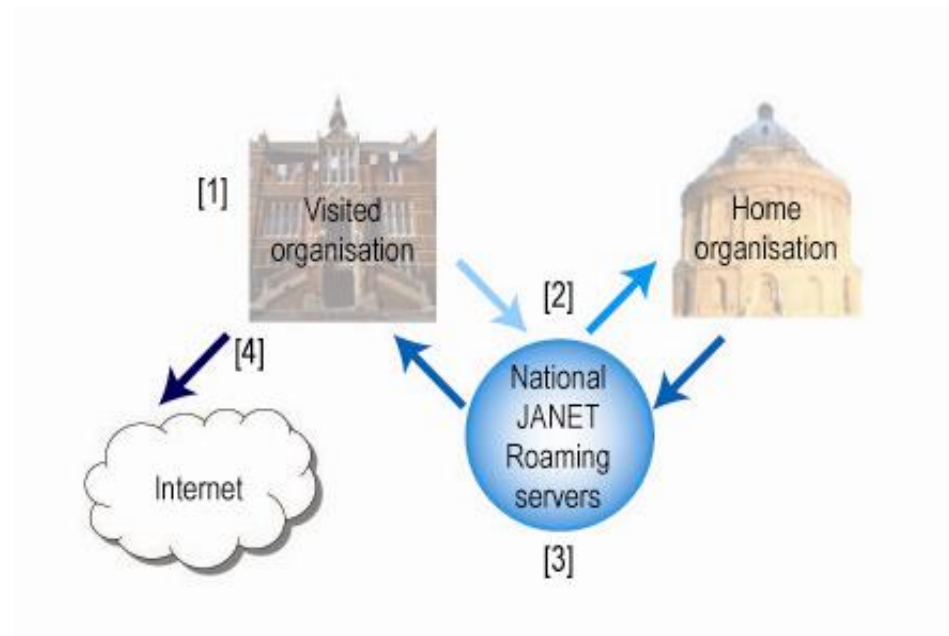
eduroam – global username and password

- Username: the same as or similar to the username as utilised on the home network
- Format: common-name@realm
e.g. fred@example-university.ac.uk
- Password: same password as used on home network
- Why? Authentication is actually carried out at the home organisation
- How? RADIUS is used to carry the authentication traffic via a national – international hierarchy of peered RADIUS servers



eduroam – remote authentication

1. User enters username and password
2. Authentication request forwarded to home organisation via JANET Roaming
3. User's credentials authenticated at home organisation, response sent back to visited site
4. User gains network access





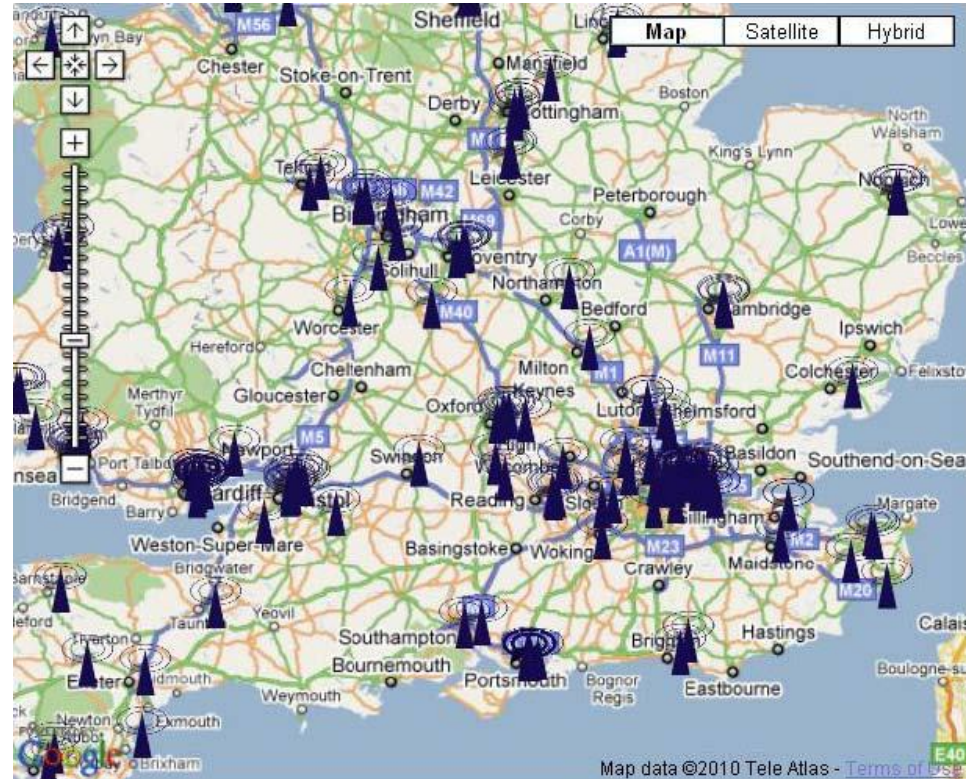
eduroam in the UK

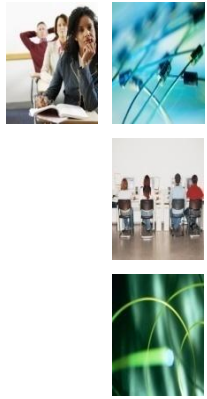
- 115 registered organisations (an increase of 18 over past year)
- 68 organisations offering operational service
- Majority are from Higher Education sector – but membership includes Further Education and research organisations
- 350 individual site locations
- 16,000 unique users per month (inter-site authentications)



eduroam in the UK – site locations

- Screenshot of zoomable map of locations where eduroam is available in UK
- www.ja.net/roaming
- Navigate to Sites Locations map





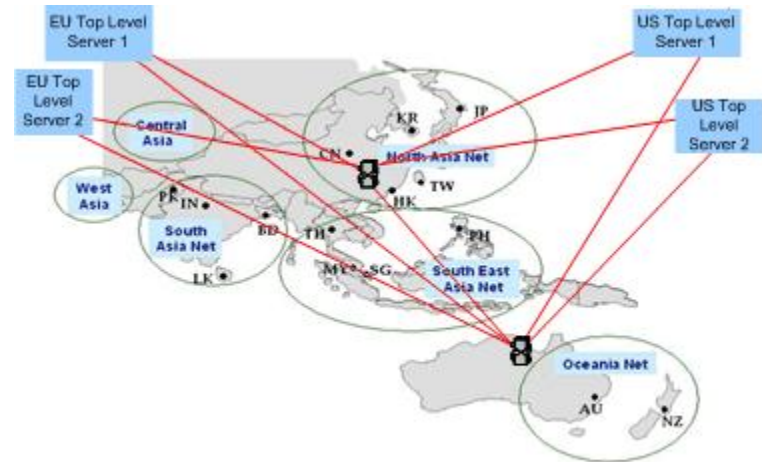
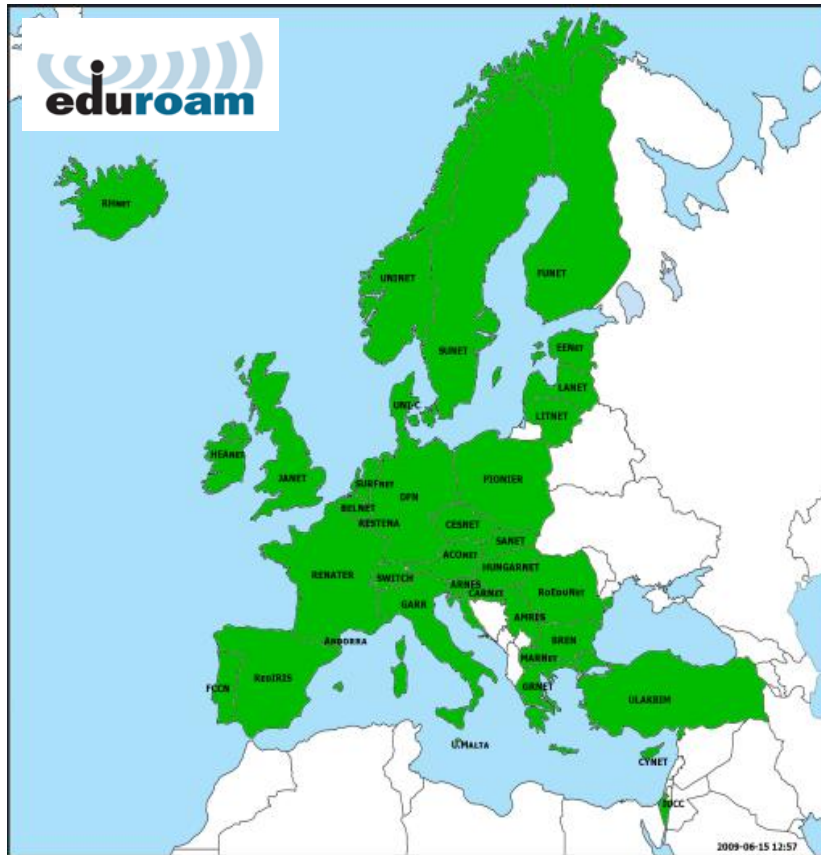
eduroam confederation



- 36 European countries
- South East Asia and North America
- Based on the same technology (RADIUS)
- European Top Level RADIUS Servers and International RADIUS Proxy Servers run by TERENA in Denmark and the Netherlands - enable international roaming
- <http://www.eduroam.org/>



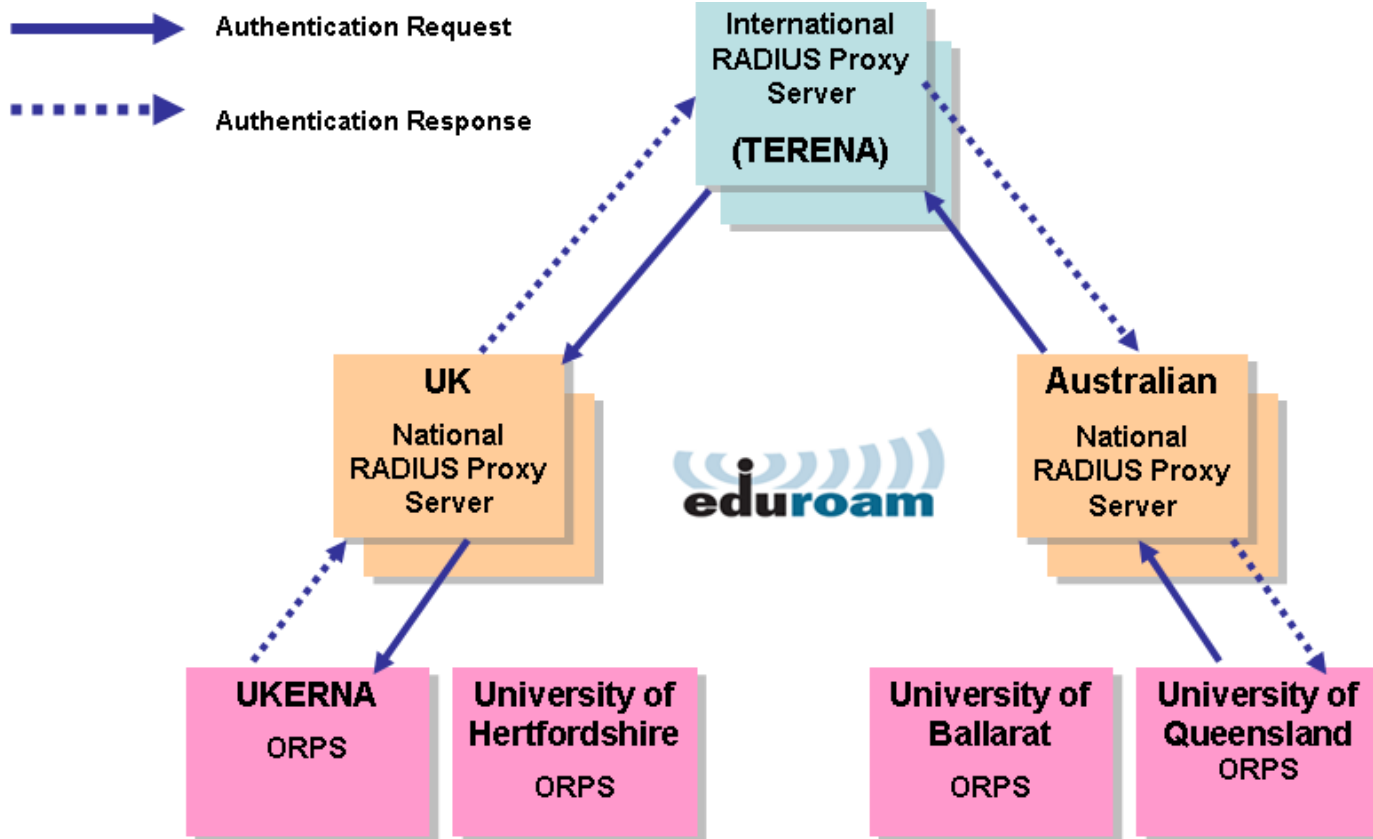
eduroam confederation members





eduroam – international RADIUS hierarchy

European Top Level Radius Servers and International RADIUS proxy servers (IRPS) operated by eduroam service activity organisation, eduroam SA (funded by TERENA/Geant)





eduroam – fundamentals

- Federated service – the only way to provide a pervasive service at participant organisations
- Co-operating organisations build their own infrastructures which interoperate to provide a global service
- Built on 802.1X technology – RADIUS server and EAP authentication
- Peering with JANET Roaming Service national proxy server infrastructure is free of charge
- Organisations which already have 802.1X infrastructure can implement a nil additional expense, otherwise cost is only RADIUS server
- Free to user at the point of use
- It is not just a wireless service, 802.1X can be provided over wired network too



JANET Roaming – why 802.1X

- Considered alternatives – VPN, web redirect/captive portal
- Investigated during Location Independent Networking trial
- Implementations had to be scalable and secure
- Initial JANET Roaming Service inclusive of WRD and WEP as well as the preferred 802.1X technology and WPA
- JANET Roaming Service differentiated from 'eduroam' - but has always interoperated with eduroam SAO
- Resulted in 'JRS Tiers' system (May 2006 – Feb 2009):
 - JRS1: WRD WEP IPv4 may-NAT eduroam-web
 - JRS2: 802.1X WEP, WPA/TKIP IPv4 may-NAT eduroam-wep
 - JRS3: 802.1X WPA2/AES IPv6 no-NAT eduroam



JANET Roaming – 802.1X today

- Web Redirection methods are not secure, eduroam is built on 802.1X port level access control
- Current 'JRS Tiers' system:
 - JRS1: discontinued
 - JRS2: 802.1X WPA/TKIP IPv4 may-NAT eduroam
 - JRS3: 802.1X WPA2/AES IPv6 no-NAT eduroam
- 802.1X provides port-level access control to networks using client supplicant s/w, EAP and RADIUS transport
- EAP extensible authentication protocol – multiple authentication methods, utilisation of certificates



JANET Roaming – infrastructure

- What has JANET Roaming has put in place:
- Resilient infrastructure of 3 National RADIUS Proxy Servers (NRPS)
 - enables logon authentication requests to be communicated between organisations
 - located at Chilton, Bracknell and London
- Support team fronted by JANET Service Desk
 - backed by technical staff drawn from community
 - Provides advice on selection of RADIUS solution, how to implement Roaming and technical support if problems are encountered

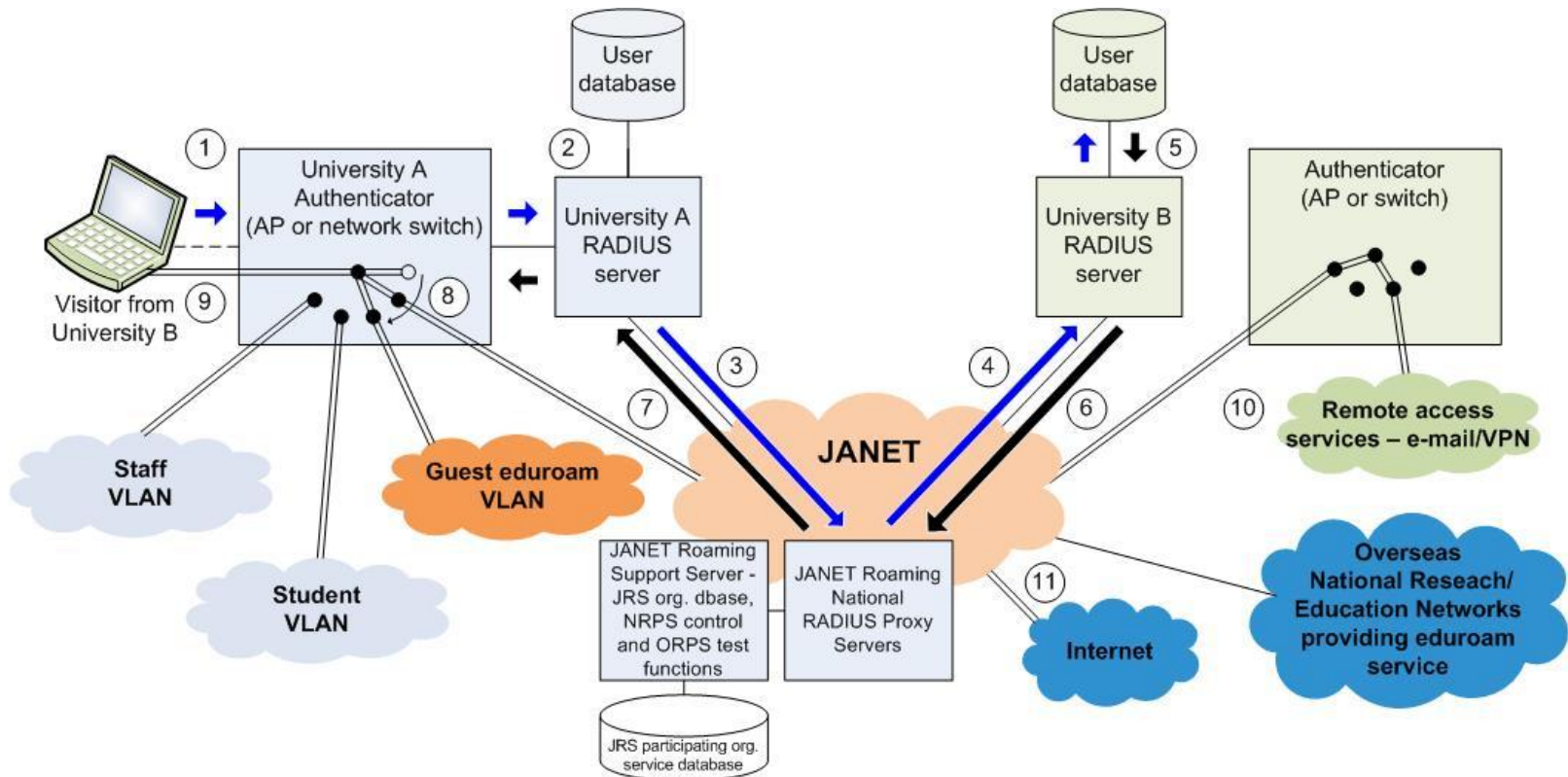


JANET Roaming – infrastructure

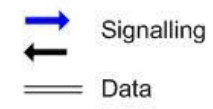
- Dedicated web front ended JRS Support server
 - enables participants to configure NRPS to peer with their RADIUS servers
- JANET Roaming area of JANET web site
 - structured to steer users, JRS administrators and general interest/decision makers to the relevant content as easily as possible
- Online documentation:
 - guidance on deploying, using and supporting the service, implementation guide, FAQs etc
- Training course:
 - JRS Fundamentals – aimed at IT Support staff engaged in supporting end users
 - Detailed RADIUS implementation course in pipeline
- Promotional material
 - Business case toolkit, case studies, eduroam awareness material



eduroam – how it works



- | | |
|--|--|
| <ol style="list-style-type: none"> 1. Visitor's supplicant s/w sends access-request to access authenticator 2. User not in local @universityA.ac.uk realm so... 3. Authentication request forwarded to JRS NRPS. 4. Request forwarded to Home institution. 5. User authenticated against Home userbase. 6. Access-accept returned to JRS NRPS. | <ol style="list-style-type: none"> 7. Access-accept forwarded to Visited organisation. 8. Network access authenticator connects visitor to eduroam network at Visited site. 9. Visitor gains access to guest's eduroam network and 10. to the remote access facilities provided by Home organisation and 11. the Internet |
|--|--|





JANET Roaming - implementation

- What is involved:
 - Participating organisation must deploy RADIUS server (FreeRADIUS, Radiator, Microsoft IAS/NPS, Cisco Secure ACS)
 - RADIUS server must communicate with back end user database (Active Directory, LDAP, NDS etc)
 - Organisational RADIUS server(s) peers with JANET National RADIUS servers (NRPS)
 - Laptops, mobile devices and wired PCs must be configured to use 802.1X authentication standard
 - Participants agree to federated trust model and trust each other to keep user databases up to date



RADIUS Platforms – March 2010

- FreeRADIUS 90
- Radiator 15
- Microsoft IAS/NPS 44
- Cisco Secure ACS 16
- Juniper Steel-Belted Radius 0



Supplicants

- Windows (native) XP, Vista, 7
- OpenSEA xsupplicant XP, Vista, linux
- SecureW2
- wpa_supplicant
- Intel PROSet
- Cisco Secure Services Client XP, Vista
(ex-Meetinghouse Aegis SecureConnect)
- Juniper Odyssey Access Client XP, Vista
(ex-Funk Software)
- Dell WiFi
- MacOSX (native)



JANET Roaming - development

- Current projects:
 - Monitoring utilisation at the NRPS – real time troubleshooting, analysis and statistics
 - Support of OpenSEA Xsuppliant development – added GUI for original xsuppliant, enhanced features and extended to cross-platform
 - Windows suppliant deployment tool (SU1X) to remotely auto-configure Windows and distribute certificates (Univ. of Swansea and Loughborough joint development)
 - GDP12 – 3D graphical representation of eduroam authentication events software
 - 802.1X SIG formed – experts forum to inform and investigate emerging issues in suppliant and 802.1X areas



JANET Roaming - joining

How Organisations Join JANET Roaming:

- Read and agree to
 - JANET Acceptable Use Policy
 - JANET Security Policy
 - JANET Roaming Policy
- Complete the application form and e-mail to service@ja.net
 - <http://www.ja.net/roaming/joining.html>
- Next step is to implement RADIUS server, peer to NRPS, create JRS service website and promote to your users



Questions?

www.ja.net/roaming

jrs@ja.net



The Vision

