FAQs for eduroam users

This page lists the most common frequently asked questions about eduroam in the UK. The table of contents summarises the questions asked; please scroll down to the relevant section for the answer.

Contents:

1) About eduroam

- When was the service launched?
- Popularity of eduroam, usage stats, where is it available
- Where can I use the service, how widely available is it?
- What is a 'Home' site / What is a 'Visited' site?
- Is eduroam safe?
- Common myths and misconceptions

2) Travelling abroad - eduroam

- How to find out status of eduroam service in visited country
- Does an organisation abroad I am visiting offer eduroam?

3) Joining eduroam / Realms / Eligibility

- Can individuals join eduroam?
- Can a person have an eduroam ID without host org joining eduroam?
- Is eduroam available to all members of an organisation?
- Do users need to have a network logon account? What about access for the public/non-registered users?
- Can my college/instution charge me for using eduroam?

4) Workstation/Laptop Setup/MS Vista issue

- Smart phone/handheld has stopped working since Nov 08
- Windows client 802.1X configuration
- Necessity of validating server certificate in supplicants
- Clearing the credentials cached by the XP supplicant
- Vista configuration for multiple WLAN encryption methods
- Vista eduroam problems
- Palm TX 802.1X

5) Web Redirect

- What is web redirect?
- Security issues with web redirect

6) User Authentication

- pGina - use for authentication of Windows client onto non-Windows network

End user queries

1) About eduroam

When was the Janet service launched?

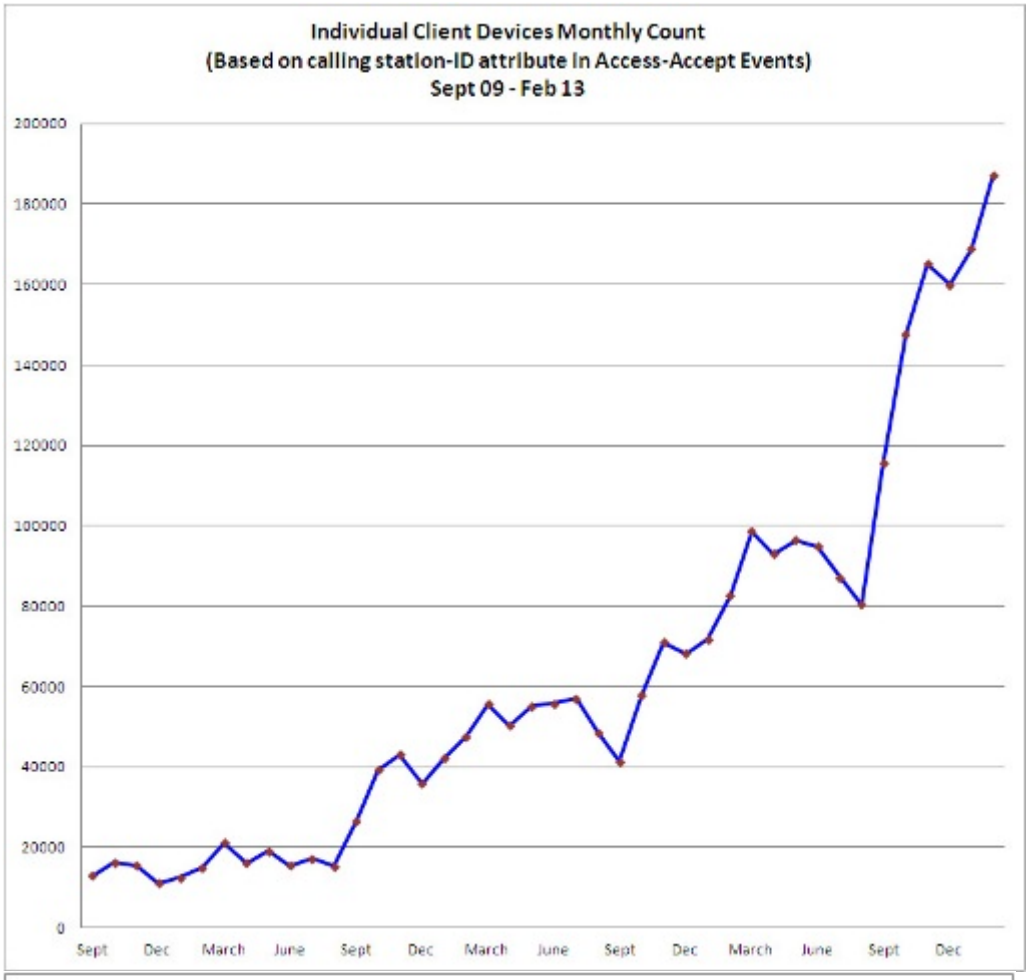
The eduroam service on Janet was launched on 2nd May 2006. This followed the LIN Trial which ran from August 2005 until December 2005 and the Service Pilot phase from 19th January 2006 to launch. Details of the LIN trial can be found at: www.webarchive.ja.net/development/aa/lin/archive/ [1]

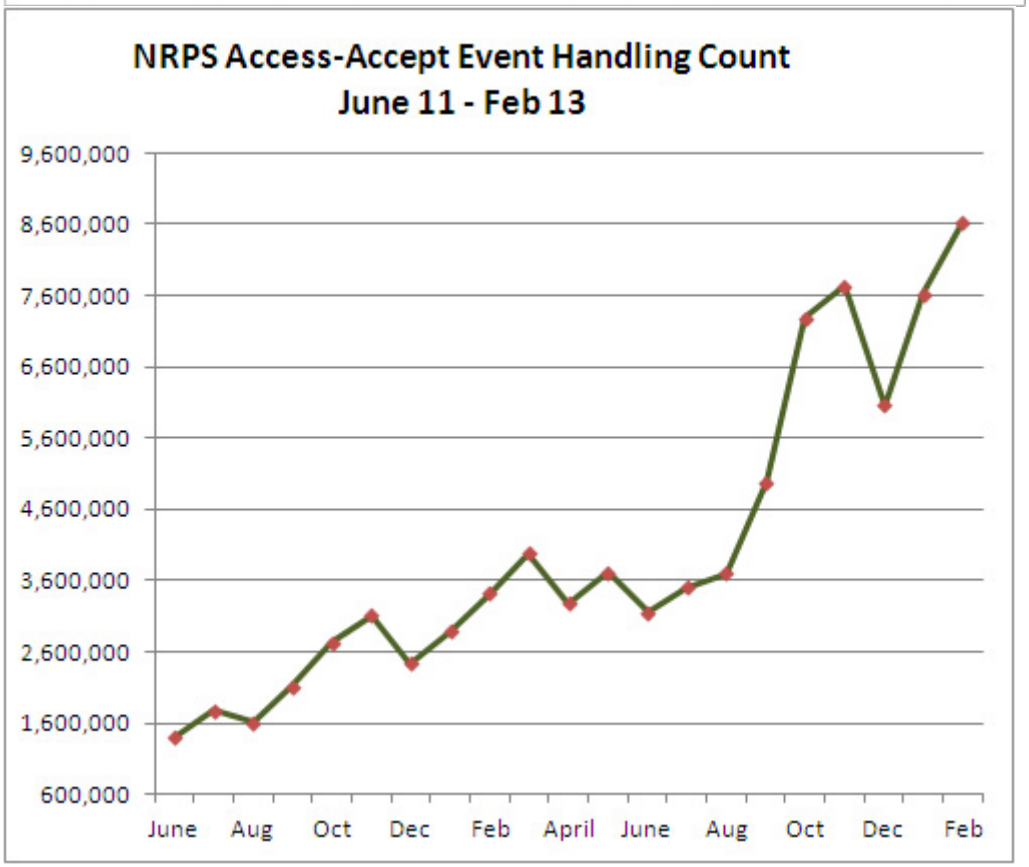
The original inception of the inter-NREN roaming project that has become eduroam was a proposal by SURFnet for test using 802.1X between two or three Geant partners in the TERENA Mobility group back in May 2002.

How popular is the service - have you got any usage figures?

Membership of the service has been steadily growing since launch and there are currently 216 registered eduroam UK participating organisations. This represents 34.3% of the total of the c.630 total of Janet-connected organisations, which is a healthy percentage considering the broad mix of Janet customers from HE to small specialist colleges (for many of which eduroam is not relevant).

Regarding usage, growth has been constant since the launch of the service. There was a threefold increase between May 2008 and March 2009 and there was a similar threefold increase over the preceeding eight months (Sept 07-May 08). Monthly measurements are based on a) successful authentication request events seen at the national proxy servers b) number of individual devices seen successfully authenticating at least once during each month. The following charts show usage growth over the past 18 months and 3 1/2 years respectively.


Individual Client Devices Monthly Count
(Based on calling station-ID attribute in Access-Accept Events)
Sept 09 - Feb 13
200000
180000
160000
140000
120000
100000
80000
60000
40000
20000
0
Sept
Dec
March
June
Sept
Dec
March
June
Sept
Dec
March
June
Sept
Dec


NRPS Access-Accept Event Handling Count
June 11 - Feb 13
9,600,000
8,600,000
7,600,000
6,600,000
5,600,000
4,600,000
3,600,000
2,600,000
1,600,000
600,000
June
Aug
Oct
Dec
Feb
April
June
Aug
Oct
Dec
Feb

What is a 'Home' site / What is a 'Visited' site?

Organisation may offer eduroam as a 'Home' and/or 'Visited' service. With a Home service, users can gain authentication at other eduroam sites they might visit (ie the Home site acts as an identity provider). Visited service sites provide an eduroam guest network that supports users visiting from organisations that provide a Home service. The idea of such a flexible approach is to be as inclusive as possible and to allow organisations to implement the type of service that suits their policies and local infrastructure/technical expertise.

Is eduroam safe to use?

eduroam is based on the most secure encryption and authentication standards in existence today. Its security by far exceeds typical commercial hotspots. Here's what our European partner says www.eduroam.org/eduroam-security/ [2]

Common misconceptions / myths about eduroam

1. eduroam only provides **wireless** network facilities for visiting guests

Not at all - the service is based on 802.1x technology which can be implemented using ordinary Ethernet LAN switches to provide eduroam guest network access JR45 outlets. In fact is it easier to implement hard-wired eduroam as you do not have the complications of wireless ciphers and AP setup to contend with.

2. eduroam is difficult for end-users working / configure laptops for

It is true that it is possible to implement a difficult system to setup/administer – e.g. if an EAP-TLS based solution is selected which requires the distribution of certificates for every machine. However the most commonly implemented systems (based on PEAP-MSCHAPv2 or EAP-TTLS/xxx) are NOT difficult to configure laptops/mobile devices for. There may be an unecessarily long series of mouse clicks involved with some wireless client software/supplicants, (eg. MS Windows) but many supplicants are in fact very straighforward to set up.

To help in this area Janet has been an active contributor to the OpenSEA Xsupplicant development project whose aim is to eliminate this problem and produce cross-platform, easy to configure 802.1x supplicant software.

The second area of potential difficulty is that since we cannot impose one standard WLAN solution on Janet customers, the various universities and colleges are free to implement their chosen WLAN wireless network authentication and data encryption methods. This is why we require all participating organisations to pubish the cipher settings on their web sites and why we will shortly be publishing this information directly on our eduroam locations map pages.

3. eduroam is an unreliable service

Not true at all - eduroam has a rock solid infrastructure and guest network reliability at participating sites is no more unreliable than any other network or WLAN. The problems arise when insufficient attention is paid to the minor s/w tweaks that may be required when roaming

from site to site.

Users should bear in mind that in the UK there are many and varied organisations and that they are independent. eduroam is a federated service and relies on the trust and co-operation of the participating organisations. It aims to support all the various different guest network implementations that the members have put in place (whilst adhering to the the eduroam technical specification).

This means that regarding wireless connectivity at UK sites (and the same applies in many other countries throughout eduroam), there is no one standard. In order to successfully connect to a network that is not your home WLAN you simply have to get the wireless network authentication and data encryption settings correct for the network you are visiting (and you've set your IP address and DNS server addresses to be obtained automatically using DHCP). You'll need admin rights on your machine to do this. Details of how to do this will be set out on the visited site's web pages.

4. eduroam is not widely available

There are now over 100 organisations in the UK participating in the service. The locations and availability of the service can be seen on the eduroam map pages [3].

2) Travelling at home and abroad

Where can I use the service: how widely available is it?

You can see where the organisations that have registered to participate in the eduroam service on Janet are in the UK at **http://www.ja.net/services/authentication-and-authorisation/janet-roaming/participating-organisations-map.html [3]**

I am travelling to an eduroam-participating country. How do I find out the status of the service provided by their NREN (local eduroam equivalent)?

The status of the NREN eduroam infrastructure is monitored at: http://monitor.eduroam.org/ [4]

The status of individual national RADIUS proxy servers is available at: http://monitor.eduroam.org/eduroam/mon_server.php [5]

To find the web site of the organisation overseas, you will be able to navigate to the country NREN eduroam site and from thence to their maps and links to the places you plan to visit, click:

- Europe: www.eduroam.org/index.php?p=europe [6]
- Asia Pacific: www.aarnet.edu.au/Content.aspx?p=137 [7]
- Canada: https://wiki.bc.net/atl-conf/display/CANEDUROAM/Canada+eduroam [8]

For a Google-maps powered zoomable map of Europe showing SSID and wireless encryption for each site see: http://monitor.eduroam.org/eduroam_map.php [9]

3) Joining eduroam / Realms

Can individuals join eduroam on Janet? Is there a way for an individual to obtain an eduroam ID without the user's home institution having to join eduroam?

No. Users must have registered network logon accounts at their home organisations and in order for individuals to use their credentials for authentication at eduroam participating sites, their home organisation has to join eduroam and install a RADIUS server which is peered with the national eduroam proxy servers.

The aim of eduroam is to reduce the amount of administration required both by organisations offering guest access to their networks and for visiting users. This is achieved by users being enabled to use their own usernames and passwords when roaming. Janet has set up the NRPS network and the support service to facilitate this through the eduroam mechanism. There is no facility for users to be issued with independent IDs since this would involve another tier of administration (and defeat the aim of the service).

Is eduroam available to all members of an organisation?

It is up to the organisation to decide which of its members it wishes to provide eduroam service for. To enable users to connect via eduroam. the organisation has to implement a Home service, which means that it acts an identity provider and authenticates the user against its network access database. Such databases typically allow users to be put into groups or otherwise categorised for administrative/mamagement of access to networked resources purposes. Whilst most organisations enable eduroam access for all users, your organisation may restirict this to certain groups or individuals.

The eduroam networks that users are able to connect to include (usually) an eduroam network at the home site and all networks advertised with the 'eduroam' SSID. These are to be found at most universities in Europe and at many research organisations, FE colleges, hospitals, commercial sites, transport providers, libraries, museums and municipal authority street areas. So, eduroam is available over a huge area. The second important characteristic is that eduroam networks are at present generally offered without any content filtering, although such filtering is permitted within the technical specification. Organisations with a duty of care to their members, for example schools and insitutions catering for vulnerable adults, may (or may not) decide on a policy of only permitting network access onto networks on which content is filtered. Since eduroam networks are usually not filtered, such organisations may decide to restrict eduroam access to only certain of their members.

Can my college/institution charge me for using eduroam?

eduroam is a 'free' service globally to members of academic institutions ***when they are roaming away from their home institution***, but the institutions are at liberty to make a charge to their own users for provision of network accounts and use of institution-provided facilities such as Wi-Fi. Most organisations bundle the costs of network access account provision and Internet access (which apply to eduroam) in with their accommodation or tuition

fees.

So, yes your institution may make a charge for setting up your network access account (which is essential for eduroam authentication) and they may make an ongoing charge for acting as an identity authenticator for use with eduroam. The institution might structure charging to be free to sign up but only start charging after use of a certain data threshold per quarter on its own Wi-Fi service. This is only likely to be encountered in collegiate environments where the college pays a central university computing services dept for fibre inter-connection and Internet services.

Whilst your college may make a charge for the eduroam Wi-Fi service while you are on/around the college site, they must not charge for you to use eduroam services elsewhere throughout your university or at other eduroam member organisations. eduroam(UK) policy is that eduroam must be free at the point of use and free to use by *visiting* eduroam users.

Visitors to your institution must be able to access eduroam without being charged and so you in turn will be able to access eduroam away from your local instituition/college.

4) Workstation/Laptop/Palmtop Setup

My smart phone/handheld device was working perfectly well with eduroam before 6th Nov '08 but now it doesn't - what's happened and how can I get it working again?

We have recently tightened up the NRPS realm handling behaviour so that now realm checking is more rigorous. Incorrectly formatted realms with spurious extensions are now not forwarded, which means that some devices that previously worked with eduroam now no longer do so.

Check your realm settings on the device - it is likely that you have incorrectly configured EAP settings and the device may be trying to use the certificate as the realm. It is possible that you may have put your userid@myorg.ac.uk [10] as your user in use id (it shoud be simply 'userid') and not configured the realm as specified, (it may read 'From certificate', which is wrong). Consult your IT dept for details about how to configure the settings correctly.

How do I configure Windows to work with 802.1X?

Details of all aspects of setting up the client and using eduroam are included in the eduroam user guide. However the following extract details setup of the client in Windows XP.

- 802.1X supplicant configuration for Windows XP

To make life easier I want to uncheck the 'Validate Server Certificate' in my XP client - what's wrong with doing that?

You should *ALWAYS* validate the server certificate - the option in the supplicant (be it Windows native, SecureW2, OpenSEA et al) should always be enabled. Certification is one of the main securing blocks of EAP, which underpins the eduroam service.

If you don't verify that the RADIUS server (which is handling your sensitive authentication credentials) is legitimate and not being spoofed by an unscrupulous person, you are leaving

yourself open to having your credentials stolen. Maintaining the security of your credentials is one of the requirements of the eduroam usage policy that you subscribe to as part of using the service - ie. it is mandatory.

How can I clear the username that the Windows (XP etc) supplicant appears to cache?

The issue is that when using the XP built-in supplicant, after successful authentication the credentials are cached and you are not prompted again for a username and password. If a different user wishes to use that machine, the problem arises that the username and password are wrong and can't be changed. You may also experience difficulties after a routine network password change.

What you need to do is to clear out the EAPOL key so that you are prompted for username/password again. This can be done by using regedit. The alternative is to delete the profile/'forget' it and reconfigure the settings preferrably by reloading your automated setup tool installer (CAT, SU1X, XpressConnect, Secure W2).

I visit organisations that use different WLAN encryption methods (WPA2/AES and WPA/TKIP [at a far flung location]). How can I configure Vista to make it easy to connect to SSID 'eduroam' for both - without having to manually change the protocol settings each time?

Using the netsh command, which allows us to manage wireless connection profiles as editable .xml files, it is possible to create two working Vista profiles - one for WPA/TKIP, the other for WPA2/AES.

The same result can also be achieved by simply using the standard Vista wireless manager - you just create two profiles, one for each method. However since Vista automatically attempts to name the profile using the SSID - which in this context will be 'eduroam' - you will not be able to add the second different profile with the same name.

So firstly set up a WLAN profile for eduroam using WPA/TKIP. The trick now is to rename this first eduroam profile, as say eduroam-tkip, so that the second profile can be added (and then renamed to say eduraom-aes). To rename a profile go to "managing wireless networks", choose eduroam, press F2 and rename the profile to eduroam-tkip. This changes the name of the profile, but not the SSID. Next you manually add the second eduroam profile, configuring it for WPA2/AES and then rename the profile to say eduroam-aes.

If you have two profiles, Vista will display both SSIDs when it sees an eduroam WLAN, but if the particular eduroam network only supports one cipher, one of the networks will be shown as unavailable. Of course both profiles can be marked as automatic and then one of them will be used, depending on the particular situation.

[If you do this for either TLS or TTLS/SecureW2, then connection to the second profile is automatic. However with PEAP you will be asked for credentials for the second time (only once, of course)].

The above applies to Vista only - not Windows XP.

Why am I having a problem using eduroam with MS Vista?

Windows Vista has a slightly different PEAP authentication to that of WinXP. This difference means that Vista 802.1X authentication will not work with older versions of Cisco ACS, RADIATOR or FreeRADIUS ORPS software at Home organisations.

Updated versions the most popular RADIUS servers have been released which fix this problem:

FreeRADIUS 1.1.4* - tested (1.1.7 was the last 1.1.x release. Latest version is now 2.1.3)
RADIATOR 3.16 - tested
Cisco ACS 4.1 - not tested (would like feedback from sites using this)

As this issue is only at the authentication end, visitors with Vista should happily be able to use eduroam at a Visited site if their Home site has upgraded their ORPS.

*Vista will work with 1.1.4 but 1.1.5 and 1.1.6 had further SSL fixes to improve/fix SSL behaviour and stability in general (as well as more than 30 other bug fixes). A 1.1.6 system would be far better than 1.1.4 and the final release of 1.1.x was 1.1.7 and is the one to use IF you must use 1.1.x. We see no reason not to go for a later 2.1.x version though. 2.1.3 is the latest release and fixes many 1.1.x issues and includes amongst other features a much enchanced stats monitoring system.

How can I get my Palm TX handheld to work with eduroam?

Palmtops need 802.1X supplicant software to work at the vast majority of eduroam sites (excepting those providing web redirect authentication JRS1) - the supplicant software must support the authentication protocols in use on your home network (EAP-TLS, EAP-TTLS, EAP-PEAP(v0 or v1)). The Palm TX uses Palm OS Garnet 5.4 which supports wireless connection, but unlike XP and Vista does not include an 802.1X supplicant. This software is however available in the Wi-Fi Enterprise Security Update (ESU) package which costs $5.99 from http://kb.hpwebos.com/wps/portal/kb/common/article/47493_en.htm [11].

5) Web Redirect

What is Web Redirect?

'Web redirect' or 'captive portal' is the system currently used in many Internet cafes and commercial wireless hotspots. However it has serious security weaknesses and Janet advises against its use. Captive portal works as follows; when a user starts their web browser, the request is intercepted and forwarded to a redirect server which usually presents the user with either a login page for authentication/payment or to an information page for the user to read/agree to conditions of use. This is simple and straightforward to use, but there are serious security flaws and the user is vulnerable to a number of attacks as detailed below.

In the academic community many early adopters of distributed authentication for network access chose to present a web-based authentication interface, typically on a guest wireless

LAN. The approach has been to intercept web traffic from the client, either by policy-based routing, DNS or HTTP manipulation, and redirect it to a web proxy. This then presents a login screen in place of the requested web pages until such time as a successful authentication has been accomplished, after which it acts as a transparent pass-through for the length of the session. Some organisations have elected to offer a web-only guest service; others used dynamic firewall rules on the proxy device to open up a wider range of protocols to the authenticated visitor. Many commercial wireless ISPs follow this strategy for user authentication, since it is intuitive and effectively self-documenting.

A number of manufacturers have introduced products implementing this model, among which Bluesocket and Vernier have attained significant market share in the higher and further education arena.

The eduroam service on Janet in the UK accommodated legacy web-redirection network access services within the old JRS1 tier for an initial period following launch of the service. WRD is now not permitted and JRS1 has been withdrawn as of 1st May 2009 for a number of reasons as follows:

- entered credentials are visible at the NAS (Network Access Server) and any intervening RADIUS servers
- subsequent data communications are not secured in any way unless additional measures are taken, such as VPN
- IP/MAC spoofing may allow trivial session hijack
- they are potentially vulnerable to the so-called ‘evil twin’ attack, whereby an attacker creates a ‘clone’ of an authorised login screen on a rogue access server in order to harvest credentials
- proxying may break some web applications.

Historical note: where web redirect systems were used in an eduroam context, for example as an adaptation of an existing standalone guest service, a number of conditions had to be met - in particular, it was required that the interface had to support SSL or TLS security based on a certificate acquired from ‘a well-known’ certificate provider. This improved security by ensuring that all WRD NASs used a certificate to identify themselves to the visitors' web browsers. These provisions did not entirely eliminate the concerns set out above (which focus on credential protection), and tier JRS1 services were considered to provide only low security contexts in which it was recommended that additional data privacy measures, such as VPN, were adopted.

The JRS1 web redirect option has always been deprecated has now been withdrawn. Organisations wishing to provide a guest infrastructure are strongly encouraged to develop an 802.1X infrastructure and to implement an eduroam service according to the eduroamUK) Technical Specification.

For further information please see:

http://www.terena.nl/activities/tf-mobility/deliverables/delF/DelF-f.pdf [12]

What are the security issues with web redirect?

WRD is widely deployed within many organisations, and is also supported by all visitor clients possessing a web browser. However, WRD has some significant limitations.

Firstly, because the visitor provides a user name and password to the WRD NAS, these credentials are visible to the NAS and any intervening RADIUS servers involved in forwarding the credentials.

Secondly, it does not provide data privacy for subsequent communications over the wireless LAN.

Thirdly, it is relatively trivial for an unauthenticated attacker to abuse the network in a non-traceable fashion. For example, an unauthenticated attacker can easily spoof the IP and MAC addresses of an authenticated user, and masquerade as that user.

Finally, WRD is vulnerable to the so-called ‘evil twin’ attack, whereby an attacker creates a ‘clone’ of an authorised WRD NAS. Users are easily tricked into entering their credentials into the ‘clone’ because it looks identical to the authorised NAS. This vulnerability is the reason that the JRS tier 1 requires all WRD NASs to use a certificate from a well-known certificate authority to identify themselves to visitors' web browsers.

In the light of these limitations, we have always strongly recommend against its deployment for eduroam and WRD is now not permitted. (Organisations may still offer their own WRD systems for use by their own users and visitors, but they are not permitted to advertise them with 'eduroam', use the 'eduroam' SSID nor connect them to the eduroam service).

6) User Authentication

I've heard of pGina, can it be used to enable authentication for a Windows machine into a non-Windows network?

As standard, the Microsoft Windows NT/2000/XP client operating system only provides for a single method of user authentication - via a Microsoft Windows Server. Should you wish to use a user database on a non-Windows server to authenticate access for Windows machines, eg. an existing Unix server and its existing base of users, there are a few non-ideal options - eg. use a Windows server for authentication and maintain identical lists of usernames/passwords on each server or use Samba to emulate a Windows NT 4 Server.

The pGina project however has developed a replacement for the authentication portion of the Windows 2000/XP OS. This has created a wide choice of many different methods for the authentication and login of a user. It has been achieved through the creation of a substitute for Microsoft's replaceable GINA (Graphical Identification aNd Authentication) dynamic link library DLL component that is loaded by the Winlogon executable. The pGINA can dynamically load “plugins', where a plugin can be created to use ANY method of authentication. For further information see: What is pGina? [13]

Links
[1] http://www.webarchive.ja.net/development/aa/lin/archive/

[2] https://www.eduroam.org/eduroam-security/
[3] http://www.ja.net/services/authentication-and-authorisation/janet-roaming/participating-organisations-map.html
[4] http://monitor.eduroam.org/
[5] http://monitor.eduroam.org/eduroam/mon_server.php
[6] http://www.eduroam.org/index.php?p=europe
[7] http://www.aarnet.edu.au/Content.aspx?p=137
[8] https://wiki.bc.net/atl-conf/display/Services/Canada+eduroam
[9] http://monitor.eduroam.org/eduroam_map.php?kml=europe_capital
[10] mailto:userid@realm.ac.uk
[11] http://kb.hpwebos.com/wps/portal/kb/common/article/47493_en.htm
[12] http://www.terena.nl/activities/tf-mobility/deliverables/delF/DelF-f.pdf
[13] http://www.pgina.org/?page_id=3