FAQs for Business Management and General Interest

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) Policy

Must all our users be authenticated and allowed onto our eduroam/other Janet-connected network(s)?

It's a common myth, but not true: Janet Policies don't require you to authenticate everyone. The actual requirement is clause 9 of the Janet Security Policy https://community.jisc.ac.uk/library/janet-policies/security-policy [1]. However this can most easily be met by ensuring that only authenticated users are permitted connection to the

network. Most Janet-connected organisations have adopted this approach. In this context, edroam provides the perfect solution for providing guest network access for the majority of visitors (although provision should also be made for visitors from non-eduroam enabled organisations).

More detail of circumstances where unauthenticated access may be appropriate is in the factsheet on User **Authentication https://community.jisc.ac.uk/library/janet-policies/user-authentication** [2]

2) Business Case Objections

We already provide free public Wi-Fi, don't see the case for eduroam?

Review your free public Wi-Fi provision:

'Free Wi-Fi' for visiting members of the public is generally offered as an open service not requiring any access key (PSK code, username/password/certificate) and the Wi-Fi radio traffic is not encrypted. This makes for easy straightforward access to the service for all users and all devices. Whilst this may seem to be advantageous it is totally insecure and exposes users to a number of potential risks as detailed below.

But firstly, let's review how you are providing the 'public' Wi-Fi service and who you are it to. The means of internet connectivity is critical - any guest access solution that routes user traffic through a Janet connection needs to comply with Janet connection policy. This means that only visitors who are members of the eduroam community or who are on campus due to the organisation's education/research/cultural engagement mission or are visting on matters of business/service provision should be provided with internet access through Janet. Walk-on passers-by / visitors to on-campus cafes etc should only be connected through a separate non-Janet internet feed or through Janet via VPN tunnelled ISP service.

For a non-eduroam guest access solution using a separate inernet feed, the organisation would need to look at i) commercial WISP solutions such as BTWiFi, The Cloud, etc ii) bolt-on vendor captive portal (or open) solutions iii) guest service solutions that are built in to some vendors' Wi-Fi management systems.

Let's look at open access systems which do require a key or some registration - 'open' systems may be implemented with a captive portal that (in it's least intrusive form) presents a 'splash page' to the user that can be dismissed by clicking on a erms and condition box, but more often these require the user to register the first time they use the service and on subsequent usage enter their registered username (although some services remember the user such that future log in is automtatic). Where registration is necessary, the user may be required to provide a lot of private data (name, date of birth, e-mail address, mobile number, favourite pet name etc). Free services may also be provided with time restrictions, eg first 30 minutes free, then chargeable thereafter. This is all time consuming, inconvenient and represents a security risk.

One alternative to open Wi-Fi services (no wireless encryption - traffic interceptable) and captive portal (vulnerable to spoofing/interception) is WPA2/AES pre-shared key access code secured services. Since a static code is utilised these systems are still vulnerable - codes can become known to hostile parties and encrypted traffic deciphered.

The above is all pretty concerning, but the good news it that there is an alternative service which is free and which does not have these drawbacks - eduroam. (Although admittedly this is limited to the research and academic community...numbered at c. 6.3 millions just in the UK!)

The security/privacy risks with open Wi-Fi services are:

Unencrypted Wi-Fi means data traffic can be eavesdropped on with ease. Anything sent in plain text can be read - so an attacker could harvest usernames, passwords and authentiation cookies together with any content that is transmitted.

Insecure/rogue AP. An attaker can easily set up a 'honeypot' AP to provide a spoofed SSID with an open service to which users connect. The attacker forwards packets from the user onwards to the legitimate Wi-Fi service/the internet, so can easily eavedrop the user's communication or indeed intercept and alter it to trick the user into providing confidential information or replacing legitimate downloads with malware.

All clients on same flat unmanaged network with no protection. With all clients, no matter what their state of patching/AV, being all on the same network, one compromised client can easily be used to attack all others in that network space.

Insecure DNS. Anyone connected to an open network can spoof traffic and generate fake DNS answers to redirect your traffic through them. You trust the site you think you have connected to and the attacker harvests everything you enter.

Captive portal security/privacy risks:

A captive portal can easily be spoofed and traffic redirect through the impostor - leading to the same exposure as for the rogue AP above. Users trust the fake captive portal, enter their personal details or go on to use social medial, internet banking services etc providing the attacker with a rich harvest of information (albeit that a savvy user can attempt to utilise TLS/HTTPS or SSH or VPN to mitigate the risk).

Further considerations:

In addition to the above, the organisation providing the service has no meaningful record of who connected to and used the network, so cannot follow up on or assist authorities in cases of abuse of the service.

Also, if the organisation uses a commercial operator to provide a free Wi-Fi service, in addition to Wi-Fi kit charges and internet circuit costs, the commercial operator usually makes a charge based on number of user connections/bandwidth/usage.

In sharp contrast to the above, eduroam services, being based on 802.1X and WPA2/AES are secure.

eduroam security, privacy and convenience advantages:

1) Security - WPA2/AES, 802.1X, only authenticated users/devices on network you are connecting to

2) Privacy - no logging in, entering details into a web page, minimal risk of traffic interception

3) Audit trail for organisation providing the service - log of user, time, IP address

4) Convenience - just turn on Wi-Fi and be online. No logging in, entering details into a web page, no time restrictions

5) Better partnerships - different users can be put onto different local network (via 802.1X and prearranged trust agreements)

6) Works worldwide - eduroam isn't just in UK or even just in Europe, it's worldwide.

7) Free. eduroam is free, not just for the users but also for the organisation providing the service - assuming that the organisation already operates its own Wi-Fi network with internet feed, since there are no user connections/bandwidth/usage charges.

Our users don't roam, the benefit of global Wi-Fi roaming is not important to us

Jisc regards eduroam as an exemplar of best practice Wi-Fi service since it is based on the 802.1X standard. 802.1X/eduroam requires WPA2/AES Enterprise security which is the best Wi-Fi authorisation and encryption standard. This is much better than open networks, captive portal and pre-shared key which all have vulnerabilities.

In addition to the best security, 802.1X/eduroam provides for network provision and management efficiency by enabling the number of SSIDs to be reduced to a minimum through dynamic VLAN assignment. The main SSID (‘eduroam’), with suitable network infrastructure configuration, can be used to provide access to multiple network VLAN services that used to be provided through multiple individual SSIDs.

The ideal deployment should comprise i) one main SSID (‘eduroam’) supporting WPA2/AES (Enterprise) security (and WPA3 as it rolls out) and a few additional SSIDs for ii) e.g. setup or devices/remediation, iii) if needed a guest service for non-eduroam visitors, iv) if needed a non-802.1X service for gaming/other devices (mainly applicable in halls of residence).

The benefits of limiting the number of SSIDs are: i) simplification of the Wi-Fi service ii) reduced user confusion iii) improved Wi-Fi efficiency and performance.

If the above were not enough, eduroam of course provides a global Wi-Fi roaming service for the organisation’s own staff and students. This is seamless and needs no user interaction when logging in wherever the eduroam SSID is detected. No username to be entered (if credentials are cached), no registration on a captive portal web page, no PSK code to be entered. The user simply ‘opens the laptop and is connected’. Equally, eduroam enables the organisation to provide a hassle-free guest Wi-Fi access for visitors from eduroam member organisations.

3) Schools Participation

Are schools eligible to participate in eduroam(UK)?

Organisations participating in the eduroam(UK) federation typically have between 4,000 and 40,000 members although there are smaller organisations and special categories of

organisation providing Visited-only services. Schools are clearly part of the Janet community and we would like to be able to welcome them to the eduroam service.

There is however a scalability issue with schools' participation since there are so many in the UK whilst individually schools have relatively few members. Current (March 2016) membership of eduroam(UK) is 380, whereas there are approx. 3,940 maintained secondary schools in the UK. In England there are some 150 local education authorities, which is a far more managable number. Therefore we would be happy for **groups** of schools (ideally at LEA level) to participate such that authentication requests can be aggregated to be channelled via a single RADIUS peer system. We would be happy to discuss approaches by schools or organisations representing schools. In technical terms, a viable scenario for participation would be where a number of schools' Wi-Fi networks are all managed through a centralized controller cluster linked to a central RADIUS system and central user database.

There is a further consideration regarding schools participation. eduroam is widely available and provides connection to the Internet at most universities in Europe and at many FE colleges, sixth form colleges, hospitals, research organisations, commercial sites, transport providers, libraries, museums and municipal authority street areas, so the service can provide connectivity at a large number of relevant locations. However, an important characteristic of eduroam 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 institutions 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 (e.g. teachers and staff). This is a policy decision that the schools need to take. (One option might be to only enable eduroam for pupils who have their parents permission to be granted access to unfiltered eduroam). (Nb. There are potential technical solutions that might be devised to resolve the issue, but there is nothing in the pipeline at present).

At the Home school site eduroam-enabled pupils may be connected to local network services which may be content filtered, if such is the school policy. The local-user-only network may provide access to in-house resources such as an intranet, local file stores and printing. It is only visitors who must be connected to eduroam-compliant internet-connected network services.

There are technical solutions which could be considered for pupils when they are away from the home school network environment and connect to (unfiltered) eduroam services at other sites. A school might want to look at technology to mitigate any duty of care worries - for example, a school could provide managed devices and only support certificate-based authentication methods. By pushing profiles/configuration via MDM systems such that all web browsing went through proxies that the school managed or controlled, the web browsing would be like it was at the 'home' site. This could be done with VPN technology so ALL internet traffic was sent back through the school's systems. Thus, no matter where pupils roamed using such managed devices, the school would be able to enforce its IT policies in this regard. (The more common password-based authentication methods are transferrable from device to device so the proficient user can set up any of their devices to work with eduroam manually.)

Nb. eduroam can be deployed simply as a service for visitors, without enabling a school's own

users to gain access to eduroam services off-campus. This is technically quite straightforward to accomplish and would benefit visiting IT support staff (e.g. from the local authority), academics and teacher training students from eduroam-enabled institutions.

Without wishing to discourage schools participation, the following may be useful reading: Managing Safety for Children and Vulnerable Guests in HE https://community.jisc.ac.uk/library/janet-policies/managing-safety-children-and-vulnerable-guests-he [3]

4) Local Authorities Participation

Are local authorities eligible to join eduroam(UK)?

The answer is a qualified 'yes'.

Jisc eligibility now extends quite broadly to include the public sector as well as research, education, health and cultural sectors. Whilst Jisc is the UK national eduroam federation operator and has the autonomy to determine the community we serve, we are members an international family of eduroam national federation operators which has members drawn from many different countries - including some in which access to the national education and research network is more restrictive than in the UK. As the UK eduroam federation operator and a member of the European Confederation we have to be sensitive to those concerns.

The good news is that local authorities, as members of the community served by Jisc, are indeed eligible to participate in eduroam - subject to certain conditions. Moreover we now have an equivalent service, 'govroam [4]', specifically for the public sector, local and central government, NHS, emergency and social services, that is based on the same technology amd uses the same implementation model as eduroam. In parallel with this a trial development of the eduroam service has been investigated on the Kent Public Sector Network which aimed to enable an wider participation in eduroam for LA staff.

What are the qualifications that apply to local authority participation; what types of users may benefit?

Schools, public libraries, museums and other learning centres feature among the services that local authorities provide. In addition to being directly involved in the delivery of these services, council staff are often involved in providing support (e.g. IT services and library administration) for these services. Councils may also be involved in joint research initiatives with universities and colleges. In line with our objective of expanding participation in eduroam, Jisc would like eduroam to be adopted by local authorities to support users engaged in the above activities. Enabling such users to utilise eduroam would be of benefit to those sectors and eduroam service availability in schools, learning centres, libraries and museums would clearly be of benefit to the wider eduroam community. We are therefore keen to encourage local authorities to participate in eduroam.

What are the different ways that local authorities can participate?

Visited-only: It is worth remembering that eduroam can be implemented simply as a Wi-Fi service to enable visiting users to connect to the Internet (usually via Janet). The business case for this would be, by providing seamless network access, to help i) teaching staff visiting from other sites, ii) students, researchers and other eduroam users maintain low cost Internet

connectivity when away from their home organisations, iii) staff engaged in supporting research and learning activities; i.e. provision of guest network services to a large part of the Janet community with the minimum of guest account administration workload.

Home: For a participating organisation to enable its own users to connect via eduroam networks elsewhere, Home (identity provider/IdP) eduroam services need to be implemented. eduroam(UK) policy permits organisations to tailor their systems to limit eduroam authentication to certain categories of their user base if they wish to (e.g. usage could be limited just to students over 18 years, or members of teaching staff). Of course most current eduroam organisations provide eduroam for all their users. For local authorities, eduroam authenitcation must be restricted to members of staff/visitors engaged in education, research, training or support of those activities.

The business case for provision of eduroam to as wide a range as possible of your members, subject to the above restrictions, is simple. Your members benefit through easy to access Wi-Fi network service, authenticated, secure, free of charge, using a single profile. From the organisation's perspective, eduroam results better effectiveness of your members: improved communication, productivity (through access to online resources) and satisfaction (people enjoy Internet access!), and you also benefit from eduroam's inbuilt security, network environment tailoring capability and you have an audit trail of your users connections.

'Umbrella'/Regional hub/collegiate member: It is fairly common practice in the academic world for one organisation to serve as an 'umbrella' member of eduroam to provide a link into the national eduroam(UK) service for a number of small collegiate participants. The umbrella member may or may not provide IT services to the downstream colleges/faculties, and historically the smaller entities would manage their own user directories (e.g. ADs) although there is a trend towards larger centrally managed directory services. Similarly, the smaller entities may or may not operate their own RADIUS services that would be peered with the umbrella organisation's RADIUS Proxy Servers (ORPS) - those are the servers registered with eduroam(UK) and which support roaming authentication traffic for the organisation's top level realm (e.g. camford.ac.uk) as well as visitor auth traffic.

Local authorities/Grids for Learning may act as umbrella members of eduroam(UK) and may serve as regional hubs for downstream RADIUS servers. **Registraton:** only the top level organisation will be registered with eduroam(UK); we will have no visibility of downstream organisations. **Duties, responsibilities and obligations:** the top level organisation will represent the service provided at all downstream entities and should ensure that any agreements with them include back-to-back conditions of membership of eduroam(UK). The top level organisation will be considered by eduroam(UK) as a standard member organisation and there are no specific conditions or concessions that are applicable.

RADIUS servers: only the top organisation's ORPS will be known to eduroam(UK). The realms that are required for use in usernames by the downstream entities will need to be registered with eduroam(UK) by the umbrella organisation and therefore either the hub organisation will need to own the DNS names or must be duly authorised by the downstream entities to register the realms with eduroam(UK).

So local authorities are welcome and encouraged to provide Visited eduroam services and also may provide Home services provided that (at present) user access is restricted as described above. Note that Jisc offers a sister product to eduroam which is specifically

tailored to the needs of local authorities and the broad public sector - Govroam https://www.jisc.ac.uk/govroam [4] Govroam is technically very similar to eduroam but is a completely separate service, catering to a different stakeholder base. All members of a local authority, government or public sector entity may be enabled to use govroam without restriction - but conversely eduroam users cannot connect to govroam services.

City Centre Public Spaces, Superconnected Cities and eduroam

In line with our objective of expanding the footprint of eduroam Wi-Fi service availability, eduroam(UK) is very keen to support initiatives to provide eduroam in parallel with public Wi-Fi services in city centre public spaces and public buildings. A dedicated Community web page is being developed in the eduroam Group area to inform this activity.

5) NHS Participation

How can NHS Healthcare Trusts participate in eduroam?

Janet eligibility now extends quite broadly to include education, health and public sector organisations, however there are technical considerations that must be addressed and policy issues which may limit the extent of NHS Trusts' participation.

The technical issues that must be considered apply to NHS Trusts whose Internet service is provided through the NHS N3 network. Organisations with independent, non-N3 based feeds do not face these challenges.

From a technical perspective, there are in theory three main approaches to NHS Trust participation in eduroam:

1. Full service member (Visited and optionally Home) - using the existing N3 network and Janet gateway - the most obvious solution, but not currently viable!
2. Full service member (Visited and optionally Home) - using an independent Internet feed
3. Visited-only - in association with a local university, extending the university's eduroam service by adopting one of three options

Firstly, let's get the bad news out of the way so that we can explore the viable solutions (2) and (3).

Participation as a full member of eduroam(UK) using the N3 network and N3-JANET gateway

Trusts whose Internet feed is provided only via the N3 network face a number of problems. A major problem is that private IP addresses are utilised throughout N3, so in order to access the Internet, network address translation (NAT) is employed at the boundaries, including the N3 - Janet gateway. Full Visited and Home eduroam service participation requires that RADIUS communications can be initiated from both a Trust's Organisational RADIUS Proxy server (ORPS) and the Janet National RADIUS Proxy Servers (NRPS). The eduroam(UK) national infrastructure was designed to work with uniquely identifiable (trusted) and uniquely addressable organisational RADIUS servers (not least because all exchanges in a single hop RADIUS conversation between two sites must go via a single RADIUS server pair) and so all client ORPS addresses are held in the NRPS client lists. Even a Visited-only service ORPS must have a unique IP address since the NRPS only accept RADIUS communication from trusted ORPS.

In order to permit N3 based OPRS to work with the Janet-based NRPS specific NATing would have to be employed at the N3 gateway. A Trust's ORPS NATed public address would have to be fixed and a fixed mapping to that Trust's ORPS would have to be permanently maintained (port address translation would not be employable because the NRPS requires UDP on port 1812 for RADIUS). The N3 gateway comprises a primary and a backup pool each of a /29 IP addresses, i.e. 8 addresses in each pool. This does not provide much scope for supporting more than a handful of Trusts.

Another factor is that the IP addresses of the ORPS in the NRPS clients list are derived from DNS-resolvable fully qualified domain names (FQDNs). This provides a number of benefits, including facilitating server IP address changes and reducing the risk of typo errors when entering IP addresses in the Support portal. This does however mean that any fixed NATing on the N3 gateway would require the address to be configured in DNS, adding an additional complexity.

So, whilst in theory it would be possible to support Home and Visited participation of Trusts via the N3-JANET gateway, fixed NATing for Trust ORPSs is not a provided facility, without fixed NATing, the IP address of any N3-based ORPS cannot be looked up via DNS by the NRPS and so cannot be added to the NRPS RADIUS clients tables and so at present NHS Trust direct membership participation using the N3 network is not available. (A possible future solution would be to incorporate a top level N3 RADIUS Proxy Server that would be peered with the NRPS through the N3-JANET gateway. NHS Trusts would be able to peer their ORPS with that N3 RPS and so be able to participate on an equal footing).

There is a further major issue. N3 Security Policy at present only permits 'sessions' to be initiated from the N3 side of the gateway. The limitation to session-initiation only from N3 policy raises a second hurdle for a Trust wanting to participate as a Home service (IdP) provider. Authentication requests from NHS users roaming to Janet-connected sites would be blocked at the gateway since such users would need authentication requests from the organisations they were visiting to be sent from Janet into N3. This would not however prevent an NHS Trust organisation from providing a Visited service (although of course the NAT issue prevents this). There is a further issue in that for heartbeat test and monitoring of basic network connectivity the NRPS and Support servers carry out ICMP echo tests which will be blocked at the N3 gateway.

Participation as a full member of eduroam(UK) using an independent Internet feed

So, the good news...In approach (2) the participating organisation can deploy its ORPS and link to the NRPSs via the Intenet. It is however recognised that a separate non-N3 Internet feed may not be cost-effective just to support eduroam, but if such a feed is already available then this is an immediately available option. It also means that the current general 100Mbps bandwidth of N3 connections will not be loaded with eduroam authentication traffic (minimal load) nor eduroam visitor data traffic (which may be significant depending on number of visitors and their activities!)

Approach (2) would be for the Trust to participate as a full member of eduroam(UK) with a non-N3 Internet feed. This would require the deployment of a RADIUS server and peering with the Janet national proxies and connection of the Trust's eduroam network to the independent Internet feed. The RADIUS server would need to have a publicly accessible IP address which must be resolvable through DNS since we require all ORPS servers to have FQDNs.

Participation as a full member would open the way for the Trust's own staff to benefit from eduroam services, e.g. consultants teaching at the hospital would be able to gain eduroam connection at local universities (and at any of the hundreds of eduroam providers elsewhere in the UK and abroad). N.b. at present we must limit this to NHS staff involved in teaching, research or the support of these activities. Whilst Janet eligibility now extends quite broadly to include education, health and public sector organisations, eduroam is an international federated service with members drawn from many different countries where access to national education and research networks is in some cases more restrictive than in the UK. As the UK eduroam provider (and participant in the European confederation) we have to be sensitive to these concerns.

Therefore NHS Trust Home/IdP services should be restricted and the roaming user group should only comprise: staff engaged in or supporting research and training functions, medical researchers, doctors in training, teaching consultants (*), IT staff supporting such activities. At present, general medical staff, doctors, nurses, admin staff etc are not eligible to be given roaming credentials.

(*) This would include consultant surgeons and theatre staff needing to connect devices to the eduroam network for remote surgical support/training/remote hands systems.

Provision of a Visited-only service in association with a local University eduroam provider

Approach (3) is perhaps the most realistic and preferred approach for NHS Trusts as can be seen from the case studies in below, i.e. NHS Trusts can participate and provide a Visited service as an extension of a local university's eduroam service. This meets the main business requirement for eduroam deployment - that of providing a trouble-free network service for medical students/visiting lecturers/researchers. With this approach there are thee variants of the solution:

i) to use a high capacity WAN link between Trust and University for both authentication and data traffic; the eduroam visitor service would be provided via a VLAN from the University's eduroam visitor service

ii) to use a WAN link for authentication whilst data traffic from the Trust's own eduroam visitor network service is supported by an independent Interent feed

iii) visitor authentication supported by a Trust RADIUS server via the N3-JANET gateway peered with the University's RADIUS server (using address translation at the NATed N3 gateway)

Solution (i) has been adopted at a number of teaching hospitals across the country (e.g. Oxford's John Radcliffe; case study available). An association between NHS and local academic institutions enables beneficial sharing of network and communication infrastructure. The Trust and the local university connect their networks via a local wide area network link and the eduroam service managed by the university is extended across the Trust's (Wi-Fi) network. The eduroam visitor network is securely tunnelled to the university's network. Basically the eduroam network provided by the Trust APs would point to the university's RADIUS server (just for the eduroam SSID) for handling of authentications. User network traffic from authenticated and connected users is piped to the university's network. This is a simple and secure way for an NHS Trust to offer an eduroam 'Visited' service; this avoids the overhead of running an eduroam RADIUS server (since it would be managed by the university), but of course Home (ID provider services for the Trust's own staff) is not available with this solution. The university would need to be agreeable to extending its eduroam Visited service, including both IP address space and network bandwidth.

Solution (ii) would be applicable if the WAN link was not capable of supporting the expected data traffic levels or if the university was reluctant to supporting the extended visited service IP address space and data traffic across its own network to the JANET feed.

Solution (iii) would be applicable if the Trust operates its own RADIUS server already for local 802.1X based AAA but did not wish to participate in eduroam(UK) directly

Approach (2) would be for the Trust to participate as a full member of eduroam(UK) with a non-N3 Internet feed. This would require the deployment of a RADIUS server and connection to the Janet national proxies and connection of the Trust's eduroam network to either an independent Internet feed or to the university's network (this latter option would require use of the university's IP address space since the RADIUS server must be reachable via DNS... we require a FQDN for the RADIUS server).

Participation as a full member would open the way for the Trust's own staff to benefit from eduroam services, e.g. consultants teaching at the hospital would be able to gain eduroam connection at local universities (and at any of the hundreds of eduroam providers elsewhere in the UK and abroad). N.b. at present we must limit this to NHS staff involved in teaching, research or the support of these activities. Whilst Janet eligibility now extends quite broadly to include education, health and public sector organisations, eduroam is an international federated service with members drawn from many different countries where access to national education and research networks is in some cases more restrictive than in the UK. As the UK eduroam provider (and participant in the European confederation) we have to be sensitive to these concerns.

Therefore NHS Trust Home/IdP services should be restricted and the roaming user group should only comprise: staff engaged in or supporting research and training functions, medical

researchers, doctors in training, teaching consultants, IT staff supporting such activities. At present, general medical staff, doctors, nurses, admin staff etc are not eligible to be given roaming credentials.

Further information/case studies:

NHS-FE Connectivity Project Group Area:https://community.jisc.ac.uk/groups/nhs-he-forum-connectivity-project/article/nhs-and-eduroamshared-use-wireless [5]

Wireless access for Oxford University staff on Oxfordshire NHS sites: https://community.jisc.ac.uk/groups/nhs-he-forum-connectivity-project/documents/best-practice-working-group-wireless-access [6]

Providing eduroam at Raigmore Hospital, Inverness:https://community.jisc.ac.uk/groups/nhs-he-forum-connectivity-project/document/oct-2012-providing-eduroam-raigmore-hospital [7]

Providing Help to Other Participating Organisations

How can Higher Education Institutions assist Further Education with eduroam Implementation?

Content awaited

6) Commercial Organisations Participation

How can commercial organisations be involved in eduroam?

Commercial organisations may get involved in eduroam in a number of ways:

1. Visited service providers
2. Managed accommodation service suppliers
3. Product developers/product evaluators
4. Consultancy service suppliers
5. Managed service solution suppliers

Commercial organisations are **not** eligible to participate as 'regular' Home service providers (IdPs) which would enable their staff to use eduroam roaming capability to connect to the eduroam services of other member organisations. This restrictions applies on a number of grounds: Janet has Private Network status (which has implications for Jisc's Janet services) and as a publicly funded organisation, use of public funds and State Aid regulations apply; in addition eduroam(UK) is a member of the European/global eduroam confederation and must abide by international eduroam policy.

i) Visited Service provider

Commercial organisations may participate in eduroam(UK) as Visited-only participants (Service Providers). There are a number of reasons why a profit-centred organisation may wish to participate and offer a service for the benefit of the eduroam community.

This is not technically difficult nor particularly expensive, especially if another Wi-Fi service is being provided at the same time, but of course commercial organisations are normally reluctant to devote resources to projects without a perceived payback. Therefore motivation

for doing this may be:

- generation of revenue/profit/benefit; a wireless service provider may provide eduroam under a contractual arrangement with a customer in return for payment or some other benefit
- to build end-user client loyalty; students using an eduroam service provided by a WISP can be converted to paying customers at the end of their courses
- to increase footfall; availability of eduroam will attract members of the student/academic community to venues
- to make conference/training centres more attractive for delegates hence increasing/protecting booking rates
- to enhance prestige and for promotional/marketing reasons
- for public benefit/altruistic reasons

Whatever the scenario of the Visited service provision, eduroam must be free to users at the point of use.

All eduroam services must comply with the eduroam(UK) Technical Specification. We do not impose any special constraints on the RADIUS/Wi-Fi controllers: an on-site depolyed RADIUS server/Wi-FI controller-APs or an internet-based RADIUS service ('RADIUS in the cloud') and internet-based wireless controller or on-site controller-APs are options. The only considerations are that the standard requirements of the Tech Spec must be met; the RADIUS service needs to have a fixed publicly accessible IP address and (for instance in cloud implementations) latency needs to be considered.

We've had a number of FAQs on various aspects of deploying a service by commercial WISPs - answers as below:

- 802.1X supplicant configuration on users' devices is the responsibility of the 'Home' organisation, NOT the Wi-Fi service provider. User authentication is carried out by the Home organisation (identity service provider) and is implemented as RADIUS authentication against user database service.
- Internet feed for each site is used for both user authentication traffic and user data traffic. A connection to Janet is not mandatory, although all universities and colleges have Janet links. The eduroam VLAN/network service for each site normally just uses the local internet feed.
- Filtering of web traffic whilst not encouraged, is permitted on eduroam services and may be based on URL or content – provided that SSL/TLS interception is not employed.
- There is no charge (at present) for participation in eduroam(UK), either for publicly funded organisations or commercial service providers.
- RADIUS servers can be physical or VM instances and the recommended software is FreeRADIUS (open source) although OSC’s Radiator is a fully supported alternative, and there is also Microsoft NPS, Aruba CloudPath, Cisco ISE/ACS.
- eduroam(UK) operates a 'Support Server' which is the portal for self-service configuration of organisational RADIUS servers into the national infrastructure. This also provides test and monitoring services. Free of charge technical support is available. Chargeable training courses and on-site consultancy services are also available.

ii) Managed accommodation service suppliers

Commercial organisations can develop and provide managed Visited service solutions for eduroam(UK) member organisations, for instance as part of a managed accommodation service. Both the managed accommodation service supplier and the contractee organisation (the 'local' organisation) are members of eduroam(UK). The managed accommodation service supplier acts as a Visited service provider with its RADIUS server(s) peered with the eduroam(UK) NRPS. However the RADIUS server is **also** peered with the 'local' contractee RADIUS server. Authentications for non-local Authentications are forwarded to the NRPS. The contractee organisation provides the Home service (IdP). Authentications for users associated with the local contractee organisation are fowarded directly to the 'local' contractee RADIUS server. The technical considerations applying to this scenario were addressed in Tech Spec v1.3.

iii) Product developers/product evaluators

A commercial organisation may be involved in the development and manufacture of 802.1X products or solutions specifically for implementation of eduroam services. Such organisations are able to join eduroam(UK) for the purposes of product development/evaluation of manufacturers products forming part of their service offering. To this end implementation of Visited and Home services may be required and this is permitted, but such activity **must** be limited to the local test lab environment. Staff of commercial organisations **must not** use eduroam roaming capability to connect to the eduroam services of member organisations unless specifically for the purpose of collaborative research.

iv) Consultancy service suppliers

Commercial organisations can provide consultancy services under contract to eduroam(UK) member organisations. Such agreements are entirely a matter between the member organisation and the contractor. Member organisations may nominate contacts at commercial organisations for access to the eduroam(UK) Support server, but the member organisation remains the entity with membership of the eduroam(UK) federation and the responsibilities associated with that. eduroam(UK) cannot endorse commercial consultancy service providers.

As for any commercial organisation, a supplier of consultancy services may implement a Visited-only service at their offices/data centres etc. and local own-staff authentication is permitted (e.g. for test/evaluation purposes). Staff of commercial organisations **MUST NOT** use eduroam roaming capability to connect to the eduroam services of member organisations. It should be noted that testing of Visited service installations at customer sites is possible using the 'visitor simulation test' described in 15.2 of the Implementation Roadmap [8].

v) Managed service solution suppliers

Commercial organisations might develop and provide managed service solutions for eduroam(UK) member organisations. This is relatively new scenario in the UK and is largely untested.

Possible scenarios:

- managed service comprises management of an on-site depolyed RADIUS server/Wi-FI controller-APs
- managed service comprises internet-based RADIUS service ('RADIUS in the cloud') and

internet-based wireless controller or on-site controller-APs

Such agreements are entirely a matter between the member organisation and the contractor. Member organisations may nominate contacts at commercial organisations for access to the eduroam(UK) Support server, but the member organisation remains the entity with membership of the eduroam(UK) federation and the responsibilities associated with that.

Whatever the scenario of the Home/Visited service provision, eduroam must be free to users at the point of use.

7) Govroam

Can an eduroam member organisation participate in Govroam? How? What's the benefit? Is there a membership cost?

Yes, an eduroam member can participate in Govroam. In fact we would like to see this since the more research and educational organisations that participate, the greater the encouragement will be for Govroam members to reciprocate and provide eduroam across their estates in venues such as libraries, sports centres and government offices.

There is also a direct benefit for the educational organisation since enabling govroam lets you offer seamless internet access to visiting public-sector professionals, resulting in:

- Emergency services being able to easily connect to the internet in the event of an emergency on your site
- You are able to support local community outreach initiatives more easily

There is no membership fee for any organisation to participate as a Visited member. (Govroam has a different stakeholder group from eduroam's R&E community, hence the charging structure that has been put in place for Govroam IdP participation).

How to participate - contact govroam@jisc.ac.uk [9] and request visitor-only participation in Govroam. You'll be sent a boarding pack that provides details of the T&C's you'd need to sign; following those being received our technical specialists will provide a shared secret to secure the RADIUS link and help you configure your local RADIUS, and we you'll be given a set of Jisc dummy credentials for testing that everything is working.

https://www.jisc.ac.uk/govroam [4]

8) International Deployments

Can we support overseas offices using our UK eduroam membership and RADIUS deployment?

eduroam(UK) would be prepared to accept overseas users to be authenticated by your UK-based RADIUS server in circumstances where there is not a local national RADIUS service operator or for a small deployment in another eduroam-member country. This would however be technically sub-optimal since all roaming requests would be forwarded by international proxies back to the UK national proxy servers and thence to your RADIUS server. This chain of RADIUS proxies and long transmission distance could result a significant accumulation of delay and therefore slow authentication (a typical authentication requires around a dozen

RADIUS messages).

In fact if you deployed an overseas campus eduroam service, then technically all on-campus user authentication requests could be forwarded across the world and through our UK national proxies. However, in addition to the above performance concerns this would represent an unacceptable additional load for our servers to handle.

We have many overseas campuses in one country - what would be the best implementation model?

The practical solution for a campus overseas/several campuses in overseas countries would be to implement RADIUS services for the countries concerned (but this could be cloud based) and for those to peer with the countries' National RADIUS Operator (NRO) RADIUS servers (you'd need to join eduroam in the overseas countries concerened).

You will also have to think about the realm names that you use in each country. The UK can support camford.com (*) but for instance Australian based users will need an Australia-specific realm so that when the Australian users roam to another eduroam site (either in Australia or elsewhere overseas) eduroam RADIUS servers can forward authentication requests ultimately to your RADIUS server for Australia.

(*) For a non-country-specific realm (e.g. .com, .org) you will need to create a NAPTR record in DNS – this is simple and there's a how-to in our technical reference documentation https://community.jisc.ac.uk/library/janet-services-documentation/advisory-improving-efficiency-international-authentication [10].

9) Captive Portal/Web Redirect Solutions

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 tier JRS1 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 was available during the early years of the eduroam service in the UK - at the time of launch known as 'Janet Roaming'. Web redirect was always deprecated and was withdrawn many years ago. Organisations wishing to provide a guest Wi-Fi service are strongly encouraged to avoid web redirect systems and instead to develop 802.1X infrastructures and to adopt eduroam to support visitors.

For futher information please see:

http://www.terena.nl/activities/tf-mobility/deliverables/delF/DelF-f.pdf [11]

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).

10) Shibboleth

What's the difference between eduroam and Shibboleth?

Shibboleth and eduroam are complementary technologies that provide solutions to two different objectives.

The eduroam infrastructure provides the network access technology to make it easier for users with valid accounts at JANET connected organisations to log on to networks (both at home and) when visiting participating organisation sites. Before authentication, a user will typically have no access to the network or Internet. Once logged in using the eduroam infrastructure, a user will have access to the network and the Internet.

After having logged on to the network Shibboleth then facilitatesadmission to online resourcesthat are subject to access control. The Shibboleth architecture defines a streamlined way of exchanging information between an individual and providers of digital data resources to authorise the user's access to the resources. It has been designed to protect both the security of access to the data and the privacy of the individual viewing it (since authentication and authorisation is controlled by the home organisation).

Therefore, once a user has logged in using the eduroam infrastructure and gained access to the Internet, Shibboleth could then be used to provide authentication and authorisation to access controlled online resources, such as journals and media content.

http://www.ja.net/development/middleware/uk-federation.html [12]

There has been a JISC-funded project, LICHEN, aimed at extending the usage of eduroam in the Shibbolith arena. The main goal of LICHEN was to demonstrate that the eduroam architecture can be extended to embrace supporting access control and authentication for virtual organisations of collaborating users on a variety of applications that may themselves authenticate through RADIUS. The secondary aim was to investigate methods to have such authentication interoperate with Shibboleth [13].

Currently there is work being done at a European level to further explore the possibilities. See: Geant2 unified Single Sign-On (uSSO) [14]

Links

[1] https://community.jisc.ac.uk/library/janet-policies/security-policy
[2] https://community.jisc.ac.uk/library/janet-policies/user-authentication
[3] https://community.jisc.ac.uk/library/janet-policies/managing-safety-children-and-vulnerable-guests-he
[4] https://www.jisc.ac.uk/govroam
[5] https://community.jisc.ac.uk/groups/nhs-he-forum-connectivity-project/article/nhs-and-eduroamshared-use-wireless
[6] https://community.jisc.ac.uk/groups/nhs-he-forum-connectivity-project/documents/best-practice-working-group-wireless-access
[7] https://community.jisc.ac.uk/groups/nhs-he-forum-connectivity-project/document/oct-2012-providing-eduroam-raigmore-hospital
[8] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-2
[9] mailto:govroam@jisc.ac.uk
[10] https://community.jisc.ac.uk/library/janet-services-documentation/advisory-improving-efficiency-international-authentication
[11] http://www.terena.nl/activities/tf-mobility/deliverables/delF/DelF-f.pdf
[12] http://www.ja.net/development/middleware/uk-federation.html
[13] http://shibboleth.internet2.edu/
[14] http://www.geant2.net/upload/pdf/GN2-06-261v4-DJ5-3-1_Documentation_on_GEANT2_uSSO_requirements_20070201095918.pdf