Management Briefing - eduroam

Executive Summary

eduroam is the worldwide, single sign-on, secure network access system provided through collaboration of participating organisations within federated trust infrastructures managed by NRENs (national research and education network organisations) - in the UK this is Janet. eduroam enables individuals to 'just connect' their devices to eduroam services wherever they are encountered using the same Wi-Fi profile as used on the home network. This maximises productive time and online opportunities for individuals by eliminating the hassle of guest account and Wi-Fi setup. It does this whilst providing maximum security confidence for the user and the audit trail capability required by the organisation, all with minimal management overhead.

eduroam achieves this through being based on a RADIUS authentication infrastructure that securely redirects a visitor’s authentication back to their home institution, thereby eliminating the need for guest network accounts to be managed locally. It is part of eduroam, an international roaming federation created in partnership with other parallel initiatives worldwide.

Deployment requires creating a RADIUS service to handle proxied authentication, and meeting the minimum security standards in terms of authenticators for the network services offered to protect visitor credentials. This is the least resource-intensive method for implementing support for guest access and staff/student roaming, and can often be accomplished by using existing infrastructure.

1.0 Introduction

This document is intended to give IT Managers at organisations interested in deploying eduroam an overview of the eduroam(UK) Service.

1.1 Background & Terminology

Collaboration between institutions is at the heart of the research objectives of Further and Higher Education. Movement of staff between sites offers returns in terms of exchange of ideas, forging ties and generating opportunities for development. Trends in educational practice towards distance learning, an increased proportion of mature students and federated multi-centre courses create a similar flow between institutions at the student level. These students and staff typically enjoy well-developed IT provision at their home institution, and carry high expectations with them when they visit other sites.

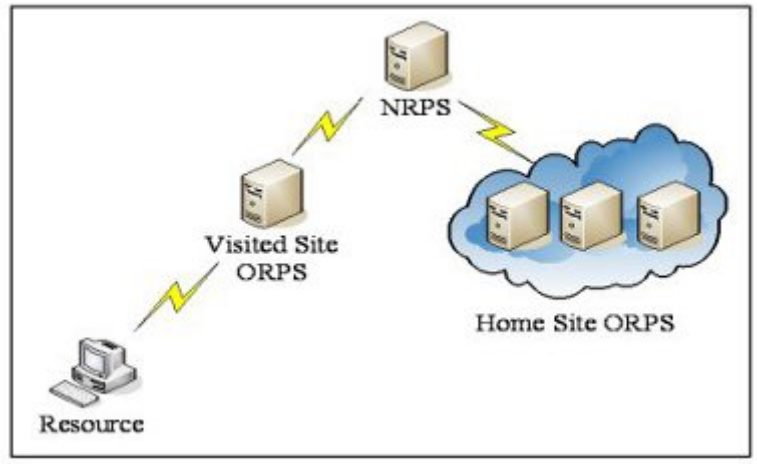
Data network connectivity contines to become increasingly essential to collaborative research, study and meeting support, which means that there is a clear requirement for IT managers to offer high quality network access to all kinds of visiting colleagues from other institutions. Dating from 2004, the MAWAA (Mobile Ad-Hoc Wireless Access in Academia) report [1] found

that:

‘as more devices become mobile, staff and students will expect to be able to carry their devices with them, and use them when travelling. Many laptop and PDA devices now come with built-in wireless networking cards. There is an expectation among users that they can use the wireless resources of another university while visiting that university, be it as a researcher at a workshop or a student attending a course. We can only expect mobility requirements to grow.’

The eduroam(UK) Service seeks to facilitate roaming access to network resources by relocating the authentication overhead from the **visited** site to the **home** site. The eduroam(UK) Service infrastructure removes the need to administer temporary accounts for individual visitors.

This is achieved by passing authentication traffic between visited and home sites using the well-established and widely deployed **RADIUS** protocol across a hierarchical network. This network consists of **ORPS** (Organisational RADIUS Proxy Servers, sited at each participating organisation) in communication with a centrally maintained **NRPS** (National RADIUS Proxy Server) which is responsible for building authentication channels. The NRPS redirects authentication queries from a visited site to the appropriate home institution for a decision. This decision is then routed back to the visited site to be acted upon – i.e. the home site confirms or denies the validity of the credentials presented by a guest claiming affiliation with them, and the visited site acts on that decision to provide or deny access to a resource such as Internet access for that guest user. The international eduroam federation adds a further [illegible] nal authentication referral between



[2]

Figure 1 - The eduroam(UK) Hierarchy.

Underlying this technological solution is a commitment from the participating sites to join a ‘federation of trust’ that each will honour the authentication decisions provided by the others, and that each will take reasonable steps to protect the credentials of visitors when provided to their local guest support infrastructure. The trust fabric is implemented as a chain of peer-to-peer shared secrets between RADIUS servers. The service is specified in a security-conscious configuration such that the likelihood of credential compromise is minimal.

1.2 Drivers for eduroam(UK)

Participation in the eduroam(UK)/eduroam initiative provides benefits both in reducing the costs associated with creating guest network services on campus and in allowing users to benefit from such facilities worldwide.

- Facilitate roaming network access for your own staff and students
    - Answer existing need and stimulate further mobility
    - Offsite meetings
    - Collaborations and secondments
    - Offsite study and participation.
- Monitor staff and student activities off-site
    - ORPS RADIUS logs provide data on when and where your users interact with roaming facilities.
- Provide network services for guests from eduroam(UK)-participant sites
    - Minimal overheads, lightweight infrastructure
    - Centralised support and incident management
    - Attract visitors through enhanced support for meetings, research collaborations, multi-centre course initiatives etc.
    - Meet visitor expectations.
- Integrate roaming support into existing local services easily
    - RADIUS-aware services may be eduroam(UK)-enabled for effectively zero capital cost.
- Aggregate the management of trust relationships with other institutions
    - Multiple bilateral agreements can be subsumed into the eduroam(UK) federation of trust
    - Standardise the baseline trust relationship without sacrificing the option of adding additional conditions to local agreements.
- Achieve experience with roaming technologies for minimal cost
    - Explore the possible benefits of enhanced roaming services without committing significant resources
    - Prepare for future devolved services as roaming technologies come to dominate (a useful step on the path towards Shibboleth, for example)
    - Deploy access technologies such as 802.1X in a limited arena, gaining experience helpful with possible future campus network access control deployment.

1.3 Costs and Benefits of eduroam(UK)

The aim of eduroam(UK) is to provide an easily deployed authentication fabric with lightweight infrastructure to reduce the costs associated with providing visitor network access.

eduroam Guest Support	
Requirements/Considerations	**Benefits**

Deployment and maintenance of an ORPS	Gain experience with RADIUS
Authentication channel does not provide data confidentiality (other than with 802.1X tiers)	Authentication currently conducted across private links (and technical solutions under development)
Possible single point of failure	Resilient ORPS easily implemented
	Future devolved services will also require this support capability: eduroam(UK) acts as a pilot in this regard

1.4 Examples of Existing CAMPUS and NREN Deployments

When the LIN (Location Independent Networking) trial, the UK antecedent to eduroam(UK), came to an end there were 33 LIN-enabled sites deploying a wide range of visitor network access facilities. In the course of the trial there were no reported security incidents or abuses of visited site Acceptable Use Policies. A number of the existing sites are organised in consortia that are continuing to depend upon eduroam(UK) authentication for course delivery or formally shared infrastructure.

One particular example of a successful eduroam(UK) deployment was that of the network provision for Networkshop 33. For this event, all wired, wireless and cluster facilities would accept eduroam(UK) credentials in addition to those generated specifically for the event.

There are a number of NREN-level roaming initiatives across Europe, but although a variety of underlying architectures are being explored, all are fundamentally interoperable via standards-based RADIUS. From this basis, an overarching federal structure has developed to create an international roaming fabric. (The geographical extent of this is discussed in 1.5 below.)

1.5 eduroam(UK) Coverage

eduroam(UK) has been implemented as a national service for UK HE/FE/research/learning support organisations which are eligible for Janet services. There are eduroam(UK) participant sites in every region, including 81% of higher education insitutions.

However, the eduroam(UK) initiative mirrors parallel international developments, and these have subsequently entered a partnership to form the eduroam federation. The map below depicts the NRENs that are currently participating in the European eduroam RADIUS hierarchy, together with Taiwan and Australia. TERENA provides the European root with which national services such as the UK NRPS peer. The two servers that provide this service are operated by SURFnet (the Netherlands) and Forskningsnettet (Denmark).

Other countries, including the USA are developing parallel infrastructures and nations in other continents have also expressed interest.

2.0 How to Get Involved

Becoming an eduroam(UK)-enabled site involves the creation of local services, appropriate policy provision, and integration with the wider eduroam(UK) community through interaction with the eduroam(UK) technical support service.

2.1 What Do I Need to do Locally?

If you already provide one or more guest network access services which you wish to eduroam(UK)-enable, or if you are looking to introduce such services, you must provide authenticators capable of facilitating the secure transfer of entered guest credentials to the National RADIUS proxy server, via a local site ORPS, for ultimate authentication at the

guest’s home organisation. If providing guest network access as part of eduroam(UK), you must make available a minimum set of services. These are listed in Appendix 1.

2.1.1 Implement an ORPS

The core eduroam(UK) component at an institutional level is the ORPS. Free and open source or commercial software for a variety of platforms is available to achieve this, and detailed configuration examples are available from the eduroam(UK) documentation and community. It is recommended that the ORPS be implemented separately from any existing RADIUS infrastructure on campus, forming a new top level to any local proxying hierarchy. Physically, it should be in a secure location with appropriate environmental conditions, and where possible dual power supplies and resilient network connections should be provided. Each ORPS must be NTP synchronised to ensure accurate timestamps on RADIUS logs. Whatever the platform, the ORPS must be kept secure by best practice administration.

The ORPS must be securely peered with the NRPS (see 3.3 below).

2.1.2 Deploy Secure Authenticators

Deployment of a secure authenticator method to handle the guest credentials and generate the initial RADIUS request is a eduroam(UK) participation requirement. The wide scope of potential services and authentication solutions preclude mandating a single solution, but suitable authenticators must be based on:

- Access-points capable of 802.1X authentication

Case studies are available from the eduroam(UK) community covering a wide variety of eduroam(UK) authentication strategies.

2.1.3 Make Administration and Support Provisions

Janet and the eduroam(UK) technical support centre must have a point of contact within your organisation responsible for ongoing support and monitoring of your ORPS. They should ensure that:

- local ORPS RADIUS transaction logs are retained in accordance with data protection (and if necessary made available to authorised parties for incident resolution) as mandated by eduroam(UK) policy
- developments in the eduroam(UK) are monitored, and any agreed changes to eduroam(UK) protocols implemented
- security incidents are reported to eduroam(UK) technical support promptly, and any subsequent investigation conducted in a timely fashion.

2.1.4 Adjust your Acceptable Use Policy

The eduroam(UK) model proposes that users in a roaming context are bound by their home site's Acceptable Use Policy but are additionally requested to respect the visited site's Acceptable Use Policy. It may therefore be necessary to ensure that these policies are worded so as to include network activities in a roaming context outside of the physical bounds of the home institution. Optionally, it may be appropriate to institute a specific policy applicable to visitors making use of the guest facilities you provide, if one does not yet exist.

2.1.5 Advertise a Service

Each participating organisation should create and maintain a web resource that contains details about the roaming services hosted at the site, to include at least the following items:

- locations from where access is available
- supported authentication methods
- the authorised services made available to the visiting user
- a link to the local Acceptable Use Policy [3].

Visited sites should provide details to visitors not only of the network services on offer and any local policies regarding their use, but also of the level of security implemented to protect transfer of their credentials, to allow the user to take personal responsibility for any additional security and privacy precautions required. This last point is particularly relevant when offering unencrypted network services.

Wireless LANs, a common technology for supporting visitors' networking needs, carry the additional eduroam(UK) requirement that a common SSID ('eduroam') be advertised by broadcast, and by other means such as signage in areas of coverage. This facilitates the use of roaming facilities across the eduroam federation without having to reconfigure client software.

This web information may optionally be supplemented by local posters or visitor guides where required.

2.1.6 Train your Roaming Users

In addition to making provision for guests wishing to make use of your local network resources, you should ensure that your own users (i.e. those for whom you are the home site) are able to benefit fully from roaming access to eduroam(UK) facilities elsewhere. As a minimum, they should be aware:

- that eduroam(UK) exists and that they should ask about eduroam(UK) when off-site
- that they remain bound by their home site Acceptable Use Policy when in a roaming context, and should also check for local rules restricting their use of the network
- of the correct format of their eduroam(UK) username
- of their responsibilities in maintaining credential security (i.e. identifying legitimate eduroam(UK)-enabled facilities)
- of their options in securing their own data transfers when interacting with low security guest services.

The eduroam(UK) Service mandates that the support load falls on the home site, so you must be prepared to support your users in a roaming context, primarily by providing remotely

accessible support information. Optionally, direct contact routes such as a phone line may be provided. There may also be a requirement to deal with purely local eduroam(UK)-related support queries (e.g. where can a laptop be charged, problems with a particular access point): if provided, the means by which this support is offered should also be clearly advertised to visitors.

3.0 Applying to Join the Service

eduroam(UK) is managed by Janet, through their eduroam(UK) support representatives, to ensure that it is accomplished efficiently and securely.

3.1 Provide Administrative Contact Details

Janet and the eduroam(UK) Technical Support centre must have a current point of contact with your organisation responsible for ongoing support and monitoring of your ORPS.

3.2 Agree a Realm Name

A unique realm must be assigned to the participating organisation to identify its users in a roaming context. The choice of this realm lies with the participating organisation, subject to approval by eduroam(UK) Technical Support. The realm format should be site.ac.uk. A typical roaming credential of a user within a realm might be james@example.ac.uk [4].

3.3 Organise Peering

eduroam(UK) Technical Support and the local site contact need to arrange the offline exchange of a shared secret to secure the communications between ORPS and NRPS. The link can then be tested using a local test account provided to the eduroam(UK) Technical Centre. This peering is a one-off process, although the test account is retained for ongoing service monitoring from the eduroam(UK) core.

3.4 Provide Details of Guest Provision

Janet maintains a centralised web resource listing the guest provision available at eduroam(UK) participant sites, typically by linking to your local eduroam(UK) web pages. Your site’s entry should be kept up to date as your visitor facilities evolve.

4.0 What Participation and Policy Guidelines Apply?

Considerable effort throughout the early trials has gone into creating a comprehensive, minimally restrictive and future-proof set of policy guidance for the service. These are published through the Janet eduroam website.

- eduroam(UK) Policy: https://community.jisc.ac.uk/library/janet-services-documentation/eduroamuk-policy [5]
- eduroam(UK) Technical Specification: https://community.jisc.ac.uk/library/janet-services-documentation/eduroamuk-technical-specification [6]

These guidelines are subject to ongoing review as technologies and circumstances change, and user input is welcomed.

5.0 What Technical Support is Available?

The central eduroam(UK) Technical Support service is designed to assist with ORPS registration, RADIUS testing, NRPS fault fixing and Acceptable Use Policy abuse and security incidents. Queries should be directed at Janet Customer Services on 0870 850 2212 or service@Janet.ac.uk [7].

For all other matters a ‘self-help’ discussion mailing list has been created and for historical reasons is named:

janet-roaming@jiscmail.ac.uk [8]

In addition, the status of the eduroam(UK) NRPS is monitored via Netsight:

`http://reading.netsight.ja.net/start.php/regional` [9]

6.0 Further Reading

RADIUS RFCs: http://www.freeradius.org/rfc/ [10]

Authentication Methods within RADIUS

EAP TLS in accordance with RFC's 2716 and 2246: http://www.faqs.org/rfcs/rfc2716.html [11] and http://www.faqs.org/rfcs/rfc2246.html [12]

EAP MD5-Challenge and One-Time-Password in accordance with RFC 2284: http://www.faqs.org/rfcs/rfc2284.html [13]

EAP TTLS (TTLS-PAP, TTLS-CHAP, TTLS-MSCHAP and TTLSMSCHAPV2) as per draft-ietf-pppext-eap-ttls-03.txt: https://datatracker.ietf.org/public/idindex.cgi?command=id_detail&id=7572 [14]

The eduroam federation

http://www.eduroam.org/ [15]

http://www.terena.nl/tech/task-forces/tf-mobility/ [16]

Related Studies

Mobile Ad-Hoc Wireless Access in Academia: http://eprints.ecs.soton.ac.uk/9518/01/mawaa-d2-v10.pdf [1]

Janet Wireless Advisory Group: http://www.ja.net/development/network-access/wireless/wag.html [17]

Appendix 1 – Technical Details of User Services

eduroam(UK) guest network services will as a minimum offer the following access to services.

1) E-mail

a. IMSP: TCP/406 egress and established.

b. IMAP4: TCP/143 egress and established.

c. IMAP3: TCP/220 egress and established.

d. IMAPS: TCP/993 egress and established.

e. POP: TCP/110 egress and established.

f. POP3S: TCP/995 egress and established.

g. SMTPS: TCP/465 egress and established.

h. Message submission: TCP/587 egress and established.

2) Web

a. HTTP: TCP/80 egress and established.

b. HTTPS: TCP/443 egress and established.

3) VPN

a. Standard IPSec VPN: IP protocols 50 (ESP) and 51 (AH) both egress and ingress; TCP/500 (IKE) egress only.

b. IPSec NAT traversal: UDP/4500 egress and established.

c. Cisco IPSec NAT traversal: TCP/10000 egress and established.

d. PPTP: IP protocol 47 (GRE) egress and established; TCP/1723 egress and established.

e. OpenVPN: TCP/5000 egress and established.

f. IPv6 Tunnel Broker NAT traversal: UDP/3653 and TCP/3653 egress and established.

4) Remote Desktop

a. RDP: TCP/3389 egress and established.

b. VNC: TCP/5900 egress and established.

c. Citrix: TCP/1494 egress and established.

5) Directory Services

a. LDAP: TCP/389 egress and established.

b. LDAPS: TCP/636 egress and established.

6) Secure Shell

a. SSH: TCP/22 egress and established.

7) File transfer

a. Passive (S)FTP: TCP/21 egress and established.

Originator: Mark O'Leary

Links
[1] http://eprints.ecs.soton.ac.uk/9518/01/mawaa-d2-v10.pdf
[2] http://community.jisc.ac.uk/system/files/images/eduroam-management-briefing01.jpg
[3] http://community.jisc.ac.uk/library/acceptable-use-policy
[4] mailto:james@example.ac.uk
[5] https://community.jisc.ac.uk/library/janet-services-documentation/eduroamuk-policy
[6] https://community.jisc.ac.uk/library/janet-services-documentation/eduroamuk-technical-specification
[7] mailto:service@janet.ac.uk
[8] mailto:janet-roaming@jiscmail.ac.uk
[9] http://netsight.ja.net/Public/HomePage.aspx
[10] http://www.freeradius.org/rfc/
[11] http://www.faqs.org/rfcs/rfc2716.html
[12] http://www.faqs.org/rfcs/rfc2246.html
[13] http://www.faqs.org/rfcs/rfc2284.html
[14] https://datatracker.ietf.org/public/idindex.cgi?command=id_detail&id=7572
[15] http://www.eduroam.org/
[16] http://www.terena.nl/tech/task-forces/tf-mobility/
[17] http://www.ja.net/development/network-access/wireless/wag.html