eduroam Deployment Guide

This document is due for revision. References to JRS and 'JRS tiers' should be disregarded.

It should be read in conjunction with

https://community.jisc.ac.uk/library/advisory-services/ieee-8021x-implementation-janet-connected-organisations [1]

Table of Figures

1. Using this Document

This document is designed to guide the deployment process of an organisation joining the eduroam(UK) service, from a ‘high altitude’ overview of the service down into the finer detail of

application configuration. It should be read in parallel with the relevant eduroam(UK) case studies. Since the mandatory requirements of eduroam(UK) participation can be met by many alternative technical solutions, one aim of this guide is to provide sufficient background information to inform choices made between these alternatives at the design stage. The structure is as follows:

- Section 2 – The context of the eduroam(UK) service
- Section 3 – How to apply for membership of eduroam(UK) and gain technical support at an early stage
- Section 4 – Background on the core technology choices to be made
- Section 5 – List of the functional requirements of eduroam
- Section 6 – References and sources of further information

Organisations with well developed existing AAA infrastructure will derive most benefit from the later sections, whereas ‘green field’ participants will initially need to focus on the background information to guide their fundamental technology choices.

2. Introduction

The Challenge

With data network connectivity becoming increasingly essential to collaborative research, study and meeting support, there is a clear requirement for IT managers to offer some measure of network access to visitors from other organisations, and to facilitate their own colleagues’ use of such facilities when off-site. The advent of mature wireless networking technology has accelerated this trend, as visitors bring with them network-aware devices and the expectation that they will be usable in the same ways as they would at their home organisations.

In addition to providing the bare connectivity, visitor connectivity provision requires that a full audit trail be maintained. Conventionally, this creates the need to issue unique credentials to the visitor for the duration of their stay, with the added overheads of robustly identifying them before credentials are issued, managing the account creation and expiry processes, providing a secondary authentication system and offering concomitant support. These overheads scale poorly under load, such as when hosting a conference or when a unique resource at an organisation becomes heavily used by the wider community.

In the policy sphere, in the event of inappropriate use of their networks by visitors, IT managers have no deterrent or sanction (short of legal action) beyond revocation of access for holders of temporary guest accounts. Thus the policing of local regulations also becomes an issue.

The Solution

The Janet eduroam facilitates roaming access to network resources by relocating the authentication overhead from the visited organisation (i.e. the physical location of the resource to which a guest is requesting access) to the home organisation with which that person is affiliated (e.g. as a student or member of staff), where it may be assumed that they already have existing credentials for access to their local resources when back at base. This authentication referral is accomplished via a hierarchical RADIUS (Remote Authentication Dial-In User Service: see section 4.2) core infrastructure. The Janet eduroam infrastructure

allows these existing accounts to be authenticated in a roaming context, saving the visited organisation the need to administer temporary accounts for individual visitors.

Janet eduroam participation is equally desirable for staff and students to access visitor services elsewhere, when they are in a roaming context. By retaining control of authentication, for the first time an audit trail of staff activities off-site becomes available. By participating in a defined schema of access tiers (see Section 4.1), the level of protection afforded to potentially-sensitive user data and credentials is predictable and staff training can be tailored accordingly. Overall, the number of variables involved in staff networking activities when off-site is greatly reduced, reducing support costs and potential undesirable consequences.

Parallel roaming initiatives have been developed across Europe under an umbrella organisation, the eduroam federation, of which the Janet eduroam is a member. By extending the RADIUS proxy hierarchy to a supra-national level and agreeing some core standards of implementation, international location-independent authentication is now possible. The eduroam system is widely implemented in Europe and has been adopted further afield, notably in Australia and Taiwan.

2.1 Janet eduroam Background & Terminology

eduroam(UK) grew out of the activities of the the UKERNA Wireless Advisory Group, which initially highlighted the benefits of wireless LAN technology in providing guest services and the need for compatibility in such services across academia to facilitate roaming. It steered a Location Independent Networking proof of concept that has since undergone an extended trial phase as a member of the eduroam federation. UKERNA (now Janet) launched the full Janet eduroam in Spring 2006 to a design derived from the experience and community feedback gathered from this extensive trialling process.

During the development of eduroam(UK), a number of core concepts have been identified for which a common terminology has been adopted in the UK. The following conventions will be used throughout this document:

- **Home organisation** – The organisation of origin for a visitor, where their credentials are authenticated.
- **Visited organisation** – The hosting organisation of the guest network service in question; the physical location of the visitor at the time access authenticated by the Janet eduroam or eduroam is requested.
- **ORPS** – Organisational RADIUS Proxy Server: the interface between authentication transactions at a local organisation and the Janet eduroam RADIUS hierarchy.
- **NRPS** – National RADIUS Proxy Service: the core of the Janet eduroam infrastructure which refers authentication requests between visited and home organisations (and to the international top level proxies when required).
- **Realm** – the component of Janet eduroam credentials that identifies the home organisation; a Network Access Identifier specification (RFC2486)-conformant string derived from the home organisation's domain name.
- **Janet eduroam credentials** – User credentials in the format user@realm [2], derived from the user's standard home organisation credentials and appropriate home realm.

3. Participation in eduroam(UK)

3.1 eduroam(UK) Technical Support

3.1.1 Role and Responsibilities

Janet eduroam Technical Support is available in the following areas:

- **General enquires** about the service – features and benefits, service details
- **Pre-deployment queries** – deployment planning, selection of ORPS systems, guidance on implementation, Janet eduroam Technical Specification
- **Support during implementation** – ORPS setup, user machine configuration
- **Post implementation technical issue resolution**
- A chargeable **consultancy service** is also available for more in-depth implementation support and technical issue investigation.

It should be emphasised that the services of Janet eduroam Technical Support are available to those considering participation or who are in the design/implementation stages of joining the service.

3.1.2 Contact Details

- E-mail: service@ja.net [3]
- Telephone: 0870 850 2212

Janet eduroam Technical Support also provides participants with tools to manage and test their organisation's Janet eduroam configuration via a website:

https://support.roaming.ja.net/ [4]

Janet eduroam Technical Support will provide credentials to access the website when an organisation submits an application to participate.

Finally, there is a mailing list for advertising all technical service-related matters and general technical discussion about the Janet eduroam and related technologies (RADIUS, 802.1X, EAP (Extensible Authentication Protocol), etc):

Janet-roaming-support@jiscmail.ac.uk [5]

Membership of this list is required for primary technical contacts at participant organisations, and is recommended for secondary contacts and others involved in roaming services.

3.2 Joining Janet eduroam

3.2.1 Guidelines and Application Process

Janet Service Desk processes initial applications to participate in Janet eduroam, as detailed on the web:

http://community.jisc.ac.uk/library/janet-services-documentation/joining-enquiry [6]

A brief online form [7] must be completed by the network management contact or IT director at the organisation wishing to participate. Before submitting this application, it would be sensible to read the eduroam(UK) Technical Specification and eduroam(UK) policy to ensure they

contain no insurmountable obstacles to participation (the page cited above links to both).

Following application, the services of eduroam(UK) Technical Support become available to assist with the implementation process. On completion of the required infrastructure, your eduroam system administrator/implementor must assert compliance with the eduroam(UK) Technical Specification via the self service and test tool Support server web site. This portal also provides your eduroam system implentor with the ability to peer your new ORPS with the eduroam(UK) national RADIUS infrastructure. The Support server also provides automated tools including a Nagios-based montoring system and a Quality Assurance Assitance Tool.

3.2.2 Common Queries

Reciprocity

eduroam(UK) policies place no obligation on a participating organisation to offer both reciprocating aspects of the roaming service at once: an organisation may allow its users to roam to other participating organisations without offering a local visitor service in return, or equally an organisation may offer guest services to external visitors without providing local users with the capacity to authenticate elsewhere. The Janet eduroam design acknowledges that local facilities or policy considerations may require either of these scenarios. However, it should be noted that the greatest benefit is derived from the service when it is implemented symmetrically, with the participant organisation serving both home organisation and visited organisation roles.

Support

eduroam(UK) participation does not entail any obligation to support visiting network users actively. The standardisation of the service tiers coupled with the referral of authentication mean that support queries can only be addressed meaningfully by the home organisation. Visited organisation provision, once documented and signposted, carries no user support component.

Exclusivity

There is no requirement that eduroam-enabled services are the only guest provision offered, or that local wireless services should be supplanted by the eduroam(UK) system. As long as the mandatory technical specifications for the eduroam(UK) service are met, alternatives can exist alongside it. It is also permissible to administer mechanisms (e.g. temporary local accounts) that allow visitors from non-participant organisations to access your local eduroam(UK) tier(s), provided that they undertake to observe both the local and Janet AUPs.

EAP Support

As discussed below, there are a bewildering variety of EAP (Extensible Authentication Protocol) types that could be deployed to create an eduroam(UK)-compliant ORPS. This does not imply that to implement the eduroam, the local infrastructure must be configured for all possibilities: any network access device (e.g. wireless access point or switch) that supports 802.1X pass-through will support all possible eduroam variants for visitor authentication without specific configuration.

4. Implementation Choices

Section 5 below summarises the minimum technical requirements for eduroam(UK) participation. Given these requirements, a number of choices have to be made, such as:

- Whether to act as a home organisation, visited organisation, or both
- Over which media to offer eduroam visitor access (wired, wireless or both)
- How to deploy RADIUS
- How to implement the ORPS.

The balance of this section seeks to give sufficient background information to assist with answering these questions. For many organisations, some of these questions may already be answered (e.g. by existing wireless guest services, existing RADIUS infrastructure for dial-up etc.)

‘Green Field’ Sites

Many organisations will already have a number of the components required by eduroam(UK) in operation for other functions, and so their design choices will be constrained. However, a number of potential participants will not have existing guest services or a well developed AAA infrastructure. For these ‘green field’ sites, the following planning process is recommended:

- Choose to offer wired, wireless or both
- Choose what type of credentials to issue to your users for eduroam and where they will be stored (options include Active Directory, NDS, User certificates, and SQL database)
- Determine the EAP type(s) you could use with the given credential database
- Select a suitable RADIUS server that can implement the chosen EAP type and communicate with the chosen credential database
- Choose suitable supplicant software based on your EAP type(s), RADIUS solution, supported operating systems etc.
- Develop a testbed system and gain familiarity with any new technologies before implementing the production service.

Organisations new to the eduroam(UK) and eduroam in general should choose a system appropriate to their existing technical expertise and their current and possible future needs from the technologies needed to participate. For example, if an organisation is implementing RADIUS purely to support the eduroam(UK) service and predicts no further expansion of its RADIUS usage, it may be appropriate to use an ‘out of the box’ implementation such as Microsoft IAS to meet the mandatory technical specification rather than to invest effort in deploying a more flexible (and therefore complex) option such as FreeRADIUS.

Similar arguments apply to the choice of ORPS operating system: an organisation with no existing UNIX® experience should not feel compelled to move to that platform for eduroam(UK) participation. That said, new technologies deployed as part of joining the eduroam(UK) may find additional unrelated applications within the organisation.

4.1 JRS Tiers

In the light of experience gained during the proof of concept and trial phases of the LIN initiative, the eduroam(UK) service was originally designed against a model of fully defined service tiers. This was designed to permit as wide a range of organisations to participate to the earliest opportunity. The number of tiers in the eduroam(UK) service was kept to three, and were designed to act as a logical progression of increasingly more fully-featured and

secure network environments for organisations to offer to guests. The lowest tier also served to accommodate existing deployments of legacy web-based access control systems that can be adapted to work within the eduroam(UK) service, offering a fast route to participation whilst more robust security systems at the higher tiers are developed by the organisation.Back in 2011 the tier system was abolished, to be replaced with a standard engineering standards specification. This removed variation in service provision in order to remove the potential discouragement of roaming users unable to readily predict whether a particular service will work at a given organisation (especially if such a fundamental service as e-mail cannot be guaranteed). Another consequence of service variability is the undermining of data security, and in particular credential protection. Fundamental to the eduroam(UK) service is a ‘web of trust’ between participants that each will take suitable care of the user credentials they will handle during the course of an authentication transaction.

The Technical Specifiation is quite strict, in order to ensure that the security evaluation that has been conducted for the eduroam(UK) service design remains valid and to maintain standardisation across participating organisations.

In choosing to deploy the eduroam(UK) service, the first step is to understand the networking requirements (see Table 1).

General properties			**IEEE 802.11 properties**			
NAS	**IPv6**	**NAT**	**WEP**	**WPA**	**WPA2**	**SSIDs**
802.1X	Permitted	Permitted	WEP not permitted. WPA not permitted in new installations		Permitted	eduroam

4.1.1 Tier JRS1 – Web-based Redirection

JRS1 was a tier specified in the original launch of eduroam(UK) - 'JRS' as it was known then. The distinction between tiews was removed several years ago and a standard engineering specification now applies.

4.1.2 Base Engineering Standard – 802.1X / ‘802.11i’

eduroam(UK) is based on authentication at the link layer via 802.1X. This is preferred because:

- the client does not need network access to authenticate, so there is no need to resolve names or obtain an IP address prior to authenticating
- NAS devices need only implement minimal layer 3 functionality
- authenticating at the link layer authorises all protocols at the same time.

a) 802.1X Issues

Firstly, some background: 802.1X defines the transport of EAPOL (EAP over LAN). EAP (defined in RFC2284) in turn defines a framework for a family of secure authentication EAP types. Of the various EAP types, three tunnelling methods are suitable for deployment on a wireless LAN in terms of security: TLS, TTLS and PEAP (see RFC4017 for properties that EAP types used on wireless LANs should possess). Furthermore, 802.1X incorporates a 'pass-through' mode whereby authentication can be tunnelled through a number of intermediaries using the RADIUS protocol to an ultimate EAP server.

These characteristics of 802.1X map neatly onto the requirements of eduroam(UK) authentication: the transfer of credentials is encrypted in the identified EAP methods and the pass-through mode allows this encrypted tunnel to persist across the visited network and any intervening public networks, all the way back to the home organisation RADIUS server for authentication. Tunnelled 802.1X EAP methods are immune to the 'evil twin' class of attack to which web redirect systems are potentially vulnerable because they implement secure authentication of the EAP server.

In practice, what the visited organisation authentication system sees during an 802.1X authentication is an access request from user anonymous@realm [8], which it can then forward to the appropriate home organisation using the realm information as usual for eduroam(UK) transactions. At the home organisation, the inner, tunnelled authentication transaction is unbundled and the real credentials are revealed. The visited organisation logs thus reflect the home organisations of users without incurring the data protection responsibilities of personally-identifiable records. However, if specific identities are ever required, these can be resolved by comparison with the relevant home organisation records and the eduroam(UK) core.

The preferred eduroam(UK) tiers all use 802.1X authentication mechanisms, and thus are reliant upon the visiting client running appropriate supplicant software. No web front end or other locally-controlled authentication mechanism is involved or, indeed, permitted. This offers the advantage that the user experience is consistent wherever they roam.

When designing an 802.1X deployment for the Jeduroam(UK), you should determine how your passwords are stored in your user database(s) and which operating systems you need to support. These factors will largely determine which EAP type(s) you deploy. For example, the native Windows® supplicant only supports MSCHAPv2 within PEAP, requiring that the EAP server deployed (i.e. your RADIUS solution) be able to authenticate MSCHAPv2 credentials. This in turn implies that the backend database of user account data needs to deliver plaintext passwords, since they are needed in MSCHAPv2 authentication. These issues are addressed more fully in the Wireless Advisory Group 802.1X factsheet [9].

b) Data Encryption Issues

eduroam(UK)-mediated guest access in a wireless environment needs to address both secure credential handling (see 802.1X Issues, above) and subsequent data privacy issues. In its turn, data privacy can usefully be considered at two levels: real-time protection, which mitigates session hijack and prevents data tampering in transit on time scales proportionate with typical session lengths, and long-term protection, which is resistant to extended brute force attacks against recorded transactions. Viewed in this context, even a technique known to be flawed as a long-term protective measure may still have value as a real-time protection to a session in progress.

Wireless encryption technology has improved over time, with a number of different standards represented among access points commonly deployed. Only the most recent offer the long term protection that is desirable for a eduroam(UK) facility, but even legacy techniques provide real time cover that offers some protection from casual exploits. The most commonly seen encryption standards are discussed briefly below.

WEP – Wired Equivalent Privacy

The original IEEE 802.11 standard aimed to provide a number of security features to secure wireless LAN communication:

- two different authentication methods: open system and shared key
- the WEP (Wired Equivalent Privacy) encryption algorithm
- an ICV (Integrity Check Value), encrypted with WEP, which provided data integrity.

Over time, these security features have proved to be insufficient to protect wireless LAN communication in common scenarios. In particular, the following weaknesses have been highlighted (and exploited):

- *The IV (initialization vector) is too small.* WEP uses an IV along with the supplied WEP encryption key as the input to an RC4 pseudo-random number generator, which produces a key stream that is used to encrypt the 802.11 frame payload. With a 24-bit WEP IV, it is easy to capture multiple WEP frames with the same IV value during an extended session, making real-time decryption easier than the nominal key length might suggest.
- *Weak data integrity*. WEP data integrity consists of performing CRC-32 checksum calculation on the bytes in the unencrypted 802.11 payload and then encrypting its value with WEP. Even encrypted, it is relatively easy to change bits in the encrypted payload and then properly update the encrypted CRC-32 result, preventing the receiving node from detecting that the frame contents have changed.
- *Uses the master key rather than a derived key*. The WEP encryption key, either manually configured or determined through 802.1X authentication, is the only available keying material. Therefore, the WEP encryption key is the master key. Using the master key to encrypt data is less secure than using a key derived from the master key.
- *No rekeying*. WEP does not provide for a method to refresh the encryption keys.
- *No replay protection*. WEP does not provide any protection against replay attacks, in which an attacker sends a series of previously captured frames in an attempt to gain access or modify data.

A number of proprietary techniques to compensate for these weaknesses (in particular rekeying) became available while the standards process worked towards a full security solution, IEEE 802.11i.

WPA – Wi-Fi Protected Access

Following recognition of the shortcomings of WEP, but prior to the ratification of the final IEEE 802.11i security standard for 802.11 networks, wireless vendors agreed on an interoperable interim standard known as WPA (Wi-Fi Protected Access™). WPA supports authentication through 802.1X (known as WPA Enterprise) or with a pre-shared key (known as WPA Personal), a new encryption algorithm known as the Temporal Key Integrity Protocol, and a

new integrity algorithm known as Michael (see below). WPA is a subset of the 802.11i specification.

WPA authentication occurs in two phases: an open system authentication followed by 802.1X with an EAP authentication method. (For environments without a RADIUS infrastructure such as SOHO networks, WPA Personal supports the use of a pre-shared key.)

WPA adds a new message integrity method, Michael. This algorithm calculates an 8-byte message integrity code (MIC) which is placed between the data portion of the 802.11 frame and the 4-byte ICV (integrity check value). The MIC field is encrypted along with the frame data and the ICV. Michael also provides replay protection. A new frame counter in the 802.11 frame is used to prevent replay attacks.

As a transitional standard, WPA is designed to support a mixture of WEP and WPA client associations. However, this is achieved by reducing the security of the WPA clients (the global encryption key is not dynamic) and is therefore deprecated.

WPA2 / 802.11i

WPA2™ is a product certification available through the Wi-Fi Alliance that certifies wireless equipment as being compatible with the now-ratified 802.11i standard. The goal of WPA2 certification is to support the additional mandatory security features of the 802.11i that are not already included for products that support WPA. Like WPA, WPA2 offers both Enterprise and Personal modes of operation and a two-phase authentication process.

WPA2 key management requires the determination of a mutual pairwise master key based on the EAP or PSK authentication processes and the calculation of pairwise transient keys through a four-way handshake.

WPA2 also requires support for the AES (Advanced Encryption Standard) using the CBC-MAC (Counter Mode-Cipher Block Chaining Message Authentication Code) Protocol (known as CCMP). AES Counter Mode is a block cipher that encrypts 128-bit blocks of data at a time with a 128-bit encryption key. The CBC-MAC algorithm produces a MIC that provides data origin authentication and data integrity for the wireless frame. A Packet Number field included in the WPA2-protected wireless frame and incorporated into the encryption and MIC calculations provides replay protection.

WPA2 also adds a number of features designed to increase roaming speed, such as pairwise master key caching and 802.1X pre-authentication with neighbouring APs.

Data Encryption and the eduroam(UK) service

At present, there are legacy and transitional implementations of wireless data security in use in the educational community and 802.11i, currently the best security standard, is only just beginning to have an impact in existing deployments. The tier structure of JRS takes this into account by specifying levels of service that adopt the features of each of the three levels of encryption discussed above, and by making recommendations to the user population based on the level of protection afforded by each.

It is expected that the less secure implementations will gradually be replaced and that the eduroam(UK) service will adapt to this changing environment by offering the best possible protection to users of the roaming network. However, this evolution will be undertaken slowly

and through consultation.

At present eduroam(UK) recommends that WEP offers real time protection only (but as such is still desirable if no better alternative is available, and is certainly much better than offering no encryption at all over the wireless network). Both WPA and 802.11i (marketed as WPA2) offer reliable long term protection at present.

c) Authenticator Issues

For eduroam(UK) compatibility, network access systems (i.e. wireless access points in the majority of eduroam(UK) deployments) must support 802.1X pass-through. Virtually all products claiming 802.1X functionality will also support pass-through. This capability allows the EAP tunnel for authentication to pass through the NAS effectively without the encrypted credentials being exposed. Between client and NAS they are transferred as EAPOL, and then at the NAS are converted to EAP-over-

RADIUS for subsequent transmission to the ultimate authentication server over the eduroam(UK) infrastructure.

4.2 RADIUS

4.2.1 RADIUS Background

[The following information has been adapted from 'RADIUS Protocol Security and Best Practices' by Joseph Davies (Microsoft Corporation, January 2002)]

Some organisations in UK higher and further education may not have deployed any RADIUS infrastructure prior to joining the eduroam(UK) service, so a brief introduction to the protocol is appropriate.

RADIUS is a protocol enabling centralised authentication, authorisation and accounting for network access. Originally developed for dial-up remote access, RADIUS has now been adopted by a number of networking services for these purposes. RADIUS is described in RFC 2865, 'Remote Authentication Dial-in User Service (RADIUS)' and RFC 2866, 'RADIUS Accounting'.

A RADIUS client sends user credentials and connection parameter information in the form of a RADIUS message to a RADIUS server. The server authenticates and authorises the client request, and sends back a RADIUS message response. RADIUS clients also send RADIUS accounting messages to RADIUS servers.

The RADIUS standards also support the use of RADIUS proxies, a feature central to eduroam(UK) operation. A RADIUS proxy is a computer that forwards RADIUS messages between RADIUS clients, RADIUS servers and other RADIUS proxies. RADIUS messages are never sent between the access client and the network access server.

RADIUS messages are sent as UDP (User Datagram Protocol) messages. UDP port 1812 is used for RADIUS authentication messages and UDP port 1813 is used for RADIUS accounting messages. (Some older servers might use UDP port 1645 for RADIUS authentication messages and UDP port 1646 for RADIUS accounting messages.) Only one RADIUS message is included in the UDP payload of a RADIUS packet.

RFCs 2865 and 2866 define the following RADIUS message types:

- **Access-Request**: sent by a RADIUS client to request authentication and authorisation for a network access connection attempt
- **Access-Accept**: sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt is authenticated and authorised
- **Access-Reject**: sent by a RADIUS server in response to an Access-Request message. This message informs the RADIUS client that the connection attempt has been rejected. A RADIUS server sends this message if either the credentials are not authentic or the connection attempt is not authorised
- **Access-Challenge**: sent by a RADIUS server in response to an Access-
- **Request message**. This message is a challenge to the RADIUS client that requires a response
- **Accounting-Request**: sent by a RADIUS client to specify accounting information for a connection that was accepted
- **Accounting-Response**: sent by the RADIUS server in response to the Accounting-Request message. This message acknowledges the successful receipt and processing of the Accounting-Request message.

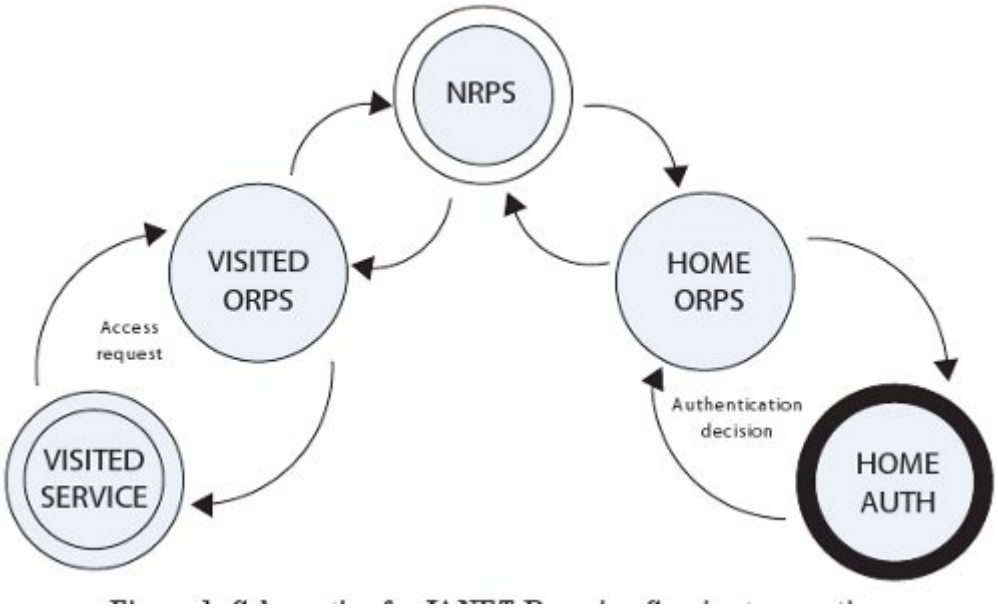
A RADIUS message consists of a RADIUS header and RADIUS attributes. Each RADIUS attribute specifies a piece of information about the connection attempt. For example, there are RADIUS attributes for the user name, the user password, the type of service requested by the user and the IP address of the access server. RADIUS attributes are used to convey information between RADIUS clients, RADIUS proxies and RADIUS servers. For example, the list of attributes in the Access-Request message includes information about the user credentials and the parameters of the connection attempt. In contrast, the list of attributes in the Access-Accept message includes information about the type of connection that can be made, connection constraints and any vendor-specific attributes.

For PPP (Point-to-Point Protocol) authentication protocols such as PAP (Password Authentication Protocol), CHAP (Challenge-Handshake Authentication Protocol), MS-CHAP (Microsoft Challenge Handshake Authentication Protocol) and MS-CHAP v2 (MS-CHAP version 2), the results of the authentication negotiation between the access server and the access client are forwarded to the RADIUS server for verification.

To provide security for RADIUS messages, the RADIUS client and the RADIUS server are configured with a common shared secret. The shared secret is used to secure RADIUS traffic and is commonly configured as a text string on both the RADIUS client and server.

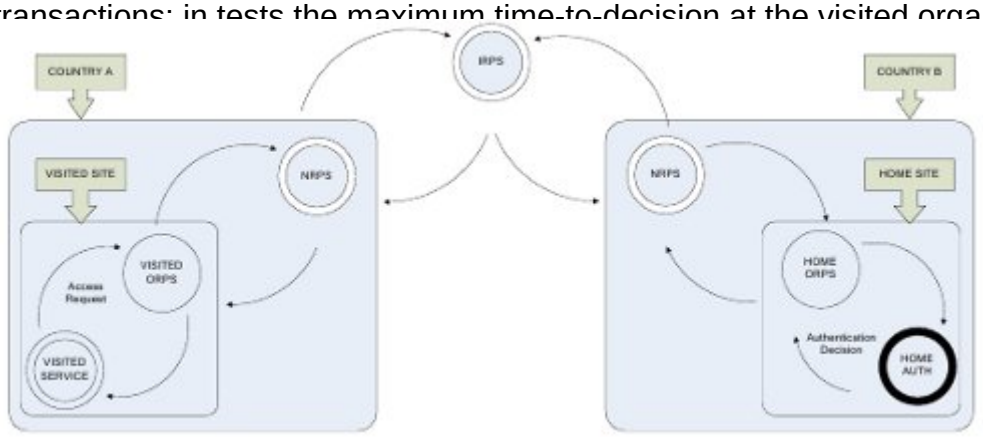
4.2.2 The eduroam(UK) RADIUS Hierarchy Model

The eduroam(UK) uses RADIUS proxying to decouple authentication transactions from physical location. The realm component of the eduroam username is used as routing information to traverse a hierarchical tree of RADIUS proxies. Requests received by the ORPS at the visited organisation are referred to an NRPS, a central hub which maintains trust relationships with all participant organisations in the UK (and can refer upwards to the eduroam federation for international authentication transactions). From there they are referred on to the ORPS at the appropriate home organisation (Figure 1).



[10]

The visited ORPS is configured to proxy requests for all non-local realms up to the NRPS. The NRPS recognises realms for all fully-registered participant organisations and can proxy the request accordingly (Figure 2). The proxy fabric handles all the routing of RADIUS transactions; in tests the maximum time-to-decision at the visited organisation was



[11]

In practice, a given organisation may have its own existing RADIUS infrastructure (i.e. multiple faculty- or service-specific RADIUS servers) into which the ORPS fits as a new top level to the local hierarchy. Organisations may also choose to implement redundant ORPS to remove a single point of failure (deployment options are discussed below).

4.2.3 The NRPS (National RADIUS Proxy Service)

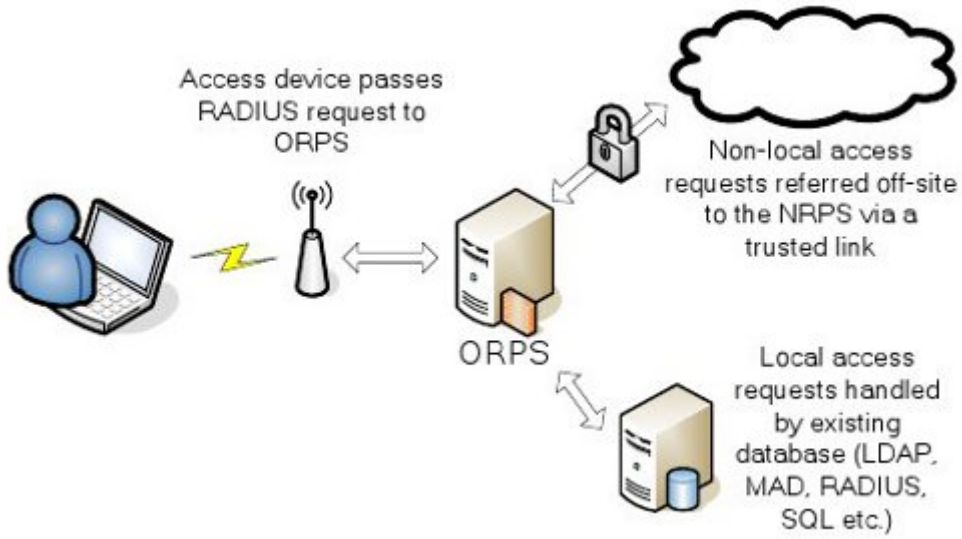
The NRPS is the hub of the eduroam(UK) infrastructure in the UK. It consists of three geographically separated high-availability RADIUS proxy servers managed by eduroam(UK) Technical Support. These servers are located behind firewalls that restrict RADIUS traffic from unknown hosts.

In operation the NRPS is entirely transparent, not modifying authentication transactions in any way as it routes them between visited and home organisations (although it does log their transit). Every ORPS negotiates a unique trust relationship with the NRPS via the standard RADIUS shared secret mechanism. A similar trusted link exists between the NRPS and the

two top level international RADIUS proxies that unite the various national domains to form the eduroam federation.

4.2.4 ORPS (Organisational RADIUS Proxy Servers)

The ORPS is the device deployed at every participant organisation, and administered by that organisation, that forms the point of entry into the eduroam(UK) hierarchy for authentication referral. The ORPS maintains a trust relationship with the national hub (the NRPS) and exchanges authentication requests with it. If the organisation offers an eduroam guest service, the ORPS passes on the authentication requests of visitors. It also integrates with local authentication systems to answer requests referred back via the NRPS from the organisation's own users when roaming off-site (Figure 3). In this latter role, an ORPS may either directly consult a user database by any of the various protocols supported by its SQL query etc.) or on.



[12]

4.2.5 ORPS Hardware Options

It is recommended that the ORPS RADIUS proxy be implemented on dedicated PC hardware separate from other aspects of campus infrastructure, although smaller organisations with an existing RADIUS requirement often amalgamate the ORPS function with their existing RADIUS configuration in a single device.

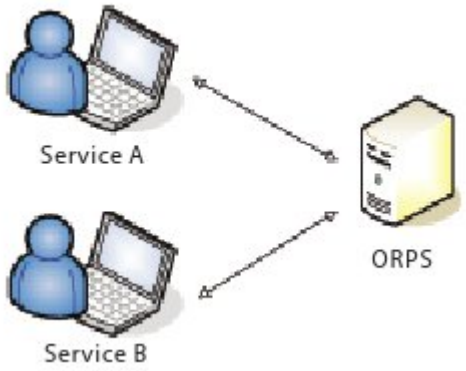
Hardware requirements for an individual ORPS will differ depending on operating system deployed, expected load and networking contexts, but the following suggested specification may be taken as a guide to ensure ample capacity into the medium term.

- Rack mountable
- Dual power supply
- VLAN-aware 10/100 ethernet card
- RAID 1 HDD array >60GB (depending on OS and logging options)
- 1 GB memory
- 3.0 GHz processor

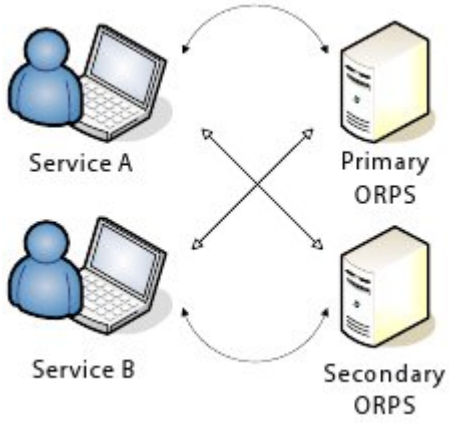
4.2.6 ORPS Deployment Strategies

Deployment strategies for the ORPS server(s) vary depending on whether RADIUS is already in use on your campus.

- **No previous RADIUS use.** Where expected visitor traffic is low and/or service level agreements can accommodate a single point of failure in the authentication chain, a single ORPS instance may be sufficient. In the majority of locations, however, we would recommend two servers, either in a primary/secondary authenticator configuration, or behind a load balancing device (the latter cases may complicate log maintenance unless also deployed) (Figures 4 and 5).

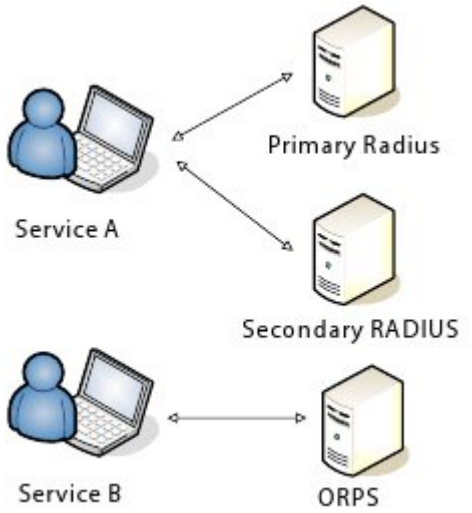


[13]



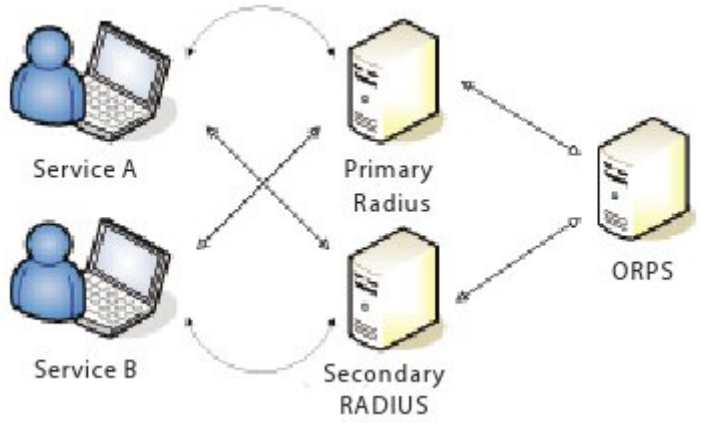
[14]

- **As part of an existing RADIUS infrastructure.** When adding an ORPS into an existing RADIUS infrastructure there are a number of benefits in mirroring the hierarchical structure of the eduroam(UK). The ORPS can be placed as a top level server to which the subordinate local RADIUS server(s) proxy traffic. Deployed in this way (as opposed to the configuration illustrated in Figure 6 in which the ORPS is a separate standalone authenticator to which requests must be directed), any existing authenticated services may be eduroam(UK)-enabled simply by honouring any realm information supplied.

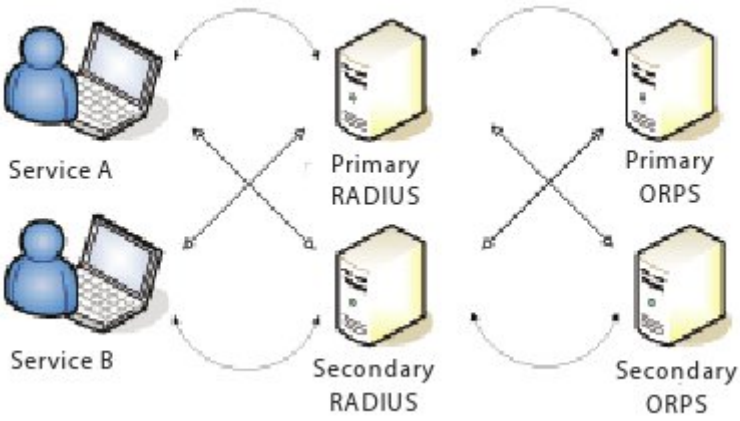


[15]

The recommendation is that to achieve a high availability environment, a dual ORPS configuration (primary/secondary or load balanced) is deployed in order to avoid a single point



[16]



[17]

4.2.7 RADIUS Software Options

Implementations of the RADIUS protocol are available for most operating systems, both as commercial packages and as open source software.

eduroam(UK) support will seek to describe in detail the implementations most commonly encountered in UK academia through technical case studies.

The RADIUS implementations most likely to be deployed or implemented at the present time are:

- **FreeRADIUS** – a free, open source implementation: http://www.freeradius.org/ [18]
- **Microsoft NPS (Network Policy Server)** - the Windows Server 2008 implementation of RADIUS, replacing **IAS (Internet Authentication Server)** – the Windows® Server 2000/2003 implementation of RADIUS: http://www.microsoft.com/windows2000/technologies/communications/ias/default.mspx [19]
- **OSC Radiator** – a feature-rich, perl-based commercial package, source supplied: http://www.open.com.au/radiator/ [20]
- **Cisco Secure ACS and Cisco ISE (Identity Services Engine) -** originally a software based GUI-fronted system, now available as an appliance
- **Aruba Clearpass**
- **Juniper SteelBelted**
- **Radsecproxy** - a proxy-only RADIUS system, which was designed to support RadSec (TLS/TCP and latterly DD)

However, any standards-compliant RADIUS implementation should be able to undertake ORPS duties. The relevant IETF standards are:

- RFC 2865: Remote Authentication Dial-In User Service (RADIUS)
- RFC 2866: RADIUS Accounting

4.2.8 Server and RADIUS Security

Whilst the eduroam(UK) tier design minimises the exposure of visitor credentials as they pass through the visited organisation ORPS (from tier JRS2 and higher, at least), the ORPS remains a component with privileged access into the eduroam(UK) hierarchy and is thus a potential target for attack. It is therefore essential that the integrity of ORPS systems be maintained at the highest level. The following recommendations may help. eduroam(UK) mandatory security practices are detailed in Section 5 below and in the associated case studies.

1. **Do not run unnecessary services.** For example, if you do not need the FTP server on your RADIUS server, do not give crackers another target: disable it, or do not install it at all. Similarly, disable scripting languages and remove sample scripts that you do not absolutely require.
2. **Subscribe to your server and OS security alert list**, or at least monitor related Web resources regularly for patches and apply them immediately. The Computer Emergency Response Team advisory list at http://www.cert.org/advisories/ [21] can be a useful resource.
3. **Practice good password habits**. Avoid simple, easy-to-guess passwords, particularly for privileged administrator accounts, and keep the number of accounts on the ORPS to a minimum for operation. Eliminate unnecessary accounts (such as guest). Make sure passwords are actually enabled for sensitive areas and administration functions. The Janet password factsheet [22] provides good advice.
4. **Use your operating system's permission mechanism**. Usually the RADIUS server

runs with the permission of a particular user. Make sure that that user has appropriately limited access.
5. **Monitor your logs**. Your RADIUS server keeps track of every request; review your logs regularly for signs of out-of-the-ordinary behaviour. Equally, monitor your syslog for unusual processes or access attempts.
6. **Be careful with your server configuration**. Run any security tools your OS or RADIUS server vendor provides, such as Microsoft's Lockdown Tool, to identify potential weak spots.

4.3 General Recommendations

Organisations may choose whether to act solely as a home organisation or visited organisation, or to offer reciprocal services. For visited organisations, there are many alternate routes to offering the standardised eduroam(UK) tiers of user service, and the tier structure itself permits a variety of eduroam(UK) variants to be presented. Overall this broad solution space grants the flexibility for organisations to accommodate unique local conditions (availability of resource, expertise or policy constraints) without compromising the standard user experience or security model.

However, where specific local conditions do not dictate the choices, some general recommendations may be made:

1. Act as both a visited and home organisation to maximise the benefit from the eduroam(UK) to your users and colleagues in the eduroam community.
2. Do not deploy Tier JRS1 – its shortcomings are discussed above and it may be withdrawn in the long term.
3. Do not deploy WEP on wireless eduroam(UK) services – its benefits are limited and it is widely believed to be insecure.
4. Minimise filtering between eduroam(UK) tier VLANs and the outside world – the roaming world embraces a greater variety of user expectations and legitimate applications that might be thwarted by a proscriptive firewall. This is not to say that access should be open between visitor services and the core campus network.
5. Do not use NAT for the guest network – NAT breaks a number of user applications and complicates the audit trail somewhat. Where existing address space is in short supply, eduroam(UK) applications are likely to be considered suitable justification for further provision.
6. Support IPv6 – this is another answer to any address shortage, and future-proofs current eduroam(UK) deployments. Bear in mind, however, the need for IPv6-aware firewalling.

5. Technical Deployment Guide

5.1 The eduroam(UK) Technical Specification

The 'tech spec' document is a vital reference when designing and implementing an eduroam(UK) presence for a new participant organisation, but it does not constitute a cook book on how to achieve the targets it sets out – that is the purpose of this document and the eduroam case studies. However, you should keep the specification on hand to ensure compliance with the service requirements. The latest version can be obtained from:

https://community.jisc.ac.uk/library/janet-services-documentation/janet-eduroam-technical-specification

[23]

5.1.1 Using this Technical Deployment Guide Section

The subsequent sections feature a list of requirements for deployment cross-referenced to the pertinent section(s) of the technical specification. There is also space provided for noting references to any case studies you may be consulting.

Please note that this section addresses only the hardware and software aspects of Janet eduroam roll-out. The technical specification also mandates a number of organisational and procedural aspects of participation (such as contact arrangements or the time periods for which logs must be retained) which must also be observed.

5.2 Common Requirements

5.2.1 ORPS

5.2.1.1 Hardware Choice

No specific mandatory requirements, beyond the implied needs of availability, and supporting the required OS, RADIUS and logging functions – indeed the ORPS function – may be implemented on existing hardware serving other purposes (although this is not recommended). Aspects of this hardware choice are discussed in section 4.2.5 above.

5.2.1.2 Operating System

The specific demands on the OS of the ORPS are restricted to NTP support, but other aspects of the ORPS requirement as a whole devolve onto the OS: for example, the firewalling requirements may most readily be implemented using a firewall package on the ORPS itself.

- **Requirement:** Time synchronised regularly with a reliable time source.
- **Tech Spec:** p 6, RQ 7.

5.2.1.3 Firewall Rules

- **Requirement:** Must be contactable by NRPS on either UDP 1812/1813 (recommended), or UDP 1645/1646
- **Tech Spec:** p 6, RQ 9.

- **Requirement:** Must respond to ICMP Echo Requests sent by the NRPS.
- **Tech Spec:**p 6, RQ 10

5.2.1.4 RADIUS Software

- **Requirement:** Must log all authentication requests exchanged with the NRPS, including at minimum Username and Calling-Station-Id
- **Tech Spec:** p 6, RQ 11; p 6, RQ 11.1; p 6, RQ 11.2

- **Requirement:** Must log all accounting requests, including at minimum Username, Accounting Session Id, Accounting status type.
- **Tech Spec:** p 6, RQ 12; p 6, RQ 12.1; p 6, RQ 12.2; p 6, RQ 12.3

- **Requirement:** Must have the capacity to timestamp log records with date and time
- **Tech Spec:** p 5, RQ 4.

- **Requirement:**Must comply with RFC 2865 and RFC 2866
- **Tech Spec:** p 6, RQ 6

5.3 Home Organisation Requirements

5.3.1 RADIUS

- **Requirement:** Must log all local authentication attempts, including at minimum: time received, result returned, and reason given for any rejection or failure
- **Tech Spec:** p 8, RQ 15; p 8, RQ 15.1; p 8, RQ 15.2; p 8, RQ 15.3

- **Requirement:** Must authenticate one or more EAP types, and generate symmetric keying for specific type(s) as per RFC 3580
- **Tech Spec:** p 9, RQ 16; p 9, RQ 16.1

- **Requirement:**Must create an authenticable test account

5.3.2 User Database

- **Requirement:** Must create a test account, which can authenticate both by PAP and the locally-adopted EAP methods.
- **Tech Spec:** p 9, RQ 17; p 10, RQ 17.1

5.4 Visited Organisation Requirements

5.4.1 User Service Characteristics

- **Requirement:** Must implement at least one of the Janet eduroam tiers.
- **Tech Spec:** p 11, RQ 19

- **Requirement:** Must ensure that the Janet eduroam is clearly identifiable as such.
- **Tech Spec:**p 11, RQ 20

- **Requirement:** Must ensure that non-participant organisation users (where granted access) must read and agree to both the Janet eduroam Policy and the local AUP before accessing the service.
- **Tech Spec:**p 11, RQ 23

- **Requirement:** Must publish a Janet eduroam website, including the local AUP and sufficient information to enable visitors to identify and access the service (tiers deployed, SSIDs, locations etc.).
- **Tech Spec:**p 15, RQ 33; p 15, RQ 33.1; p 15, RQ 33.2

5.4.2 Addressing

- **Requirement:** Must allocate IPv4 addresses to visitors using DHCP.

- **Tech Spec:** p 18, RQ 43

- **Requirement:** Must log IPv4 addresses allocated to visitors against the corresponding MAC addresses.
- **Tech Spec:** p 18, RQ 44

- **Requirement:** If NAT is deployed, address mappings must also be logged.
- **Tech Spec:** p 18, RQ 45

5.4.3 RADIUS

- **Requirement:** Must ensure that the NAS generates RADIUS Access-Requests which include the supplicant's MAC address in the Caller-Station-IS attribute and the NAS IP in the NAS-IP-Address attribute.
- **Tech Spec:** p 13, RQ 29; p 13, RQ 29.1; p 13, RQ 29.2

- **Requirement:** Must forward Janet eduroam-related RADIUS requests containing usernames with non-local realms via an ORPS to an NRPS.
- **Tech Spec:** p 12, RQ 25

- **Requirement:** Access-Requests must be addressed to UDP/1812.
- **Tech Spec:** p 12, RQ 25.1

- **Requirement:** Accounting-Requests must be addressed to UDP/1813.
- **Tech Spec:** p 12, RQ 25.2

- **Requirement:** Must not forward RADIUS requests to any domain (besides the NRPS) that the participant does not administer.
- **Tech Spec:** p 12, RQ 26; p 12, RQ 27; p 12, RQ 28

5.4.4 Wired Networking Context

- **Requirement:** Must implement a separate VLAN for each Janet eduroam tier deployed.
- **Tech Spec:** p 11, RQ 22

- **Requirement:** May implement IPv4/6 filtering between the visitor VLAN(s) and other external networks, providing that this permits the forwarding of the defined list of common protocols from the tech spec.
- **Tech Spec:** p 14, RQ 30; p 14, RQ 30.1 – 30.22

5.4.5 Wireless Networking Specifics

- **Requirement:** Must reserve the 'eduroam' prefix for SSIDs used with Janet eduroam tiers only.
- **Tech Spec:** p 11, RQ 21

- **Requirement:** Must broadcast the SSID 'eduroam' to identify a Janet eduroam wireless service (or 'eduroam-wep' / 'eduroam-web' as appropriate if multiple wireless Janet eduroam tiers are deployed).
- **Tech Spec:** p 16, RQ 34; p 16, RQ 34.1; p 16, RQ 34.2

- **Requirement:** Must not offer visitors any wireless media other than IEEE

802.11.
- **Tech Spec:** p 11, RQ 24

- **Requirement:** Where WEP is deployed, APs must be configured to require 128-bit keys rotated at least every 5 minutes.
- **Tech Spec:**p 18, RQ 48

5.4.6 Proxies (Optional)

- **Requirement:** Organisations deploying application or ‘interception’ proxies on the visitor LAN must publish this fact on their Janet eduroam website.
- **Tech Spec:** p 15, RQ 31; p 15, RQ 33.3

- **Requirement:** If the proxy is not ‘transparent’, the visited organisation must also provide documentation on the required user configuration(s).
- **Tech Spec:** p 15, RQ 32

5.4.7 JRS1 Specifics

- **Requirement:** Must only implement WRD NASs.
- **Tech Spec:** p 16, RQ 35

- **Requirement:** WRD NASs must support RADIUS PAP authentication.
- **Tech Spec:** p 16, RQ 36

- **Requirement:** WRD NASs must support SSL or TLS and be configured to present visitors with a server certificate from a well-known certificate authority.
- **Tech Spec:** p 16, RQ 37

5.4.8 JRS2 Specifics

- **Requirement:** Must only implement IEEE 802.1X; no form of WRD is permitted.
- **Tech Spec:** p 17, RQ 38

- **Requirement:** NASs must support symmetric keying using keys provided by the home organisation within the RADIUS Access-Accept packet, in accordance with RFC 3580.
- **Tech Spec:** p 17, RQ 39

- **Requirement:** Only a single user is permitted per NAS port.
- **Tech Spec:** p 17, RQ 40

- **Requirement:** JRS2 services must implement one of WEP or WPA.
- **Tech Spec:** p 18, RQ 46; p 18, RQ 49

5.4.9 JRS3 Specifics

- **Requirement:** Must only implement IEEE 802.1X; no form of WRD is permitted.
- **Tech Spec:** p 17, RQ 38

- **Requirement:** NASs must support symmetric keying using keys provided by the home organisation within the RADIUS Access-Accept packet, in accordance with RFC 3580.
- **Tech Spec:** p 17, RQ 39

- **Requirement:** Only a single user is permitted per NAS port.
- **Tech Spec:** p 17, RQ 40

- **Requirement:** NAT is not permitted.
- **Tech Spec:** p 18, RQ 41

- **Requirement:** Must allow routing of IPv6 on the visitor VLAN.
- **Tech Spec:** p 18, RQ 42

- **Requirement:** Must not implement WEP.
- **Tech Spec:** p 18, RQ 47

- **Requirement:** Must implement WPA2.
- **Tech Spec:** p 20, RQ 50

6. Reference Materials

- The Janet eduroam homepage: http://www.ja.net/eduroam/ [24]

6.1 Core Documentation

- Document index: https://community.jisc.ac.uk/library/janet-services-documentation/documentation [25]
- Roaming policy: https://community.jisc.ac.uk/library/janet-services-documentation/eduroam-policy [26]
- Technical specification: https://community.jisc.ac.uk/library/janet-services-documentation/janet-eduroam-technical-specification [23]
- Security overview: http://community.jisc.ac.uk/library/advisory-services/janet-eduroam-security-measures [27]
- Management briefing: http://community.jisc.ac.uk/library/janet-services-documentation/management-briefing [28]
- User guide: http://community.jisc.ac.uk/library/eduroam/eduroam-user-guide [29]

6.2 eduroam

- eduroam homepage: http://www.eduroam.org/ [30]
- Candidate eduroam policy: `http://www.eduroam.org/docs/GN2-eduroam-policy-draft_2006_02_15_no_tracking.pdf`
- eduroam use cases:
  `http://www.eduroam.org/docs/use_case_eduroam_example_1.pdf`
  `http://www.eduroam.org/docs/use_case_eduroam_example_2.pdf`
  `http://www.eduroam.org/docs/use_case_eduroam_example_3.pdf`
- eduroam development: `http://www.eduroam.org/wiki/HomePage`

6.3 Other Materials

- 802.1X workshop: http://www.terena.nl/activities/tf-mobility/1x/doc/handson06.pdf [31]

- Janet WAG: https://community.jisc.ac.uk/library/advisory-services/wireless-technolo... [32]

Source URL: https://community.jisc.ac.uk/library/janet-services-documentation/eduroam-deployment-guide

Links
[1] https://community.jisc.ac.uk/library/advisory-services/ieee-8021x-implementation-janet-connected-organisations
[2] mailto:user@realm
[3] mailto:service@ja.net
[4] https://support.roaming.ja.net/
[5] mailto:JANET-roaming-support@jiscmail.ac.uk
[6] http://community.jisc.ac.uk/library/janet-services-documentation/joining-enquiry
[7] https://community.jisc.ac.uk/library/janet-services-documentation/how-does-organisation-join-service
[8] mailto:anonymous@realm
[9] http://community.jisc.ac.uk/library/advisory-services/%E2%80%98alphabet-soup%E2%80%99-80211-family-wireless-standards%20
[10] http://community.jisc.ac.uk/sites/default/files/jrs-deployment-guide01.jpg
[11] http://community.jisc.ac.uk/sites/default/files/jrs-deployment-guide02.jpg
[12] http://community.jisc.ac.uk/sites/default/files/jrs-deployment-guide03.jpg
[13] http://community.jisc.ac.uk/sites/default/files/jrs-deployment-guide04.jpg
[14] http://community.jisc.ac.uk/sites/default/files/jrs-deployment-guide05.jpg
[15] http://community.jisc.ac.uk/sites/default/files/jrs-deployment-guide06.jpg
[16] http://community.jisc.ac.uk/sites/default/files/jrs-deployment-guide07.jpg
[17] http://community.jisc.ac.uk/sites/default/files/jrs-deployment-guide08.jpg
[18] http://www.freeradius.org/
[19] http://www.microsoft.com/windows2000/technologies/communications/ias/default.mspx
[20] http://www.open.com.au/radiator/
[21] http://www.cert.org/advisories/
[22] http://community.jisc.ac.uk/library/janet-services-documentation/using-passwords
[23] https://community.jisc.ac.uk/library/janet-services-documentation/janet-eduroam-technical-specification
[24] http://www.ja.net/eduroam/
[25] https://community.jisc.ac.uk/library/janet-services-documentation/documentation
[26] https://community.jisc.ac.uk/library/janet-services-documentation/eduroam-policy
[27] http://community.jisc.ac.uk/library/advisory-services/janet-eduroam-security-measures
[28] http://community.jisc.ac.uk/library/janet-services-documentation/management-briefing
[29] http://community.jisc.ac.uk/library/eduroam/eduroam-user-guide
[30] http://www.eduroam.org/
[31] http://www.terena.nl/activities/tf-mobility/1x/doc/handson06.pdf
[32] https://community.jisc.ac.uk/library/advisory-services/wireless-technology-advisory-service