eduroam(UK) Technical Specification

A correctly formatted and downloadable copy of the Technical Specification can be found at:

https://community.jisc.ac.uk/groups/eduroam/document/eduroamuk-technical-specification-v14 [1]

That page also contains handy **Summary of Requirements** and **Summary of Recommendations** checklists which may help when conformance assurance checking of your deployment.

eduroam(UK) Technical Specification

Version 1.4
14 July 2016

Originator: Josh Howlett

Revisions by: Edward Wincott

Advisors: Dr Alan Buxey, Scott Armitage, Alec Edworthy

OD/MO/EDUROAM/DOC/001

Contents:

1.Introduction

1.1. Acknowledgements

The authors would like to acknowledge the many important contributions provided by the following during the original production and subsequent revisions of this document:

- the members of the Jisc (formerly Janet) 802.1X Special Interest Group and the Wireless Access Group (WAG);
- the subscribers of the Jisc Wireless-Admin mailing list;
- the members of the GÉANT Mobility Task-Force (TF-Mobility);
- the members of European eduroam confederation national roaming operator (NRO) community;
- the Janet Location Independent Networking (LIN) National Trial participants.

The authors also thank colleagues at Jisc (formerly Janet) and particularly the eduroam(UK) Technical Support team based at Loughborough University for their contributions, support and assistance.

1.2. Overview

This document is the Technical Specification for the federated eduroam service operated by Jisc for participants in the UK and associated territories and is effective from 14th July 2016. It complies with the requirements mandated by the GÉANT European confederation policy (GN3-12-194) [1]. This document is subject to periodic revision; changes will be notified to

registered contacts at participating organisations and to the community via the Jisc Community eduroam website [2], at which the most recent revision will be found.

1.2.1. Using this Document

This document uses the conventions specified in RFC 2119 [3] for indicating requirement levels.

This document consists of five sections. The first (‘Introduction’) and fifth (‘Appendices’) are for informational purposes only. The latter section contains four appendices: two summaries of the requirements and recommendations laid out in this document; a glossary defining various technical and non-technical terms; and a bibliography.

The remaining three sections are normative. These are:

- Section 2 (‘Common Requirements and Recommendations’). This section is concerned with general requirements that are common for all participating organisations.
- Section 3 (‘Home Organisation Requirements and Recommendations’). This section is concerned with the requirements for Home organisations, and primarily the authentication of users.
- Section 4 (‘Visited Organisation Requirements and Recommendations’). This section is concerned with the requirements for Visited organisations, and primarily those relating to the visitor network.

1.3. Change log

To assist the reader the most significant changes to the requirements have been italicised.

1.3.1. Changes from version 1.3

- All references to ‘Janet’ in an organisational context changed to ‘Jisc’; references to Janet in the context of the network and network-related documentation remain unaltered.
- Overview, reference 1 to GÉANT European confederation policy, updated. Scope of document updated to accommodate provision of service in all UK associated territories.
- Section 4 introduction: removed explanation of the historical legacy of the JRS technical standards tiers system, which allowed WPA and captive portal technologies to be included in service variations as defined in previous versions of this specification up to and including v1.1.
- New Requirement 4: participating organisations must accurately assert both the service type and compliance level, and the operational status of their service via the Support server; and these assertions must be kept up to date. v1.3 requirement 4 renumbered to 5 and subsequent requirements numbering incremented by 1.
- Requirement 5 (previously 4) worded to improve readability and clarity.
- Requirement 6 (previously 5) changed timestamp requirement to be ‘in GMT’ to the more correctly applicable ‘UTC’ standard.
- Requirement 11 (previously 10) revised to remove requirement for ORPS to be reachable on accounting ports UDP/1813 or UDP/1646 since NRPS no longer forward accounting requests to ORPS, and wording updated to more RFC conventional style.
- Requirement 14 deleted because whilst the NRPS will continue to respond to accounting requests if forwarded to them, the content of the requests is not important as

they are not forwarded onwards. Subsequent requirements numbering decremented by 1.

- Requirement 16 deleted because provided that the requirements relating to logging are satisfied, exactly how organisations do this is outside the scope of this specification. It is for the organisation to determine what logging of RADIUS accounting requests and attributes are appropriate. Subsequent requirements numbering decremented by 1.
- Discussion 2.4.3: paragraph 3, 4 edited to remove references to accounting ports (1813 and 1646). New paragraph appended to explain reasoning behind deprecation of forwarding of accounting requests and notice of future mandatory requirement to not forward such requests to the NRPS.
- Requirement 19.4 (previously 20.4): reference to ‘User ID’ changed to ‘User-Name’ to clarify need for all parts of the user name to be logged.
- Requirement 19.7 added: Operator-Name attribute must logged if present in Access-Request.
- Requirement 22 (previously 23) reworded to more accurately tie the requirements relating to test accounts to the capability of the Support server
- Requirement 23 (previously 24) changed to align with current self-service process of making updates to test account details through the Support server web portal rather than via the support team personnel.
- Discussion 3.4.3 updated to reflect withdrawal of support for PAP in the Support server monitoring system and the self-service nature of the Support web portal now.
- Recommendation 3.6.2 reworded to improve readability.
- Discussion 3.6.3 updated to more accurately qualify NAS-Port-Type attribute and to include Service-Type in the explanation.
- Section 4 introduction: base engineering standards summary table updated to reflect the requirement that WPA/TKIP must not be supported in any circumstances and IPv6 specification uprated to SHOULD.
- Requirements 31.3 (previously 32.3) and 31.4 (previously 32.4) deleted.
- New Requirement 39: the setting on the Support server web portal to enable Status-Server requests sending from the NRPS to an ORPS MUST NOT be enabled if the ORPS cannot correctly respond to such requests.
- New recommendations 16 and 17 inserted relating to utilisation of and response to Status-Server queries if ORPS have such capability. Subsequent recommendation numbering adjusted.
- Visited service IP forwarding: list of ports and protocols that must as a minimum be permitted updated to **remove** LDAP and POP. Table tidied up.
- Recommendation 4.5.2 updated to specify ‘the Internet’ rather than specifically ‘Janet’ since Visited network services providing access to the Internet can be implemented other than via a Janet connection.
- New Requirement 48: Transport Layer Security (TLS)/Secure Sockets Layer (SSL) interception proxies MUST NOT be applied to network services for eduroam visitors.
- Discussion 4.6.3 expanded to include reference to TLS interception and noting that users when at their home organisation may be connected to non-eduroam network services.
- Requirement 50 (previously 49) reworded for clarification.
- Discussion 4.8.2: paragraph relating to XP deleted since XP is no longer a current operating system.
- Discussion 4.9.4 updated as IPv6 is becoming increasingly widely deployed.
- Requirement 56 (previously 55) reworded to explicitly disallow WPA and TKIP.
- Recommendation paragraph 4.10.2 and Recommendation 22 removed since no longer

applicable.
- Discussion paragraph 4.10.3 removed since text on WPA and the transition period no longer relevant.
- Discussion paragraph 4.11.2 updated and altered to reflect specification that WPA2/AES is the only standard and cipher permitted in the UK, although noting that in some countries mixed TKIP/AES environments may be encountered.
- Appendices updated.

2. Common Requirements and Recommendations

This section is concerned with the requirements that are common to all participants.

2.1. Participation

2.1.1. Requirements

1. All participating organisations MUST observe the requirements set out in section 2 of this document.
2. Participants that choose to participate as a Home organisation MUST observe the requirements set out in section 3 of this document.
3. Participants that choose to participate as a Visited organisation MUST observe the requirements set out in section 4 of this document.
4. Using the eduroam(UK) Support web portal, participating organisations MUST assert the type of service being provided or being worked towards and the current level of compliance of such a service with this Technical Specification. The current operational level of the service MUST also be asserted.

2.1.2. Recommendations

1. Participants SHOULD observe the recommendations set out in this document.

2.1.3. Discussion

Only members of the eduroam(UK) federation may participate and provide eduroam services in the UK and all members must abide by this Technical Specification.

A Visited service provider is one that makes available a network connectivity service for eduroam users. A Home organisation is one that provides an authentication service for its users. The two service types can be provided independently of each other.

It is anticipated that most organisations will participate as both a Visited and a Home service type provider; however participation as either Visited-only or Home-only is acceptable.

Although it is recommended that organisations participate as Visited organisations, it is not mandatory. This allows an organisation that may be unable or unwilling to act as a network access service provider (SP) to participate as a Home organisation and enable its own users to benefit from Visited services provided by other participants.

Participation as a Home organisation is not mandatory, although it is recommended. This permits an organisation that may be unable, unwilling or ineligible to act as an identity

provider (IdP) and provide an authentication service, to participate as a Visited organisation and offer visitors network access through eduroam.

Organisations may partially or wholly out-source provision of their Home or Visited services. In such situations the obligations of the participant to comply with this specification do not alter; therefore the terms of the agreement with the out-source provider should reflect this.

Alternatively, services may be provided (possibly on a commercial basis) in partnership with other organisations in which the partner organisation is an independent member of the eduroam(UK) federation, as would be the case where the partner operates its own RADIUS infrastructure and possibly authentication system, for instance on behalf of a group of small institutions. This can be described as the provision of a managed Visited or managed Home service.

2.2. Technical Contact

2.2.1. Requirements

5. Participants MUST designate a technical contact that can be contacted using e-mail and telephone during normal business hours. The contact may be either a named individual or an organisational unit. Arrangements must be made to cover for absence of a named technical contact owing to eventualities such as illness and holidays.

2.2.2. Discussion

A technical contact is required to facilitate the resolution of matters such as technical problems and abuse. Participants should ensure that changes in staff are promptly advised to eduroam(UK).

2.3. Logging

2.3.1. Requirements

6. Every log entry MUST state the date and time it was logged, derived from a reliable time source. The timestamp MUST be in UTC.
7. Logs MUST be kept for a minimum period of at least three months.

2.3.2. Discussion

Accurate logging is necessary for resolving technical problems and tracking abuse. The ability of a host to refer to a standard time is necessary for the production of logs that can be compared with logs maintained at other organisations. Jisc offers a Network Time Protocol [4] (NTP) service [5] that can be used for synchronising the clocks of hosts.

Whilst the minimum period for retention of logs is specified above, the maximum period is a matter for the organisation's general data protection compliance. It is recommended that raw logs should not be kept indefinitely and that six months is a commonly used threshold for deletion or anonymization. The Janet ‘Logfiles’ [6] technical guide provides further information and advice regarding logging and should be referred to for definitive recommendation on this matter.

2.4. RADIUS Hosts

2.4.1. Requirements

8. Participants’ RADIUS (Remote Authentication Dial In Service) clients and servers MUST comply with RFC 2865 [7] and RFC 2866 [8].
9. Participants’ RADIUS clients’ and servers’ clocks MUST be configured to synchronise regularly with a reliable time source
10. Participants MUST deploy at least one ORPS (organisational RADIUS proxy server).
11. Participants’ ORPSs, if operating a Home (IdP) service, MUST be reachable from the eduroam(UK) National RADIUS Proxy Servers (NRPS). ORPS SHOULD be configured to listen on UDP/1812 and SHOULD NOT be configured to listen on UDP/1645. ORPS using RadSec MUST be reachable from the NRPSs on TCP port 2083.
12. Participants using RadSec MUST use X.509 certificates provided by the GÉANT eduPKI service [9] to identify their ORPSs.
13. If the ORPS’s RADIUS implementations support it, both the NRPS and eduroam(UK) Support Server MUST be able to receive responses to Internet Control Message Protocol (ICMP) Echo Requests they send to participants’ ORPSs.
14. The following RADIUS attributes MUST be forwarded unaltered by participants’ ORPSs if present in RADIUS Access-Request, Access-Challenge, Access-Accept or Access-Reject messages.

    14.1. User-Name

    14.2. Reply-Message

    14.3. State

    14.4. Class

    14.5. Message-Authenticator

    14.6. Proxy-State

    14.7. EAP-Message

    14.8. MS-MPPE-Send-Key

    14.9. MS-MPPE-Recv-Key

    14.10. Calling-Station-Id

    14.11. Operator-Name

14.12. Chargeable-User-Identity

15. Participants' ORPSs MUST log all RADIUS authentication requests exchanged with the NRPS; the following information must be recorded.

    15.1. The value of the user name attribute in the request.

    15.2. The value of the Calling-Station-Id attribute in the request.

2.4.2. Recommendations

2. Participants SHOULD deploy a secondary ORPS.
3. Participants SHOULD NOT forward accounting messages to the NRPS.

2.4.3. Discussion

The ORPS is the interface between a participating organisation's network and the eduroam(UK) RADIUS proxy infrastructure. A secondary ORPS should be implemented to improve the resilience of the participant's service and by ensuring that a receptive ORPS is always online, to minimise RADIUS packet queuing on the NRPS.

The inclusion of spurious RADIUS attributes in packets exchanged between organisations can have unexpected effects and result in problems, it is therefore best practice to filter out unnecessary attributes. It is however essential that the key attributes detailed in this specification are not filtered and must be retained in forwarded packets.

RADIUS authentication typically uses port UDP/1812; port UDP/1645 is deprecated but is in occasional use and so whilst not recommended its use is also permitted.

Detailed logging of authentication requests and accounting requests if applicable is necessary for problem resolution and the tracking of network abuse. Note that the eduroam(UK) Policy (available from the Jisc eduroam website) states that Visited organisations have responsibilities in relation to the online activities of visitors, and consequently it is in the interests of the Visited service provider to ensure that this logging is accurate and complete.

The IP addresses of the NRPSs and the eduroam(UK) Support Server may be obtained by enquiry through the Janet Service Desk or DNS….

RADIUS accounting is not relevant in eduroam outside of participants' networks and receiving and responding to these by the NRPS consumes processing resources that could be better utilised. In addition, the configuration of ORPS to forward accounting messages to the NRPS represents unnecessary complication. Forwarding of accounting messages to the NRPS is therefore now deprecated and participants should check the configuration of their ORPS and remove such behaviour if found. The next release of this technical specification will include the mandatory requirement that ORPS MUST NOT forward accounting messages to the NRPS.

2.5. eduroam Service Information Website

2.5.1. Requirements

16. Participants MUST publish an eduroam service information website which MUST be generally accessible from the Internet and, if applicable, within the organisation to allow visitors to access it easily on site. The website MUST include the following information as a minimum.

16.1. The text of, or a link to, the participant's acceptable use policy (AUP), where applicable.

16.2. A link to the eduroam(UK) Policy [10].

16.3. The eduroam logo linking to the eduroam website [11].

16.4. The type of service offered where the scope of the eduroam service is limited, such as Visited-only or Home-only; and the operational status of the service if the web page is published before the service becomes operational.

16.5. A link to the eduroam(UK) sites listing and location web page [12].

2.5.2. Discussion

The participant's eduroam service information website is used to publish relevant information to help visitors and local users at the organisation connect to and make use of the participant's eduroam service.

Since users will have a reasonable expectation of being able to connect to eduroam wherever the eduroam SSID is broadcast, any limitation affecting users' ability to utilise the service, such as Visited-only and Home-only service types, must be advertised on the organisation's eduroam website.

Note that Visited organisations' eduroam service information websites are subject to further requirements; these are set out in that section of this specification.

3. Home Organisation Requirements and Recommendations

This section is concerned with the requirements pertaining to Home organisations.

3.1. User Names

3.1.1. Requirements

17. Home organisations' eduroam user names MUST conform to the Network Access Identifier (NAI) specification (RFC 4282 [13]), i.e. comprise identity name, @ and realm components.
18. The realm component MUST conclude with participant's realm name, which MUST be a domain name in the global Domain Name System (DNS) that the Home

organisation administers, either directly or by delegation.

3.1.2. Discussion

The purpose of the NAI is to specify a user name format for use within roaming services. Compliance with this requirement reduces the likelihood of problems arising from applications (such as RADIUS proxies) parsing user names in unexpected ways. Note that the use of privacy-preserving anonyms or pseudonyms is permitted, although care must be taken to ensure that the identity of the end user can always be established by the Home organisation.

One of the major elements of the eduroam ethos is that users should be able to connect to eduroam services in a seamless manner, without the user having to alter credentials in supplicant software. The requirement that only RFC 4282 compliant user names are permitted for use with eduroam, whether at the user's Home site or when roaming, ensures that users are more readily able to connect wherever an eduroam service is encountered.

3.2. Logging

3.2.1. Requirements

19. Home organisations MUST log all authentication attempts; the following information MUST be recorded.

    19.1. The time that the authentication request was received.

    19.2. The authentication result returned by the authentication database.

    19.3. The reason given, if any, if the authentication was denied or failed.

    19.4. User-Name in the outer-EAP and the User-Name from the inner-EAP (if a tunnelled EAP method is used).

    19.5. Chargeable-User-Identity (CUI) if one was generated.

    19.6. Calling-Station-ID.

    19.7. Operator-Name if one was present in Access-Request.

3.2.2. Discussion

Detailed logging of authentication is necessary for problem resolution and investigation of network abuse.

3.3. EAP Authentication

3.3.1. General Requirements

20. Home organisations MUST configure their RADIUS server to authenticate one or more Extensible Authentication Protocol [14] (EAP) types.
21. Home organisations MUST select an EAP type, or EAP types, for which their RADIUS

server will generate symmetric keying material for encryption ciphers and encapsulate the keys, following section 3.16 of RFC 3580 [15], within RADIUS Access-Accept packets.

3.3.2. Recommendations

4. Home organisations SHOULD choose a type, or types, that fulfil all or most of the ‘mandatory requirements’ section of RFC 4017 [16].

    4.1. The EAP types TLS [17], PEAP [18], and TTLS [19] are recommended.

3.3.3. Discussion

RFC 4017 defines requirements for EAP types used on IEEE 802.11 [20] LANs. While it is recommended that Home organisations select an EAP type (or types) that fulfils as many of these requirements as possible, it is mandatory that the ‘Generation of symmetric keying material’ requirement is met, and that the keys are returned in the RADIUS Access-Accept packet.

The Janet ‘Extensible Authentication Protocol’ [21] technical sheet provides further information on EAP.

3.4. Test Account

3.4.1. Requirements

22. If the Home organisation has chosen to support PEAP or TTLS type methods, the organisation MUST create an authenticatable test account and the relevant methods MUST be supported by the test account; additionally PAP may be used.
23. If the password for this account is changed then the eduroam(UK) Support web portal MUST be updated immediately to reflect this change. If it is believed the password has been compromised then the password MUST be changed immediately and the eduroam(UK) Support portal updated as soon as possible.

3.4.2. Recommendations

5. The test account SHOULD be created in the organisation’s primary user database. If more than one user database exists, it SHOULD be created in the user database that is likely to be most authenticated against.
6. Other privileges SHOULD NOT be assigned to the test account.
7. The test account SHOULD be configured to allow at least five consecutive failed authentication attempts without the account being locked.

3.4.3. Discussion

A test account is required for monitoring and test purposes by eduroam(UK) Support. The Support server monitoring system currently supports PEAP, TTLS methods and the method selected by the participating organisation should match the method most commonly used by the organisation. PAP may be configured for the test account as this is still supported by the

on-demand test. The credentials for the test account will only be known by eduroam(UK) Support and the Home organisation. The test account credentials are supplied to eduroam(UK) support via the eduroam(UK) Support web portal and should be updated there whenever changes are made.

3.5. User Security Awareness

3.5.1. Recommendations

8. Home organisations SHOULD educate their users to use protocols that provide appropriate levels of security when using eduroam.

3.5.2. Discussion

Home organisations should be mindful of the fact that their users' communications are forwarded over networks with unknown security characteristics, and so eduroam does not provide any guarantees regarding the privacy of this data.

3.6. RADIUS Hosts

3.6.1. Requirements

24. Home organisations MUST attempt to authenticate all authentication requests forwarded from the NRPS.

3.6.2. Recommendations

9. Where an authentication request is received from a NRPS, as opposed to being received from an internal RADIUS client or NAS, a Home organisation's Access-Accept reply SHOULD NOT contain dynamic VLAN assignment attributes, unless a mutual agreement is in place with the Visited organisation. This may be achieved by the Home organisation filtering out dynamic VLAN assignment attributes if present in Access-Accept packets sent to the NRPS.
10. If the Home RADIUS server supports Chargeable-User-Identity (CUI) then Access-Accept replies SHOULD contain the CUI attribute, where CUI is solicited in the authentication request from the Visited organisation, as described in RFC 4372 [22].

3.6.3. Discussion

It has been noticed that some participating organisations have applied filters to drop authentication requests where the NAS-Port-Type attribute does not match 'Wireless - IEEE 802.11' and/or Service-Type = 'Framed-User'. However some NASs do not send such attributes and there is no requirement to do so within this Technical Specification. All authentication requests forwarded by the NRPSs are valid and therefore must not be filtered.

4. Visited Organisation Requirements and Recommendations

This section is concerned with the requirements pertaining to Visited organisations.

The ‘base level engineering standards’ table below summarises and highlights the standards and features of greatest impact on users:

	SSID	***WPA/TKIP***	***WPA2/AES***	***NAT***	***Application Proxy***	***Port Restrictions***	***IPv6***
Compliance:	**eduroam**	**MUST NOT**	**MUST**	**MAY**	**MAY**	**MAY**	**SHOU**

In order to establish a development path for the service that will permit future improvements to be gradually introduced to the technical profile of the service, a dynamic ‘Advanced eduroam Service Engineering Components’ [23] web page is published on the Jisc Community website which evolves over time. The planned changes described on that page will be migrated into the base level engineering standards table and this technical specification in future versions over time. This will give the community as much notice as possible of planned changes and will provide a target set of technical standards for participants to aim for.

4.1. Network Presentation

4.1.1. Requirements

25. Visited organisations MUST implement the base level engineering standards defined in this specification.
26. Visited organisations MUST ensure that is not possible for a non-eduroam service to be mistaken by visitors for the participant’s eduroam service.
27. The word ‘eduroam’ MUST NOT be used in an SSID for a non-compliant network.
28. Visited organisations’ eduroam networks MUST NOT be shared with any other network service.
29. Visited organisations that provide access to eduroam for local users, or visitors from organisations not participating in eduroam, MUST ensure that the user has the opportunity to read and has agreed to the eduroam(UK) Policy.
30. Visited organisations MUST NOT offer visitors any wireless media other than IEEE 802.11.

4.1.2. Recommendations

11. Where possible Visited organisations SHOULD implement the enhanced features/advanced level engineering standards in preference to the base engineering standards for their eduroam networks.

4.1.3. Discussion

The base level engineering standards is intended to be the standard technical level that participants deploy. The enhanced features/advanced level provides a higher specification

network environment and it is hoped that Visited organisations will work towards its implementation.

Some participants may wish to deploy a non-eduroam wireless service, in addition to an eduroam service. For example, a participant’s own users may require access to a wireless network that should remain inaccessible to visitors. Participants may offer such services; for example, by using another Service Set Identifier (SSID). However, visitors should not be able to confuse these services with the participant’s eduroam service.

Note that it is permissible for a participant to place their own users onto a network which does not comply with eduroam policy (e.g. one which has greater port/protocol restrictions), even if they have connected to an SSID bearing the name ‘eduroam’; it is not permissible to do this to visitors.

It is anticipated that organisations will use VLAN technology to segregate networks; however, this is not mandatory and participating organisations may choose to realise the necessary segregation through other means (such as physical isolation).

While it is anticipated that IEEE 802.11 will be the dominant access media for eduroam, participants are permitted to use other media, such as wired Ethernet, providing that the other technical requirements are adhered to. With the same proviso, the mixing of media on the same network is also permitted.

At present this specification prohibits the use of non-IEEE 802.11 wireless media, such as Bluetooth, because their suitability for eduroam has not yet been adequately explored. These media may be considered for inclusion in subsequent revisions of this specification if interest in their use is expressed.

4.2. RADIUS Forwarding

4.2.1. Requirements

31. Visited organisations MUST forward RADIUS requests originating from eduroam Network Access Servers (NASs) which contain user names with non-local realms to a NRPS via an ORPS. A non-local realm name is defined as one that is neither associated with the participant nor the participant's partner where a service is provided in partnership with another organisation. Requests containing local realm names (those associated with the participant or partner organisation) MUST NOT be forwarded to the NRPS.

    31.1. RADIUS Access-Requests MUST be sent to port UDP/1812.

    31.2. Access-Requests using RadSec MUST be sent to port TCP/2083.

32. Visited organisations MUST NOT forward requests containing user names which do not include a realm nor any which are non-NAI compliant.
33. Visited organisations MUST NOT forward requests that have originated from NASs that do not conform to the requirements of this specification.
34. Visited organisations MAY configure additional realms to forward requests to other internal RADIUS servers, but these realms MUST NOT be derived from any domain in

the global DNS that the participant or a partner organisation does not administer.

35. Visited organisations MAY configure additional realms to forward requests to external RADIUS servers in other organisations, but these realms MUST be derived from domains in the global DNS that the participating organisation or partner organisation administers (either directly or by delegation).
36. In situations where a participating organisation is in partnership with another participating organisation to provide managed Visited services at sites belonging to the partner and where that partner operates its own Home service, the managed Visited service provider MUST forward requests containing user names with a realm associated with the partner directly to the RADIUS server of that partner and MUST NOT forward those requests to the NRPS.
37. In situations where the organisation providing the managed Visited service is also working as a partner with further participating organisations, the Visited organisation MUST ensure that requests originating from a managed site of such an organisation are NOT forwarded to any other partner.
38. Visited organisations MUST NOT otherwise forward requests directly to other eduroam participants.
39. If an ORPS is not capable of responding correctly to a Status-Server request then the setting to enable Status-Server on the Support server for that ORPS MUST NOT be enabled.

4.2.2. Recommendations

12. Visited organisations SHOULD configure their ORPS to load balance between the NRPS servers.
13. Visited organisations MAY configure their ORPS to fail-over between the NRPS servers.

    13.1. If the fail-over algorithm has a configurable timer that specifies the length of time after which an unresponsive server is considered unreachable, this timer SHOULD be configured to zero seconds (or as low a value as possible).

14. Visited organisation SHOULD configure their ORPS to insert the Operator-Name attribute, accurately composed for their realm, into all Access-Request packets forwarded to the NRPS.
15. Visited organisations SHOULD request Chargeable-User-Identity (CUI) in Access-Request packets forwarded to the NRPS if CUI is supported by the ORPS.
16. If an ORPS is capable of using Status-Server (RADIUS Code 12) to detect the operational state of the NRPS, then it SHOULD be configured to do so.
17. If an ORPS is capable of being queried by Status-Server then that functionality SHOULD be enabled so that the NRPS are able to make a more informed decision on the operational status of the ORPS.

4.2.3. Discussion

eduroam(UK) is part of the eduroam confederation, which consists of organisations holding domain names derived from many of the top level Domain Name Service (DNS) [24] domains. Consequently it is necessary to ensure that the RADIUS realm and DNS name-spaces remain congruent; otherwise, RADIUS requests may not be routed correctly.

It is not permissible to use the NRPS as a general-purpose authentication system. At the

present time, only NASs that conform to the requirements of this specification may use the NRPS.

With the emergence of partnerships between organisations wherein one provides an eduroam service for another through a formal agreement (which may be commercially based) and where both partners are full members of the eduroam(UK) federation, the issue of routing of RADIUS messages has needed clarification. Such a situation exists for instance where a contracted organisation provides a managed network at a hall of residence for another or for a group of other organisations. This can be described as the provision of a managed Visited service. Where both organisations operate RADIUS servers which are peered with the national proxies, the potential exists for the routing of all requests to the NRPS, including those for users from the partnered organisation. This would effectively turn the NRPS into an off-campus relay for a large proportion of an organisation's home users, a task for which the NRPS were never designed.

This technical specification now includes rules governing routing of such RADIUS messages; requests arising from users who are members of the partnered organisation must be routed directly to the partner's ORPS and not to the NRPS. In cases where the managed service provider at a particular site provides services to more than one partner, requests arising from users of the other partner organisations at that managed site must still be forwarded to the NRPS as per Requirement 32; i.e. bypassing the NRPS for authentications between partner organisations is prohibited. This is to avoid the creation of hidden mini-eduroam proxy infrastructures.

Note; this does not proscribe inter-organisation authentication between members of an association of co-operating organisations in which the individual organisations are not members of eduroam(UK) in their own right. In such cases the organisations may share a common top level/association level realm name, such as would be the case where a number of small institutions are managed by a collegiate university, association or local authority and where that association or local authority is a member of the eduroam(UK) federation and provides eduroam services throughout the association.

Chargeable-User-Identity attribute is useful in troubleshooting and its use is included in the GÉANT GN4 research project. When a Visited organisation sets a NUL character in a CUI attribute included an Access-Request, the Home organisation's RADIUS server, if it supports CUI, can (and should be configured to) return an identifier (although not necessarily the identity), of the user via CUI in the Access-Accept to the Visited organisation ORPS. The values of CUI may be included in RADIUS logs.

4.3. NAS Requirements

4.3.1. Requirements

40. NASs MUST implement IEEE 802.1X [25] authentication.
41. On receipt of a RADIUS Access-Accept, the NAS and network MUST immediately forward traffic to, and from, the visitor according to the requirements set out in section 4.5; no form of local authorisation is permitted that would deny this to the visitor except in the case where network abuse has been detected.
42. Wireless IEEE 802.11 NASs MUST support symmetric keying using keys provided by the Home organisation within the RADIUS Access-Accept packet, in accordance with

section 3.16 of RFC 3580.

43. A NAS port MUST NOT connect more than one user unless the NAS is not capable of being configured other than to use the same port for the connection of multiple users and the NAS maintains client traffic separation by other means.
44. All NASs that are deployed by Visited organisations to support eduroam MUST include the following RADIUS attributes within Access-Request packets.

    44.1. Calling-Station-ID attribute containing the supplicant's MAC address.

    44.2. NAS-IP-Address attribute containing the NAS's IP address.

4.3.2. Discussion

When version 1.0 of this specification was written the NAS was the self-contained individual AP. The requirement was to avoid having two or more users on the same NAS port because that reduced the security context since users technically could communicate with each other without authenticating to the NAS. This is not permissible. In version 1.0, each visitor was required to have a unique port on a NAS that supported IEEE 802.1X. However with modern wireless controller equipment the NAS is the controller which in most implementations just uses a single port. Security relies on client traffic being separated internally by the controller. The requirement has been changed to permit use of wireless controller equipment. Note that this restriction may prohibit the use of some gateway devices that provide IEEE 802.1X authentication to multiple users over a single NAS port.

The Janet 'IEEE 802.1X' [26] technical sheet provides further information on IEEE 802.1X.

Knowledge of supplicants' MAC and NAS's IP addresses allows detailed logging of authentication and accounting that is necessary for problem resolution, the tracking of network abuse and trend analysis.

The use of other network access control technologies that restrict a visitor's connection to the network is not permitted.

4.4. Securing Host Network Configuration

4.4.1. Recommendations

18. Visited organisations SHOULD configure the network to prevent a visitor from masquerading as an authorised Dynamic Host Configuration Protocol (DHCP) [27] server or router.

4.4.2. Discussion

A visitor's client, once authenticated, requires information about the visitor network. DHCP and Address Resolution Protocol (ARP) are used for this purpose in IPv4; DHCPv6 and Neighbourhood Discovery (ND) in IPv6. However, most implementations of these protocols do not provide a mechanism for authenticating the sender. Hence, a concern arises from the introduction of devices that act as 'rogue routers'.

Such a router can perform a man-in-the-middle attack by issuing DHCP responses, gratuitous ARP requests or ND Router Advertisements (RA) that indicate that it is the default gateway for

the network. All of the client's subsequent communications are sent to the rogue router. It might also forward them on to a masquerading target such as a faked banking service.

While there are no standards that address this problem directly for IPv4, most vendors have implemented proprietary solutions which participants should use, if available, to prevent the abuse of ARP, DHCP and RAs. Standards that address this problem exist for IPv6 but these have yet to be implemented widely by vendors.

4.5. IP Forwarding

4.5.1. Requirements

45. Visited organisations MAY implement IPv4 and IPv6 filtering between the visitor network and other networks, providing that this permits the forwarding of the following mandatory protocols to external networks.

45.1 IPv6 Tunnel Broker NAT traversal:	UDP/3653;TCP/3653 egress and established.
45.2 IPv6 Tunnel Broker Service:	IP protocol 41 egress and established.
45.3 IPSec NAT traversal:	UDP/4500 egress and established.
45.4 Cisco IPSec NAT traversal:	UDP/10000; TCP/10000 egress and established.
45.5 PPTP:	IP protocol 47 (GRE) egress and established; TCP/1723 egress and established.
45.6 OpenVPN:	UDP/1194; TCP/1194 egress and established.
45.7 NTP:	UDP/123
45.8 SSH:	TCP/22 egress and established.
45.9 HTTP:	TCP/80 egress and established.
45.10 HTTPS:	TCP/443 egress and established.
45.11 LDAPS:	TCP/636 egress and established.
45.12 IMSP:	TCP/406 egress and established.
45.13 IMAP4:	TCP/143 egress and established.
45.14 IMAP3:	TCP/220 egress and established.
45.15 IMAPS:	TCP/993 egress and established.
45.16 POP3S:	TCP/995 egress and established.

45.17 Passive (S)FTP:	TCP/21 egress and established.
45.18 SMTPS:	TCP/465 egress and established.
45.19 Message submission:	TCP/587 egress and established.
45.20 RDP:	TCP/3389 egress and established.
45.21 VNC:	TCP/5900 egress and established.
45.22 Citrix:	TCP/1494 egress and established.
45.23 AFS:	UDP/7000 through UDP/7007 inclusive.
45.24 ESP:	IP protocol 50 egress and established
45.25 AH:	IP protocol 51 egress and established
45.26 ISAKMP and IKE:	UDP/500.
45.27 SQUID Proxy:	TCP/3128 egress and established
45.28 HTTP Proxy:	TCP/8080 egress and established

4.5.2. Recommendations

19. Visited organisations MAY implement arbitrary IP filtering of packets addressed to other hosts on the Visited organisation's own network.

20. Visited organisations SHOULD provide visitors with unimpeded access to the Internet and *vice versa*, where local policy permits.

4.5.3. Discussion

An important aim of eduroam(UK) is to provide visitors with unimpeded access to Janet and the Internet. This maximises the probability of a visitor's applications working as expected, thereby improving the visitor's experience of the service and reducing the support burden on the Home organisation.

However, participants may wish to implement some filtering of IP traffic entering and leaving the visitor network. For example, a participant may wish to limit the usage of bandwidth by potentially demanding applications, and so forth. This is permitted provided that the filtering policy allows the forwarding of the protocols laid out above.

Content filtering, whilst deprecated on eduroam networks, is permitted. If content filtering is implemented, this must be stated on the organisation's eduroam information website.

Filtering of packets addressed to other hosts on the Visited organisation's own internal network is permitted.

4.6. Application and Interception Proxies

4.6.1. Requirements

46. Visited organisations deploying application or ‘interception’ proxies on their eduroam network MUST publish this fact on their eduroam service information website.
47. If an application proxy is not transparent, the Visited organisation MUST also provide documentation on the configuration of applications to use the proxy.
48. Transport Layer Security (TLS)/Secure Sockets Layer (SSL) interception proxies MUST NOT be used for eduroam visitors.

4.6.2. Recommendations

21. Visited organisations SHOULD NOT deploy application or ‘interception’ proxies on the eduroam network.

4.6.3. Discussion

Applications commonly require special configuration to use a proxy, which reduces usability and may increase the support burden. The presence of a proxy may also break some applications. Likewise ‘interception’ proxies, often used by intrusion and virus detection systems, may result in the user experiencing unexpected network behaviour. A TLS/SSL interception proxy represents an unacceptable security risk and breach of user privacy.

Whilst TLS interception proxies are not permitted on the eduroam network onto which visitors are connected, at the home site organisations may connect their own users to non-eduroam network services to which this requirement does not apply.

4.7. eduroam Service Information Website

4.7.1. Requirements

49. In addition to the requirements detailed in section 2.5, Visited organisations’ eduroam information websites MUST state:

    49.1. Sufficient information to enable visitors to identify and access the service; at a minimum this must include the locations covered.

    49.2. Where applicable, the information specified in section 4.6 regarding application and interception proxies.

4.7.2. Recommendations

12. Visited organisations SHOULD ensure that their eduroam information website is accessible using small form-factor devices.

13. Visited organisations MAY publish the IP forwarding policies imposed on the visitor network.

4.7.3. Discussion

Publishing the IP forwarding policies imposed on the visitor network may assist Home organisations in supporting their users without needing to contact local support staff at the Visited organisation.

4.8. SSID

4.8.1. Requirements

50. Operational eduroam Wi-Fi services, as described in this specification, MUST use a broadcast SSID of ‘eduroam’ in lower case characters only.
51. Organisations that are in the process of developing Home or Visited services but are not yet offering operational services MUST limit broadcast of the ‘eduroam’ SSID to small development environments.

4.8.2. Discussion

Since users have a reasonable expectation of being able to connect to eduroam wherever the eduroam SSID is visible, during the development stage of implementing eduroam when an operational service is not available at an organisation, the possibility of users detecting a broadcast eduroam SSID must be minimised.

4.9. Network Addressing

4.9.1. Requirements

52. eduroam networks MAY make use of NAT.
53. Visited organisations MUST allocate IPv4 addresses to visitors using DHCP.
54. Visited organisations MUST log the IPv4 addresses allocated to visitors and the corresponding MAC addresses.
55. Visited organisations MUST log NAT address mappings, if NAT is used as part of an eduroam implementation.

4.9.2. Discussion

The DHCP server logs are required to enable participants to correlate DHCP leases to users.

4.9.3. Recommendations

24. As part of the enhanced features/advanced level standard, participants are recommended to implement IPv6 and allow routing of IPv6 on the eduroam network.

4.9.4. Discussion

IPv6 is the next generation Internet Protocol. Increasing adoption of IPv6 by service providers means that there is a benefit to participants in offering IPv6 connectivity to visitors. It is strongly recommend that visited sites implement IPv6 wherever possible. This recommendation is included in the enhanced features/advanced level specification published on the Community library web pages.

4.10. WPA

4.10.1. Requirements

56. The WPA specification MUST NOT be supported and the TKIP algorithm MUST NOT be employed in eduroam services.

4.11. WPA2

4.11.1. Requirements

57. Both established and new deployments of eduroam Visited Wi-Fi services MUST implement WPA2 Enterprise with the use of the CCMP (AES) algorithm.

Discussion

WPA2 Enterprise is the Wi-Fi Alliance's interoperability compliance certification scheme for IEEE 802.11 security features. This is regarded as the strongest WLAN security specification available.

WPA2 Enterprise is mandatory for eduroam services, as it contributes towards a higher security context and it is has been the only permitted standard in the UK since the beginning of 2015.

Support for legacy WPA/TKIP deployments within mixed TKIP/AES environments is however still permitted in some other countries, so eduroam users may encounter this standard/cipher when roaming. Note, services that only support WPA/TKIP should never be experienced, therefore there is no need for clients to be set up with configurations that support both WPA/TKIP and WPA2/AES and there is a positive advantage in not implementing such configuration.

The Wi-Fi Alliance specifies both WPA2 and WPA2 with Protected Management Frames (WPA2 with PMF). Currently there is no requirement regarding which WPA2 standard must be used (WPA2 or WPA2 with PMF) for eduroam. However, participants deploying WPA2 with PMF should be aware this may cause interoperability issues with clients which are not certified for WPA2 with PMF.

Links

[1] https://community.jisc.ac.uk/groups/eduroam/document/eduroamuk-technical-specification-v14