eduroam(MD) Technical Specification

Version 1
19 January 2015

Originator: Alexandru Cacean (Based on eduroam.uk documents)

1. Introduction

1.1. Acknowledgements

The authors would like to acknowledge that this document is made based on UK eduroam policy elaborated by Janet for their members. The original source can be found here https://community.ja.net/library/janet-services-documentation/eduroamuk-technical-specification

1.2. Overview

This document is the Technical Specification for the eduroam service provided in the MD by RENAM. It complies with the requirements mandated by the GÉANT eduroam service. This document is subject to periodic revision; changes will be notified to registered contacts at participating organisations and to the community via the RENAM eduroam website, at which the most recent revision will be found.

1.2.1. Using this Document

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

This document consists of for sections. The first ('Introduction') is for informational purposes only. The latter section contains four appendices: two summaries of the requirements and recommendations laid out in this document.

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.

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

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. 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.

2.1.2. Recommendations

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

2.1.3. Discussion

Only members of the eduroam(MD) federation may participate and provide eduroam services in the MD 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(MD) 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

4. 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.

2.3. Logging

2.3.1. Requirements

5. Every log entry MUST state the date and time it was logged, derived from a reliable time source. The timestamp MUST be in GMT.

6. 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.

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.

2.4. RADIUS Hosts

2.4.1. Requirements

7. Participants' RADIUS (Remote Authentication Dial In Service) clients and servers MUST comply with RFC 2865 and RFC 2866.

8. Participants' RADIUS clients' and servers' clocks MUST be configured to synchronise regularly with a reliable time source

9. Participants MUST deploy at least one ORPS (organisational RADIUS proxy server).

10. Participants' ORPSs MUST be reachable from the eduroam(MD) RADIUS Proxy Servers (NRPS) on either port UDP/1812 and port UDP/1813 (recommended), or port UDP/1645 and port UDP/1646 (if required by the participating Organisation). ORPS using RadSec MUST be reachable from the NRPSs on TCP port 2083.

11. Participants using RadSec MUST use X.509 certificates provided by the GÉANT eduPKI service to identify their ORPSs.

12. If the ORPS's RADIUS implementations support it, both the NRPS and eduroam(MD) Support Server MUST be able to receive responses to Internet Control Message Protocol (ICMP) Echo Requests they send to participants' ORPSs.

13. The following RADIUS attributes MUST be forwarded by participants' ORPSs if present in RADIUS Access-Request, Access-Challenge, Access-Accept or Access-Reject messages.

13.1. User-Name

13.2. Reply-Message

13.3. State

13.4. Class

13.5. Message-Authenticator

13.6. Proxy-State

13.7. EAP-Message

13.8. MS-MPPE-Send-Key

13.9. MS-MPPE-Recv-Key

13.10. Calling-Station-Id

13.11. Operator-Name

13.12. Chargeable-User-Identity

14. The following RADIUS attributes MUST be forwarded by participants' ORPSs if present in RADIUS Accounting messages.

14.1. User-Name

14.2. Acct-Status-Type

14.3. Acct-Session-ID

14.4. Proxy-State

14.5. Class

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.

16. Participants MUST log all RADIUS accounting requests exchanged with the NRPS; the following information must be recorded.

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

16.2. The value of the accounting session identifier.

16.3. The value of the request's accounting status type.

2.4.2. Recommendations

2. Participants SHOULD deploy a secondary ORPS.

2.4.3. Discussion

The ORPS is the interface between a participating organisation's network and the eduroam(MD) 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 and accounting typically use ports UDP/1812 and UDP/1813 respectively.

Detailed logging of authentication and accounting requests is necessary for problem resolution and the tracking of network abuse. Note that the eduroam(MD) Policy (available from the RENAM 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(MD) Support Server may be obtained by enquiry through the RENAM Service Desk.

2.5. eduroam Service Information Website

2.5.1. Requirements

17. 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.

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

17.2. A link to the eduroam(MD) Policy.

17.3. The eduroam logo linking to the eduroam.org website.

17.4. 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.

17.5. A link to the eduroam(MD) sites listing and location web page.

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

18. Home organisations' eduroam user names MUST conform to the Network Access Identifier (NAI) specification (RFC 4282), i.e. comprise identity name @ and realm components.

19. 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

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

20.1. The time that the authentication request was received.

20.2. The authentication result returned by the authentication database.

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

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

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

20.6. Calling-Station-ID.

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

21. Home organisations MUST configure their RADIUS server to authenticate one or more Extensible Authentication Protocol (EAP) types.

22. 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, within RADIUS Access-Accept packets.

3.3.2. Recommendations

3. Home organisations SHOULD choose an EAP type, or types, that fulfil all or most of the 'mandatory requirements' section of RFC 4017.

3.1. The EAP types TLS, PEAP, and TTLS are recommended.

3.3.3. Discussion

RFC 4017 defines requirements for EAP types used on IEEE 802.11 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.

3.4. Test Account

3.4.1. Requirements

23. Home organisations MUST create an authenticatable test account. If the Home organisation has chosen to support PEAP or TTLS type methods, these MUST be supported by the test account, else PAP may be used.

24. eduroam Support MUST be informed immediately if the password for this account is changed. However, if it is believed that the password has been compromised then the password MUST be changed immediately and eduroam(MD) Service Support informed as soon as possible.

3.4.2. Recommendations

4. 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.

5. Other privileges SHOULD NOT be assigned to the test account.

6. The test account SHOUD 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(MD) Support. The credentials for the test account will only be known by eduroam(MD) Support and the Home organisation.

3.5. User Security Awareness

3.5.1. Recommendations

7. 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(MD) does not provide any guarantees regarding the privacy of this data.

3.6 RADIUS Hosts

3.6.1 Requirements

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

3.6.2 Recommendations

8. 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.

9. Home organisations SHOULD respond with a Chargeable-User-Identity (CUI) attribute in an Access-Accept, if the Home RADIUS server supports CUI, where CUI is solicited in the authentication request from the Visited organisation, as described in RFC 4372.

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 '802.11'. However some NASs do not send a NAS-Port-Type attribute 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.

Here we provided a set of best practice technical standards that participants could aspire to.

A 'base level engineering standards' table of features most interest to users are follows:

	SSID	***WPA***	***WPA2***	***NAT***	***Application Proxy***	***Port Restrictions***	***IPv6***	***Injection of O-N***
Compliance:	**eduroam**	**MAY**	**MUST**	**MAY**	**MAY**	**MAY**	**MAY**	**SHOULD**

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, an 'enhanced features/advanced level engineering standards' precursor table will be developed and will be published on the RENAM eduroam website as it evolves. The standards defined in this table will be migrated into the base level engineering standards table 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

26. Visited organisations MUST implement the base level engineering standards defined in this specification.

27. Visited organisations MUST ensure that is not possible for a non-eduroam service to be mistaken by visitors for the participant's eduroam service.

28. The word 'eduroam' MUST NOT be used in an SSID for a non-compliant network.

29. Visited organisations' eduroam networks MUST NOT be shared with any other network service.

30. Visited organisations that provide access to eduroam for local users, or visitors from organisations not participating in eduroam, MUST ensure that the user has read and agreed to the eduroam(MD) Policy.

31. Visited organisations MUST NOT offer visitors any wireless media other than IEEE 802.11.

4.1.2. Recommendations

10. 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 to place local users on 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 FastEthernet, 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

32. 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.

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

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

32.3. RADIUS Accounting-Requests MUST be addressed to port UDP/1813.

32.4. Accounting-Requests using RadSec MUST be sent to port TCP/2083.

33. Visited organisations MUST NOT forward requests containing user names which do not include a realm nor any which are non-NAI compliant.

34. Visited organisations MUST NOT forward requests that have originated from NASs that do not conform to the requirements of this specification.

35. 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.

36. 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).

37. 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.

38. 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.

39. Visited organisations MUST NOT otherwise forward requests directly to other eduroam participants.

4.2.2. Recommendations

11. Visited organisations SHOULD configure their ORPS to load balance between the NRPS servers.

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

12.1. 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).

13. 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.

14. Visited organisations SHOULD request Chargeable-User-Identity (CUI) in Access-Request packets forwarded to the NRPS if CUI supported by the ORPS.

4.2.3. Discussion

eduroam(MD) is part of the eduroam confederation, which consists of organisations holding domain names derived from many of the top level Domain Name Service (DNS) 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.

Chargeable-User-Identity attribute is useful in troubleshooting and its use is included in the Géant SRA-3 research programme. 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 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 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

In 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 permits 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.

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

15. Visited organisations SHOULD configure the network to prevent a visitor from masquerading as an authorised Dynamic Host Configuration protocol (DHCP) 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 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 external networks, providing that this permits the forwarding of the following mandatory protocols.

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;

UDP/5000-5110 egress and established

45.7. NTP: UDP/123 egress and established

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. LDAP: TCP/389 egress and established.

45.12. LDAPS: TCP/636 egress and established.

45.13. IMSP: TCP/406 egress and established.

45.14. IMAP4: TCP/143 egress and established.

45.15. IMAP3: TCP/220 egress and established.

45.16. IMAPS: TCP/993 egress and established.

45.17. POP: TCP/110 egress and established.

45.18. POP3S: TCP/995 egress and established.

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

45.20. SMTPS: TCP/465 egress and established.

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

45.22. RDP: TCP/3389 egress and established.

45.23. VNC: TCP/5900 egress and established.

45.24. Citrix: TCP/1494 egress and established.

45.25. AFS: UDP/7000 through UDP/7007 inclusive egress and established.

45.26. ESP: IP protocol 50 egress and established

45.27. AH: IP protocol 51 egress and established

45.28. ISAKMP: and IKE: UDP/500 egress

45.29. SQUID Proxy: TCP/3128 egress and established

45.30. HTTP Proxy: TCP/8080 egress and established

4.5.2. Recommendations

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

17. Visited organisations SHOULD provide visitors with unimpeded access to RENAM, and *vice versa*, where local policy permits.

4.5.3. Discussion

An important aim of eduroam(MD) is to provide visitors with unimpeded access to RENAM 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.

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

Arbitrary filtering of packets addressed to other hosts on the Visited organisation's own 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.

4.6.2. Recommendations

18. 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.

4.7. eduroam Service Information Website

4.7.1. Requirements

48. In addition to the requirements detailed in section 2.5, Visited organisations' eduroam service information websites MUST state:

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

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

4.7.2. Recommendations

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

20. 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

49. A broadcast SSID of 'eduroam' in lower case characters only MUST be used for operational eduroam wireless network services as described in this specification.

50. 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

Windows XP is unable to authenticate against a non-broadcast SSID offering IEEE 802.1X where a visible alternative broadcast SSID is available. Such a situation is likely in most environments, therefore in order to ensure service provision for XP broadcast of the eduroam SSID is required.

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

51. eduroam networks MAY make use of NAT.

52. Visited organisations MUST allocate IPv4 addresses to visitors using DHCP.

53. Visited organisations MUST log the IPv4 addresses allocated to visitors and the corresponding MAC addresses.

54. 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

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

4.9.4. Discussion

IPv6 is the next generation Internet Protocol. IPv6 is likely to be critical for supporting the large number of mobile devices, such as WLAN-capable mobile telephones, that may become common in the near future.

While IPv6-enabled services are not widely deployed at present, some Home organisations have already deployed them and therefore visitors from these participants would benefit.

4.10. WPA

4.10.1. Requirements

55. Existing eduroam deployments MAY provide WPA with the use of the TKIP algorithm until the end of December 2015.

4.10.2. Recommendations

22. All networks supporting WPA with the use of the TKIP algorithm should phase out such support as soon as possible and certainly no later than December 2015. WPA2 with the AES algorithm is the recommended cipher for use on eduroam networks.

4.10.3. Discussion

WPA is a specification from the Wi-Fi Alliance that implements a subset of IEEE 802.11i. WPA only implements those parts of IEEE 802.11i that are compatible with all IEEE 802.11b clients, thereby allowing these clients to be upgraded to WPA with a firmware update. The majority of vendors have provided a firmware update. WPA is regarded as secure, although not as secure as WPA2. TKIP is considered not secure.

WPA2 is now mandatory for eduroam networks. Use of WPA will be permitted for a transition period to allow those organisations that have older legacy network equipment that does not support WPA2 to offer a service whilst migrating to equipment that supports the latest standard.

4.11. WPA2

4.11.1. Requirements

56. Visited organisations' eduroam networks MUST implement WPA2 with the use of the CCMP (AES) algorithm. New organisations joining eduroam MUST only implement WPA2/AES.

4.11.3. Discussion

WPA2 is the Wi-Fi Alliance's more complete profile of IEEE 802.11i. This is regarded as the strongest WLAN security specification available.

WPA2 is mandatory for the eduroam network, as it contributes towards a higher security context.