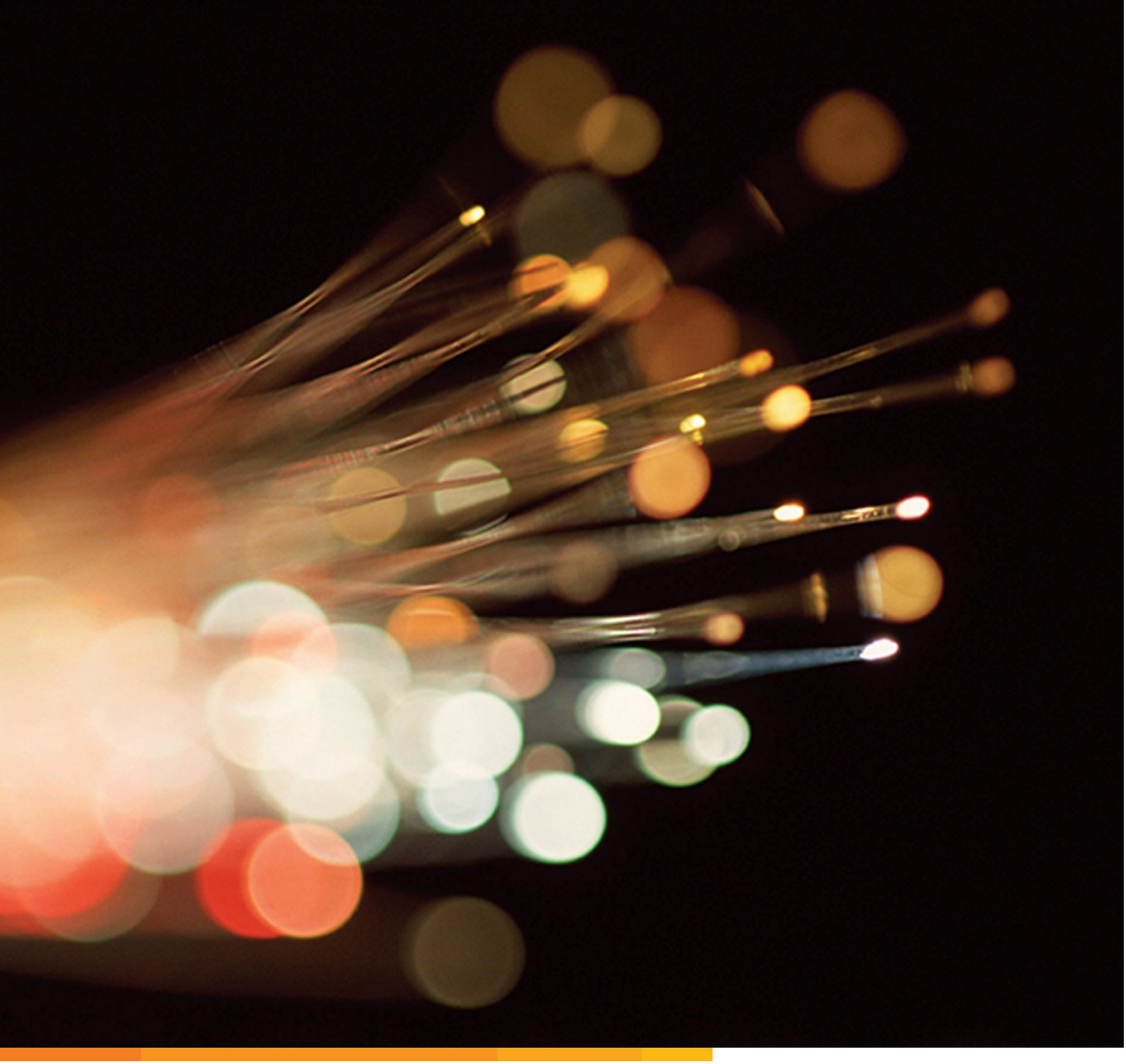

eduroam AU Technical Specifications

aarnet
Australia's Academic and Research Network

eduroam

Contents

1 Introduction

1.1 Acknowledgements

This eduroam AU technical specification is based on the JISC (UK) eduroam technical specification [1]. Our thanks go to JISC for being a consistently reliable source of high-quality eduroam documentation.

1.2 Overview

This document is the Technical Specification for the “eduroam AU” service which enables Australian institutions to participate in the global eduroam service. AARNet Pty Ltd is the “National Roaming Operator” (NRO) for eduroam AU.

This Technical Specification complies with the requirements mandated by the eduroam AU Policy [2] , which in turn reflects requirements in the eduroam Compliance Statement (eCS) [3] , which serves as the eduroam Global Policy which NROs must sign up to.

This document is subject to periodic revision; changes will be notified to designated institutional eduroam contacts, and to the eduroam AU institutional participant and user community in general via AARNet’s eduroam AU website [4], where the most recent revision will be made available.

1.3 Using this Document

This document uses the conventions specified in RFC2119 [5] 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 institutions.

Section 3 (‘Identity Provider Requirements and Recommendations’). This section is concerned with the requirements for Identity Providers (IdPs), and primarily those relating to authentication of users.

Section 4 (‘Service Provider Requirements and Recommendations’). This section is concerned with the requirements for Service Providers (SPs), and primarily those relating to the eduroam network provided by SP institutions.

2 Common Requirements and Recommendations

This section is concerned with the requirements that are common to both IdP and SP participants.

2.1 Participation

2.1.1 Requirements

1. All participating institutions MUST observe the requirements set out in section 2 of this document.
2. Institutions that participate as an Identity Provider MUST observe the requirements set out in section 3 of this document.
3. Institutions that participate as a Service Provider MUST observe the requirements set out in section 4 of this document.
4. Institutions MUST assert, via the eduroam AU AdminTool [7], the type of service being provided or being worked towards (IdP+SP, SP-Only, IdP-Only) and the current operational level of the service (Pre-Production and Production).
5. When using a 3rd-party provider for deployment of an eduroam service, the terms of the IdP and/or SP institution's agreement with the out-source provider MUST reflect requirements and recommendations of this technical specification.

2.1.2 Recommendations

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

2.1.3 Discussion

The global eduroam service enables a user engaged in research and/or education ('end-user') to gain access to the "eduroam" network provided by a visited institution ('service provider', SP) by virtue of the user's remote authentication by the user's home institution ('identity provider', IdP).

The main value propositions of participation in and use of eduroam, from institutional (IdP, SP) and user perspectives respectively, are security, scalability, ease-of-use, and accountability. Adherence to this technical specification by participating institutions enables these value propositions to be delivered.

A Service Provider (SP) is an institution that makes available an IEEE 802.1x network service identified as "eduroam" (e.g. Wi-Fi network SSID) for visiting users. An Identity Provider (IdP) is an institution that provides a remote IEEE 802.1x authentication service for its users. The two service types can be provisioned independently of each other.

Network costs for eduroam are borne by Service Providers, hence it is recommended that any institution seeking to operate as an Identity Provider also participates as a Service Provider ('giving' as well as 'taking' in the context of the global eduroam service).

Participating as an SP is not mandatory. If an IdP-eligible institution (i.e. users engaged in R&E) satisfies 'exceptional circumstances' (e.g. eduroam SP coverage already provided by another institution, or providing an eduroam network is of negligible value to the eduroam user community), it will be given approval for IdP-only participation, enabling its users to benefit from eduroam network services provided by SP participants.

Participation as an IdP is not mandatory, however is recommended if the institution satisfies eligibility requirements for its users (i.e. engaged in R&E). SP-only participation is commonly delivered where a business case exists for R&E users to access an eduroam network provided by the institution (e.g. Health services institutions providing training/experience to visitors from educational institutions). To promote utility of eduroam AU, AARNet encourages health, library, gallery, museum, artistic, and other public space Wi-Fi providers to operate as a an SP-only participant and offer R&E visitors "eduroam" network access by virtue of remote authentication via eduroam infrastructure.

Institutions may partially or wholly out-source provision of their IdP or SP services to a 3rd-party. In this case, the obligations of the participant institution to comply with this technical specification do not alter, hence the institution must convey requirements to the 3rd-party to ensure compliance.

Deployment services may be provided (possibly on a commercial basis) in partnership with other institutions in which the partner institution is an independent member of eduroam AU, 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 SP or managed IdP service. In this case, IdP and/or SP institutional responsibilities still apply and should be reflected in any agreements.

Only institutional participants of eduroam AU may participate and provide eduroam services in Australia and all participating institutions must comply with this Technical Specification.

Published information regarding an institution preparing to participate or participating in eduroam AU must convey the operational status or the institution. There are three key labels which must be displayed:

- Participant Type (IdP+SP, IdP-only, SP-only)
- Deployment Status (Pre-Production, Production)

Following deployment, during the final "audit" stage of the on-boarding process, the deployment status will be denoted as "Pre-Production" (information submission to the Global Database will commence). Following successful completion of auditing, the institution's Deployment Status will be denoted as "Production"

An institution should be regarded as non-compliant with regards to this technical specification until it has undergone the final audit stage of the on-boarding process. An institution participating with "Production" status may be transitioned to "Pre-Production" if any issue is reported or discovered indicating non-compliance with the Technical Specification. In this case remedial action will be requested, and a further audit will be undertaken to confirm compliance before being transitioned to "Production".

The Pre-Production and Production status in the AdminTool map to the "preproduction/test" and "active" statuses defined in the Global Database schema [6].

2.2 Network Acceptable Use Policies

2.2.1 Requirements

1. Participants MUST publish and provide open access to their institutional network Acceptable Use Policy (AUP).

2.2.2 Discussion

Users of eduroam are required to comply with their home institution (IdP) network Acceptable Use Policy. It is assumed that compliance is required by virtue of the user's affiliation with the institution.

Users of eduroam are recommended to read and comply with the visited institution (SP) AUP.

IdP institutions are responsible for the users' network behaviour on SP "eduroam" networks. In case of user behaviour non-compliant with the SP's AUP, where the SP requires action to be taken to stop and take remedial action if required, and the user be appropriately taken to account, SPs are advised to report the behaviour (sharing relevant eduroam network logs) to the home institution associated with the 'realm' (the user's home institution i.e. eduroam IdP). The IdP is required to cooperate with the SP to identify the user, and to take action against the user as if the non-compliance occurred on the IDP's own network.

It is assumed that, given the closed eduroam user community (users engaged in research and/or education) IdP institutional AUPs will impose a reasonably equivalent set of requirements for network use, including the requirements not to infringe copyright, not to access inappropriate content, and not to engage in network activities that would adversely impact other users. This assumed AUP 'near equivalence' is one of the foundations of federated trust in eduroam.

The IdP institution's publication of its AUP enables its users to read and understand their home institution's network acceptable use requirements, and enables SP institutions to read and understand a visiting users' home institution's network acceptable use requirements. The SP institution's publication of its AUP enables visitors to read and comply with the SP's network acceptable use requirements.

2.3 Institutional Contact

2.3.1 Requirements

1. Participants MUST designate at least one eduroam contact that can be contacted using e-mail and telephone during normal business hours. The contact may be either a named individual or an institutional unit. Arrangements must be made to cover for absence of a named contact owing to eventualities such as illness and holidays. Contact information must be kept up to date via entry into the eduroam AU AdminTool.

2.3.2 Recommendations

1. Participants SHOULD designate two or more eduroam contacts in order to facilitate reliable communication between AARNet and the institution, and between participating institutions.

2.3.3 Discussion

The institution's eduroam contact is required to facilitate the resolution of matters such as technical problems and end-user non-compliance with AUP.

Contact information entered into the eduroam AU AdminTool may be designated as "private" or "public". Those contacts designated "public" are included in the eduroam AU Admin mail-list, and published to other institutional admins. Participants must ensure that changes in

staff are promptly updated via the eduroam AU AdminTool [7] . Contact information designated as “private” remains visible only to AARNet as the eduroam AU NRO.

As a global trust federation, it is important that participating institutions are able to identify a contact point in any other participating institution globally. To this end, contact details for ‘public’ contacts, are shared globally via the eduroam Global Database [8] (operated by eduroam Europe Operation Team, with access only currently available to NRO admins). The contact details for “public” contacts is provided in a data feed from the eduroam AU AdminTool to the Global Database. Participation in eduroam AU is interpreted as implicit consent from institutions to share their public eduroam contact information via the Global Database.

2.4 Logging

2.4.1 Requirements

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

2.4.2 Discussion

End-user traceability and accountability underpins the ‘federated trust’ required for eduroam to operate globally. Accurately time-stamped logging is necessary for enabling traceability between a user access event at an SP and a remote authentication event by an IdP. Cooperative investigation using logs is critical for resolving technical problems and responding to network abuse.

To ensure accuracy of time-stamps, institutional RADIUS, network and identity management services are required to utilise a reliable time source, e.g. Network Time Protocol (NTP) service, for synchronising the clocks of hosts.

To eliminate confusion and facilitate efficient cooperation between IdPs and SPs, the time zone for timestamping logs is required to be UTC.

Whilst the minimum period for retention of logs is specified above, the maximum period is a matter for the institution's internal IT policies and general data protection compliance requirements.

2.5 RADIUS Hosts

2.5.1 Requirements

1. Participants’ RADIUS (Remote Authentication Dial in Service) clients and servers MUST comply with RFC 2865 [9] and RFC 2866 [10].
2. Participants’ RADIUS clients’ and servers’ clocks MUST be configured to synchronise regularly with a reliable time source (e.g. NTP service)
3. Participants MUST deploy at least one institutional RADIUS server (IRS).
4. Participants’ IRSs, if operating as an eduroam Identity Provider server, MUST be reachable from the eduroam AU National RADIUS Proxy Servers (NRSs). IRSs using UDP MUST be configured to listen on UDP port 1812 and IRSs using RadSec [11] MUST be reachable from the NRSs on TCP port 2083.

5. Participants using RadSec MUST use X.509 certificates provided by the PKI service prescribed by AARNet to identify their IRSs.
6. If the IRS's RADIUS implementations support it, the NRS MUST be able to receive responses to Internet Control Message Protocol (ICMP) Echo Requests they send to participants' IRSs.
7. The following RADIUS attributes MUST be forwarded unaltered by participants' IRSs if present in RADIUS Access-Request, Access-Challenge, Access-Accept or Access-Reject messages.

7.1. User-Name (RFC2865) [9]
7.2. Chargeable-User-Identity (RFC4372) [12]
7.3. Calling-Station-Id (user device MAC address)
7.4. Operator-Name (RFC5580) [13]
7.5. Framed-MTU
7.6. EAP-Message (RFC3579) [14]
7.7. Message-Authenticator
7.8. Reply-Message
7.9. NAS-IP-Address (IP address of the NAS or adjacent peer RADIUS server)
7.10. NAS-Identifier (identifier of the NAS or adjacent peer RADIUS server)
7.11. State
7.12. Class
7.13. Proxy-State
7.14. MS-MPPE-Send-Key
7.15. MS-MPPE-Recv-Key

8. Participants MUST NOT forward accounting messages to the NRS.
9. Participants' IRSs MUST log all RADIUS authentication requests exchanged with the NRS; the following information must be recorded.

9.1. Timestamp (UTC)
9.2. The value of the user-name attribute in the request.
9.3. The value of the Calling-Station-Id attribute in the request.

2.5.2 Recommendations

1. Participants SHOULD deploy a secondary IRS.
2. IRSs SHOULD be configured to listen on UDP/1812 and SHOULD NOT be configured to listen on UDP/1645.
3. IRSs SHOULD NOT proxy RADIUS attributes other than those listed in Requirement 17. In particular, VPN and vendor specific attributes SHOULD NOT be proxied to the NRS.
4. If the RADIUS implementation supports it, IRSs SHOULD enable the Status-Server protocol [15] for active polling of non-responsive RADIUS servers.
5. Participants SHOULD ensure their Framed-MTU attribute is set according to their local network infrastructure MTU constraints.
6. Where RADIUS implementations do not respect Framed-MTU (i.e. do not perform EAP fragmentation to ensure UDP packets don't exceed the Framed-MTU value) the RADIUS server SHOULD be configured to ensure generated UDP packet-size does not exceed 1500 bytes.

2.5.3 Discussion

The IRS is the interface between a participating institution's network and the eduroam AU RADIUS proxy infrastructure. A secondary IRS should be implemented to improve the resilience of the participant's service and by ensuring that a receptive IRS is always online, to minimise RADIUS packet queuing on the NRS.

The inclusion of vendor specific and VPN related RADIUS attributes in packets exchanged between institutions 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 Requirement 17 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 AU National Policy (available from the AARNet eduroam website) states that Identity Providers have responsibilities in relation to the online activities of their users when visiting an eduroam SP institution, and consequently it is in the interests of the Service Provider to ensure that this logging is accurate and complete.

The IP addresses of the NRSs and the eduroam AU Test & Monitoring Server will be provided in communications between AARNet and the participating institution as part of the on-boarding process, and may be ascertained by enquiry through the AARNet Service Desk.

RADIUS accounting is not relevant in eduroam outside of Service Providers' networks and receiving and responding to these by the NRS consumes processing resources unnecessarily. In addition, the configuration of IRS to forward accounting messages to the NRS introduces unnecessary complication. Forwarding of accounting messages to the NRS is therefore not allowed and participants should check the configuration of their IRS and remove such behaviour if found.

One implication of using RADIUS over UDP, due to UDP's 'stateless' nature i.e. no acknowledgement that packets are actually received, is that network failures resulting from oversized UDP packets are silent. I.e. from the proxying RADIUS server's perspective, the only indication is lack of a response from the destination RADIUS server. This introduces considerable complexity in troubleshooting if a chain of RADIUS servers (institutional, national, regional) are involved in routing the authentication request from visited institution to home institution. It is important therefore that every measure is taken to ensure that UDP packets are not oversized, nor fragmented. Fragmentation should be performed at the EAP message level. The Framed-MTU RADIUS attribute enables a proxying RADIUS server to provide information to the destination RADIUS server on the MTU constraints of the SP institution network. Some RADIUS implementations respect (i.e. respond accordingly to) this attribute (e.g. FreeRADIUS, Radiator), and some do not (e.g. CISCO, MS implementations).

The gradual transition of institutional eduroam deployment from RADIUS over UDP to using RADIUS over TCP (with TLS) (aka RadSec) will make the issue of silent transaction failures irrelevant. However it will take considerable time before RadSec is widely adopted.

2.6 eduroam Service Information Webpage

2.6.1 Requirements

1. Participants MUST publish an eduroam service information webpage which is openly accessible from the Internet to allow users to understand the eduroam service and configure their devices for remote authentication, and for visitors to access it easily prior to travelling or when on-site at the SP institution. The webpage MUST include the following information as a minimum:

1.1. The text of, or a link to, the participant's acceptable use policy (AUP), including a statement of end-user requirement to comply with their home institution AUP, and recommendation that users read and comply with the visited institution AUP.

1.2. A link to the eduroam AU National Policy [2] and statement of compliance.

1.3. The eduroam logo linking to the eduroam AU website [4].

1.4. The type of eduroam service offered (IdP+SP, SP-only or IdP-only) and the operational status of the service (Pre-Production, Production).

1.5. A link to the eduroam AU website web-page listing eduroam AU participating institutions and locations [16].

1.6. A note regarding the logging of user eduroam authentication interactions and privacy implications, and protection from unauthorised access to logged information.

2.6.2 Recommendation

1. Participants SHOULD ensure that their eduroam information webpage is accessible using small form-factor devices.

2.6.3 Discussion

The participant's eduroam service information webpage is used to publish relevant information to help visitors and local users at the institution connect to and make use of the participant's eduroam service. The overall goal is to enable users to 'help themselves' rather than submitting a request to the institution's IT support system.

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 SP-only and IdP-only service types, must be advertised on the institution's eduroam webpage.

AARNet will provide templates covering information content required for the eduroam webpage as part of the institutional on-boarding process.

Note that both Identity Providers' and Service Providers' eduroam service information webpages are subject to further requirements; these are set out in that section of this specification.

3 Identity Provider Requirements and Recommendations

The following requirements and recommendations are specific to eduroam AU Identity Providers.

3.1 Realms

3.1.1 Requirements

1. Identity Providers' MUST determine the 'local realms' that are to be handled by the IdP RADIUS servers.

3.1.2 Recommendations

1. Institutional realms SHOULD be registered domain names of the institution.
2. The institutional realm SHOULD include a country-code top-level domain name part

3.1.3 Discussion

Realms determined by the institution for use by its user communities and handling by its RADIUS servers will be determined by a number of factors, including the identity store characteristics (e.g. different AD domains), or wish to perform some form of network segmentation based on VPNs, for example.

Unless identified as a special case by AARNet having understood the rationale, the institutional realm should include a country-code top-level domain name part. Country-code information is used by the regional RADIUS server configuration to determine routing at the top level (i.e. between regional RADIUS servers, and from regional to national RADIUS Servers). Using generic top-level domain name parts introduces the need for exception handling and configuration, hence additional complexity of routing, at regional RADIUS servers.

3.2 User Names

3.2.1 Requirements

1. Identity Providers' eduroam user names MUST conform to the Network Access Identifier (NAI) specification (RFC 7542 [17]), i.e. comprise an identity name string, "@" separator, and realm string.
2. The realm string MUST be, or conclude with, the institutions primary domain name which MUST be registered in a public Domain Name System (DNS), that the Identity Provider administers, either directly or by delegation.

3.2.2 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 Identity Provider.

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.

3.3 Logging

3.3.1 Requirements

1. Identity Providers MUST log all authentication attempts; the following information MUST be recorded.

1.1. The time that the authentication request was received.
1.2. The authentication result returned by the authentication database.
1.3. The reason given, if any, if the authentication was denied or failed.
1.4. User-Name in the outer-EAP and the User-Name from the inner-EAP (if a tunnelled EAP method is used).
1.5. Chargeable-User-Identity (CUI) if one was generated.
1.6. Calling-Station-ID.
1.7. Operator-Name if one was present in Access-Request.

3.3.2 Recommendations

Identity Providers SHOULD capture and retain logs from their identity store to further assist in troubleshooting and identification of the end-user.

3.3.3 Discussion

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

3.4 EAP Authentication

3.4.1 General Requirements

1. Identity Providers MUST configure their RADIUS server to authenticate one or more Extensible Authentication Protocol [18] [14] (EAP) types.
2. Identity Providers 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 [19], within RADIUS Access-Accept packets.

3.4.2 Recommendations

1. Identity Providers SHOULD choose a type, or types, that fulfil all or most of the 'mandatory requirements' section of RFC 4017 [20].
2. One or more of the EAP types TLS [21], PEAP [22], and TTLS [23] SHOULD be used.

3.4.3 Discussion

RFC 4017 defines requirements for EAP types used on IEEE 802.11 [24] LANs. While it is recommended that Identity Providers 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.

Use of 'tunnelled EAP' protocols by eduroam delivers secure network communications (cf. open 'guest' network access). SPs may further differentiate their "eduroam" network from other guest networks in terms of network service performance and functionality.

3.5 IdP Test Account

3.5.1 Requirements

1. If the Identity Provider has chosen to support PEAP or TTLS type methods, the institution MUST create an authenticatable test account and the relevant methods MUST be supported by the test account; additionally PAP may be used.
2. If it is believed the password has been compromised then the password MUST be changed immediately and the eduroam AU Support portal updated as soon as possible.

3.5.2 Recommendations

1. The test account SHOULD be created in the institution'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.
2. Other privileges SHOULD NOT be assigned to the test account.
3. The test account SHOULD be configured to allow at least five consecutive failed authentication attempts without the account being locked.

3.5.3 Discussion

A test account is required for test purpose by eduroam AU Support. The credentials for the test account will only be known by eduroam AU Support and the Identity Provider.

3.6 User Security Awareness

3.6.1 Recommendations

1. Identity Providers SHOULD educate their users to use protocols that provide appropriate levels of security when using eduroam.

3.6.2 Discussion

Identity Providers 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.

3.7 RADIUS Hosts

3.7.1 Requirements

1. Identity Providers MUST attempt to authenticate all authentication requests forwarded from the NRS.
2. For IdP+SP participants, the IdP MUST enable local access to the "eduroam" network to enable uses to configure eduroam authentication while on their home campus and ensure authentication is successful.

3.7.2 Recommendations

1. Where an authentication request is received from a NRS, as opposed to being received from an internal RADIUS client or NAS, a Identity Provider's Access-Accept reply SHOULD NOT contain dynamic VLAN assignment attributes, unless a mutual agreement is in place with the Service Provider. This may be achieved by the Identity Provider filtering out dynamic VLAN assignment attributes if present in Access-Accept packets sent to the NRS.
2. 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 Service Provider, as described in RFC 4372 [12].
3. For IdP-only participants, the IdP SHOULD provide a mechanism whereby users can configure and verify authentication while on their home campus.

3.7.3 Discussion

It has been noticed that some participating institutions 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 NRSs are valid and therefore must not be filtered.

3.8 eduroam Service Information Webpage

3.8.1 Requirements

1. In addition to the requirements detailed in section 2.5, an Identity Providers' eduroam information webpage MUST provide sufficient information to enable users to configure their devices to authenticate to eduroam, and statements relating to the importance of:

1.1. Consistent and secure device configuration, and the availability of device configuration scripts from the eduroam Configuration Assistant Tool [25], including a link to the tool.

1.2. Configuring end-user device authentication to eduroam while on the home institution campus, i.e. before travelling and using eduroam at a visited institution.

1.3. Certificate based authentication of the home institution's RADIUS server, in order to avoid susceptibility to rogue eduroam deployments, and recommend the CAT installation script for best-practice authentication.

1.4. The Identity Providers' eduroam information webpage MUST provide information regarding the user's responsibility to comply with their home institution's AUP, and commitment of the institution to take action against any non-compliance as if any violation occurred on the home institution's network.

1.5. The user's reading and compliance with the visited institution's AUP, with any non-compliance potentially leading to a report of the non-compliance to the home institution.

2. Identity Providers MAY choose to download and make available locally (e.g. via links) the scripts generated by the eduroam CAT.

3.8.2 Discussion

Publishing the IP forwarding policies imposed on the Service Provider's eduroam network may assist Identity Providers in supporting their users without needing to contact local support staff at the Service Provider.

4 Service Provider Requirements and Recommendations

The following requirements and recommendations are specific to eduroam AU Service Providers.

The table below summarises and highlights the standards and features of greatest impact on users:

Compliance:	
SSID	eduroam
WPA/TKIP	MUST NOT
WPA2/AES	MUST
WPA3-Transition	MAY
NAT	MAY
Application Proxy	MAY
Port Restrictions	MAY
IPv6	SHOULD
Inject Operator-Name	SHOULD

4.1 Network Presentation

4.1.1 Requirements

1. Service Providers MUST ensure that is not possible for a non-eduroam service to be mistaken by visitors for the participant's eduroam service.
2. The word 'eduroam' MUST NOT be used in an SSID for a non-compliant network.
3. Service Providers' eduroam networks MUST NOT be shared with any other network service.
4. Service Providers that provide access to eduroam for local users, or visitors from institutions not participating in eduroam, MUST ensure that the user has the opportunity to read and has agreed to the eduroam AU Policy.
5. Service Providers MUST NOT offer visitors any wireless media other than IEEE 802.11.

4.1.2 Discussion

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 institutions will use VLAN technology to segregate networks; however, this is not mandatory and participating institutions 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

1. Service Providers MUST forward RADIUS requests originating from eduroam Network Access Servers (NASs) which contain user names with non-local realms to a NRS via an IRS. 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 institution. Requests containing local realm names (those associated with the participant or partner institution) MUST NOT be forwarded to the NRS.
2. RADIUS Access-Requests MUST be sent to port UDP/1812.
3. Access-Requests using RadSec MUST be sent to port TCP/2083.
4. Service Providers MUST NOT forward requests containing user names which do not include a realm nor any which are non-NAI compliant (RFC7542 [17]).
5. Service Providers MUST NOT forward requests that have originated from NASs that do not conform to the requirements of this specification.
6. Service Providers 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 institution does not administer.
7. Service Providers MAY configure additional realms to forward requests to external RADIUS servers in other institutions, but these realms MUST be derived from domains in the global DNS that the participating institution or partner institution administers (either directly or by delegation).
8. In situations where a participating institution is in partnership with another participating institution 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 NRS.
9. In situations where the institution providing the managed Visited service is also working as a partner with further participating institutions, the Service Provider MUST ensure that

requests originating from a managed site of such an institution are NOT forwarded to any other partner.
10. Service Providers MUST NOT otherwise forward requests directly to other eduroam participants.
11. If an IRS is not capable of responding correctly to a Status-Server request then the setting to enable Status-Server on the Test & Monitoring Server for that IRS MUST NOT be enabled.

4.2.2 Recommendations

1. Service Providers SHOULD configure their IRS to load balance between the NRS servers.
2. Service Providers MAY configure their IRS to fail-over between the NRS servers.
3. 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).
4. Service Provider SHOULD configure their IRS to insert the Operator-Name attribute (RFC5580 [13]) accurately composed for their realm, into all Access-Request packets forwarded to the NRS.
5. Service Providers SHOULD request Chargeable-User-Identity (CUI) in Access-Request packets (RFC4372 [12]) forwarded to the NRS if CUI is supported by the IRS.
6. If an IRS is capable of using Status-Server (RADIUS Code 12) (RFC5997 [15]) to detect the operational state of the NRS, then it SHOULD be configured to do so.
7. If an IRS is capable of being queried by Status-Server then that functionality SHOULD be enabled so that the NRS are able to make a more informed decision on the operational status of the IRS.

4.2.3 Discussion

eduroam AU is part of the eduroam confederation, which consists of institutions 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 NRS as a general-purpose authentication system. At the present time, only NASs that conform to the requirements of this specification may use the NRS.

With the emergence of partnerships between institutions 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 eduroam AU, the issue of routing of RADIUS messages has needed clarification. Such a situation exists for instance where a contracted institution provides a managed network at a hall of residence for another or for a group of other institutions. This can be described as the provision of a managed Visited service. Where both institutions operate RADIUS servers which are peered with the national proxies, the potential exists for the routing of all requests to the NRS, including those for users from the partnered institution. This would effectively turn the NRS into an off-campus relay for a large proportion of an institution's home users, a task for which the NRS 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 institution must be routed directly to the partner's IRS and not to the NRS. 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 institutions at that managed site must still be forwarded to the NRS as per Requirement 32; i.e. bypassing the NRS for authentications between partner institutions is prohibited. This is to avoid the creation of hidden mini-eduroam proxy infrastructures.

Note; this does not proscribe inter-institution authentication between members of an association of co-operating institutions in which the individual institutions are not members of eduroam AU in their own right. In such cases the institutions 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 eduroam AU 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 Service Provider sets a NUL character in a CUI attribute included an Access-Request, the Identity Provider'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 Service Provider IRS. The values of CUI may be included in RADIUS logs.

4.3 Logging

4.3.1 Requirements

1. Service Providers MUST log all network access requests proxied to the NRS. The following information MUST be recorded:

1.1. The time that the access-accept or access-reject was received
1.2. User-Name in the outer-EAP method
1.3. Chargeable-User-Identity (CUI) if one was provided by the IdP
1.4. Calling-Station-ID
1.5. Operator-Name if one was present in Access-Request
1.6. The reply-message received including information regarding reason for Access-Reject.

4.3.2 Recommendations

1. Service Providers SHOULD capture and retain logs from their network infrastructure (e.g. DHCP server) to accurately associate an assigned IP address with a user device MAC address.

4.3.3 Discussion

Detailed logging of network access events and retention of logs enables user traceability over the retention period (hence identification of a real user and request for IdP action during investigation of network abuse) and may be used to assist in problem resolution during that period.

User traceability in case of network service AUP non-compliance is an SP prerogative, hence IdPs are required to capture and retain prescribed logging information.

If there are institutional business or policy reasons whereby visitor access logging enabling traceability should avoided, the SP institution is not required to capture and retain logs.

4.4 NAS Requirements

4.4.1 Requirements

1. NASs MUST implement IEEE 802.1X [26] authentication.
2. 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.
3. Wireless IEEE 802.11 NASs MUST support symmetric keying using keys provided by the Identity Provider within the RADIUS Access-Accept packet, in accordance with section 3.16 of RFC 3580.
4. 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.
5. All NASs that are deployed by Service Providers to support eduroam MUST include the following RADIUS attributes within Access-Request packets.

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

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

4.4.2 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 AARNet '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.

4.5 Securing Host Network Configuration

4.5.1 Recommendations

1. Service Providers SHOULD configure the network to prevent a visitor from masquerading as an authorised Dynamic Host Configuration Protocol (DHCP) server or router.

4.5.2 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.

With the aim of preventing peer-to-peer communication between devices connected to the same subnet, many wireless vendors provide functionality which allows clients to be placed in their own broadcast domain and thus are isolated from their neighbours with the same subnet.

4.6 IP Forwarding

4.6.1 Requirements

1. Service Providers MUST implement IPv4 filtering between the visitor network and other networks, providing that this permits the forwarding of the following mandatory protocols to external networks.

VPN		
1.1.	IPv6 Tunnel Broker NAT traversal:	UDP/3653; TCP/3653 egress and established.
1.2.	IPv6 Tunnel Broker Service:	IP protocol 41 egress and established.
1.3.	IPsec NAT traversal:	UDP/4500 egress and established.
1.4.	Cisco IPsec NAT traversal:	UDP/10000; TCP/10000 egress and established.
1.5.	L2TP:	UDP/1701 egress and established.
1.6.	PPTP:	IP protocol 47 (GRE) egress and established;
1.7.		TCP/1723 egress and established.
1.8.	OpenVPN:	UDP/1194; TCP/1194 egress and established.
1.9.	ESP:	IP protocol 50 egress and established.
1.10.	AH:	IP protocol 51 egress and established.
1.11.	ISAKMP and IKE:	UDP/500.
E-mail		
1.12.	IMAP4:	TCP/143 egress and established.
1.13.	IMAP3:	TCP/220 egress and established.
1.14.	SMTPS:	TCP/465 egress and established.
1.15.	Message submission:	TCP/587 egress and established.
1.16.	IMAPS:	TCP/993 egress and established.
1.17.	POP3S:	TCP/995 egress and established.

Web		
1.18.	HTTP:	TCP/80 egress and established.
1.19.	HTTPS:	TCP/443 egress and established.
1.20.	HTTP Proxy:	TCP/8080 egress and established
Other		
1.21.	SSH:	TCP/22 egress and established.
1.22.	NTP:	UDP/123 egress and established.
1.23.	LDAPS:	TCP/636 egress and established.
1.24.	IMSP:	TCP/406 egress and established.
1.25.	Passive (S) FTP:	TCP/21 egress and established.
1.26.	RDP:	TCP/3389 egress and established.
1.27.	VNC:	TCP/5900 egress and established.
1.28.	Citrix:	TCP/1494 egress and established.
1.29.	AFS:	UDP/7000 through UDP/7007 inclusive.
1.30.	SQUID Proxy:	TCP/3128 egress and established

2. Service Providers MAY implement IPv6 filtering between the visitor network and other networks, providing that this permits the forwarding of the above mandatory protocols to external networks.
3. Service Providers MAY implement arbitrary IP filtering of packets addressed to other hosts on the Service Provider's own network.

4.6.2 Recommendations

1. Service Providers MAY implement arbitrary IP filtering of packets addressed to other hosts on the Service Provider's own network.
2. Service Providers SHOULD provide visitors with unimpeded access to the Internet and vice versa, where local policy permits.

4.6.3 Discussion

An important aim of eduroam AU is to provide visitors with unimpeded access to AARNet 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 Identity Provider.

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 IP traffic or content filtering is implemented as described above, these must be stated on the institution's eduroam information website.

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

4.7 Application and Interception Proxies

4.7.1 Requirements

1. Service Providers deploying application or 'interception' proxies on their eduroam network MUST publish this fact on their eduroam service information website.
2. If an application proxy is not transparent, the Service Provider MUST also provide documentation on the configuration of applications to use the proxy.
3. Transport Layer Security (TLS)/Secure Sockets Layer (SSL) interception proxies MUST NOT be used in the "eduroam" network.

4.7.2 Recommendations

1. Service Providers SHOULD NOT deploy application or 'interception' proxies on the eduroam network.

4.7.3 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 institutions may connect their own users to non-eduroam network services to which this requirement does not apply.

4.8 eduroam Service Information Webpage

4.8.1 Requirements

1. In addition to the requirements detailed in section 2.5, Service Providers' eduroam information webpage MUST state:

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

1.2. Where applicable, the information specified in section 4.6 regarding IP traffic/content filtering and 4.7 regarding application and interception proxies.

4.8.2 Recommendations

1. Service Providers SHOULD publish the IP forwarding policies imposed on their eduroam network.

4.8.3 Discussion

Publishing the IP forwarding policies imposed on the Service Provider's eduroam network may assist Identity Providers in supporting their users without needing to contact local support staff at the Service Provider.

4.9 SSID

4.9.1 Requirements

1. Operational eduroam Wi-Fi services, as described in this specification, MUST use a broadcast SSID of 'eduroam' in lower case characters only.
2. Institutions that are in the process of developing IdP or SP operability but are not yet offering operational services MUST limit broadcast of the 'eduroam' SSID to small development environments.

4.9.2 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 institution, the possibility of users detecting a broadcast eduroam SSID must be minimised.

4.10 Network Addressing

4.10.1 Requirements

1. Service Providers MUST allocate IPv4 addresses to visitors using DHCP.
2. Service Providers MUST log the IPv4/v6 addresses allocated to visitors and the corresponding MAC addresses.
3. Service Provider eduroam networks MAY make use of NAT. If using NAT, Service Providers MUST log NAT address mappings.

4.10.2 Recommendations

1. Service Providers SHOULD implement IPv6 and allow routing of IPv6 on the eduroam network.
2. If using IPv6,
    - 2.1. Service Providers MUST allocate IPv6 addresses using SLAAC or DHCPv6.
    - 2.2. Service Providers SHOULD NOT use NAT with IPv6 but, if used, MUST log the address mappings.
    - 2.3. Service Providers SHOULD provide IPv6 DNS service.

4.10.3 Discussion

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

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 recommended that Service Providers implement IPv6 wherever possible.

Both SLAAC and DHCPv6 are acceptable ways to assign addresses. NAT SHOULD be avoided as address space is not limited and should not be used as a security feature. To complete the IPv6 implementation, provision of suitable IPv6 DNS servers should be considered.

4.11 WPA

4.11.1 Requirements

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

4.12 WPA2

4.12.1 Requirements

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

4.13 WPA3

4.13.1 Requirements

1. Service Providers providing Wi-FI services in the 2.4GHz or 5GHz RF bands MAY implement WPA3-Enterprise in transition mode; Protected Management Frames (PMFs) MAY be implemented but MUST be set to 'Supported' rather than 'Required'.
2. Service Providers providing Wi-FI services in the 6GHz RF band with WPA3-Enterprise MUST NOT implement WPA3-Enterprise 192-mode.

4.13.2 Recommendations

1. WPA3-Entperise in transition mode SHOULD be implemented in the 2.4GHz and 5GHz RF bands.

4.13.3 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 has been the only permitted standard in the Australia 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 in the 2.4GHz and 5GHz RF bands where WPA3 is optional. Since deploying WPA2 with PMF may cause interoperability issues with clients which are not certified for WPA2 with PMF, the use of PMF should only be set to supported and not required.

5 Appendices

5.1 Appendix 1: Glossary

Term	Definition
802.11	See IEEE 802.11.
802.1X	See IEEE 802.1X.
AAA	Authentication, Authorisation, Accounting.
AARNet	AARNet is Australian's National Research and Education Network. AARNet Pty Ltd (APL) manages the operation and development of the Australian Academic and Research Network. AARNet and APL may be used synonymously, the meaning being clear from the context.
Accounting	The process of reporting the utilisation of a NAS to an accounting server.
Application proxy	An intermediary host which acts as both a server and a client for the purpose of making requests on behalf of other clients. Requests from clients are serviced internally or by passing them, with possible translation, on to other servers. Web proxies, which fetch web pages on behalf of web browser, are amongst the commonest type.
Authentication	The process of a supplicant attempting to confirm its identity to a NAS.
Authorisation	The process of enforcing the privileges accorded to an identity, and restricting access to resources accordingly.
Bluetooth	A specification for seamless wireless short-range communications of data and voice between both mobile and stationary devices.
Broadcast	See Broadcast SSID.
Broadcast SSID	An SSID that is advertised by a WAP.
Credentials	Information, such as a password or user certificate, that is used by an authentication protocol to establish a claimed identity.
DHCP	See Dynamic Host Configuration Protocol.
DHCPv6	See Dynamic Host Configuration Protocol for IPv6.
Dynamic Host Configuration Protocol	A protocol used to assign IP configuration information, such as an IP address, to hosts dynamically.

Dynamic Host Configuration Protocol for IPv6	A protocol used to assign IPv6 configuration information, such as an IP address, to hosts dynamically.
EAP	See Extensible Authentication Protocol.
EAP-PEAP	An EAP type implementing TLS to secure a tunnel in which a second EAP type is used to provide authentication.
EAP-TLS	An EAP type implementing authentication using certificates.
EAP-TTLS	An EAP type implementing TLS to secure a tunnel in which a Diameter-based transaction is performed to provide authentication.
eduroam	A federated roaming service that provides secure network access by virtue of remote authentication of the user with their institutional credentials issued by their home (Identity Provider) institution.
Eduroam AU	The Australian eduroam service, governed and supported by AARNet which provides technical support services, national RADIUS proxy infrastructure and defines this Technical Specification.
Extensible Authentication Protocol (EAP)	An authentication framework that supports multiple authentication types, including passwords, token cards, and certificates. EAP is specified in RFC2284 [10].
Home institution	An institution with affiliated users, providing identity management, configured to remotely authenticate their users when they attempt to access the “eduroam” network at a Service Provider organisation.
ICMP	See Internet Control Message Protocol.
IEEE 802.11	A family of specifications for wireless LANs.
IEEE 802.11i	An amendment to the 802.11 standard specifying improved security mechanisms for IEEE 802.11 LANs.
IEEE 802.1X	A specification for port-based network access control, part of the IEEE 802 (802.1) group of protocols. It provides authentication to supplicants attached to a LAN port, establishing a network connection or preventing access from that port if authentication fails.
Internet Control Message Protocol	An IP protocol for reporting errors and other information relevant to IP packet processing.
IPv4	The most commonly deployed version of IP.

IPv6	The next generation version of IP. It includes a much larger address space, amongst other significant improvements.
Man in the middle	An attack in which an attacker is able to read, insert and modify at will, messages between two parties without either party knowing that the link between them has been compromised.
NAI	See Network Access Identifier.
NAS	See Network Access Server.
ND	See Neighbour Discovery.
Neighbour Discovery	IPv6 Neighbour Discovery is an IPv6 protocol that determines relationships between other hosts on the LAN.
Network Access Identifier (NAI)	The NAI is used to address a user within a specific realm using the general format user@realm. The NAI is specified by RFC4282 [28] (supersedes 2486).
Network Access Server (NAS)	A router or bridge that provides network access to a locally attached network for authenticated supplicants.
NREN	National Research and Education Network.
NRS	National RADIUS Server. A host managed by AARNet that forwards packets between eduroam AU participants' IRSs, or between IRSs and the APAN regional (aka "top-level") RADIUS servers.
IRS	Institutional RADIUS Server. A host deployed by a participant that forwards RADIUS packets between the NRS and internal RADIUS clients and servers.
Proxy	See RADIUS proxy or Application proxy.
Public Key Infrastructure	The framework in which digital certificates are created and used, based on a public and private keys.
RA	See Router advertisement.
RADIUS	Remote Authentication Dial-In User Service. A protocol for carrying authentication, authorisation, accounting and configuration information between a Network Access Server which desires to authenticate its links and a shared Authentication Server. RADIUS authentication is specified in RFC2865 [4] and RADIUS accounting in RFC2866 [5].
RADIUS proxy	A RADIUS server that can receive RADIUS requests from RADIUS clients and perform a decision to determine which RADIUS server the request should be forwarded onto for processing.

Router advertisement	An ND message used by routers to advertise their presence on the LAN.
Service Set Identifier	An identifier that a WAP and wireless stations use to communicate with each other.
Supplicant	A party requesting authentication from a NAS in order to access a network.
SSID	See Service Set Identifier.
Service Provider	An institution that provides the remotely authenticated eduroam user with access to its “eduroam” network.
WAG	See Wireless Advisory Group.
WAP	See Wireless Access Point.
Wireless Access Point	A bridge that enables forwarding between its associated wireless stations, and hosts on a directly-connected wired network.
WPA	A subset of the features offered by IEEE 802.11i and profiled by the Wi-Fi Alliance. WPA is a less complete profile of IEEE 802.11i than is WPA2.
WPA2	A subset of the features offered by IEEE 802.11i and profiled by the Wi-Fi Alliance. WPA2 is a more complete profile of IEEE 802.11i than is WPA.

5.2 Appendix 2: Bibliography

[1] JISC, "eduroam UK Technical Specification," https://community.jisc.ac.uk/library/network-and-technology-service-docs/eduroamuk-technical-specification-15. [Accessed 2025]

[2] AARNet, "eduroam AU National Policy," https://support.aarnet.edu.au/hc/en-us/categories/200217798-eduroam.

[3] GeGC, "eduroam Compliance Statement," https://eduroam.org/support/eduroam-documentation/. [v2 Accessed 2025]

[4] AARNet, "eduroam AU Website," https://eduroam.edu.au/.

[5] "Key words for use in RFCs to Indicate Requirement Levels," https://tools.ietf.org/html/rfc2119.

[6] "Specification eduroam-database," https://monitor.eduroam.org/fact_eduroam_db.php.

[7] AARNet, "eduroam AU AdminTool," https://admin.eduroam.edu.au.

[8] GEANT, "eduroam Global Database," https://monitor.eduroam.org/.

[9] "Remote Authentication Dial In User Service (RADIUS)," https://tools.ietf.org/html/rfc2865.

[10] "RADIUS Accounting," https://tools.ietf.org/html/rfc2866.

[11] "Transport Layer Security (TLS) Encryption for RADIUS," https://tools.ietf.org/html/rfc6614.

[12] "Chargeable User Identity," https://tools.ietf.org/html/rfc4372.

[13] "Carrying Location Objects in RADIUS and Diameter," https://tools.ietf.org/html/rfc5580.

[14] "RADIUS Support For EAP," https://tools.ietf.org/html/rfc3579.

[15] "Use of Status-Server Packets in the RADIUS Protocol," https://tools.ietf.org/html/rfc5997.

[16] AARNet, "eduroam AU Participants," https://admin.eduroam.edu.au/participants.

[17] "The Network Access Identifier," https://tools.ietf.org/html/rfc7542.

[18] "Extensible Authentication Protocol (EAP)," https://tools.ietf.org/html/rfc3748.

[19] "IEEE 802.1X RADIUS Usage Guidelines," https://tools.ietf.org/html/rfc3580.

[20] "EAP Method Requirements for Wireless LANs," https://tools.ietf.org/html/rfc4017.

[21] "PPP EAP TLS Authentication Protocol," https://tools.ietf.org/html/rfc2716.

[22] D. S. G. Z. S. J. Ashwin Palekar, Protected EAP Protocol (PEAP), 2003.

[23] S. B.-W. Paul Funk, EAP Tunneled TLS Authentication Protocol Version 0 (EAP-TTLSv0), 2005.

[24] IEEE Computer Society, Supplement to 802.11-1999,Wireless LAN MAC and PHY specifications] Higher speed Physical Layer (PHY) extension in the 2.4 GHz band, 1999.

[25] GEANT, "eduroam Configuration Assistant Tool," https://cat.eduroam.org/.

[26] IEEE Computer Society, Port-Based Network Access Control, 2004.

5.3 Appendix 3: Change log

Version	Date	Description
1.0	13 November 2019	Prepared by Authentication and Authorisation Services Technical Manager (Neil Witheridge)
1.1	19 November 2025	Removed Test & Monitoring and deployment 'Staging' Updated IP Forwarding requirements, IPv6 information Added WPA3 information (Paul Hii)