



JANET Roaming Service Technical Specification

Version 1.1 (1 February 2009)

Author: Josh Howlett, JANET(UK)



Table of Contents

1. Introduction	3
1.1. Acknowledgements	3
1.2. Overview	3
1.3. Change log.....	4
2. Common Requirements and Recommendations	6
2.1. Participation.....	6
2.2. Technical Contact.....	6
2.3. Logging.....	7
2.4. RADIUS Hosts	7
2.5. JANET Roaming Website	8
3. Home Organisation Requirements and Recommendations	9
3.1. User Names	9
3.2. Logging.....	9
3.3. EAP Authentication.....	9
3.4. Test Account.....	10
3.5. User Security Awareness.....	10
4. Visited Organisation Requirements and Recommendations	11
4.1. Network Presentation	11
4.2. RADIUS Forwarding.....	12
4.3. NAS Requirements.....	13
4.4. Securing Host Network Configuration.....	13
4.5. IP Forwarding.....	14
4.6. Application and Interception Proxies	15
4.7. JANET Roaming Website	15
4.8. SSID	16
4.9. Network Addressing.....	16
4.10. WPA	16
4.11. WPA2	17
5. Appendices.....	18
5.1. Appendix I – Summary of Requirements	18
5.2. Appendix II - Summary of recommendations	22
5.3. Appendix III – Glossary	23
5.4. Appendix IV - Bibliography.....	27

1. Introduction

1.1. Acknowledgements

The author would like to acknowledge the many important contributions provided by the following:

- the members of the JANET(UK) Wireless Access Group (WAG);
- the subscribers of the JANET(UK) Wireless-Admin mailing list;
- the members of the TERENA Mobility Task-Force (TF-Mobility);
- the members of GÉANT2 JRA5;
- the Location Independent Networking (LIN) National Trial participants.

The author also thanks his colleagues at JANET(UK) for their contributions, support and assistance.

1.2. Overview

This document is the Technical Specification for the JANET Roaming service with effect from 1 May 2009. It complies with the requirements mandated by the GÉANT2 eduroam service [1]. The most recent revision of this document can be found at the JANET(UK) Roaming website [2].

1.2.1. Using this Document

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

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

The remaining three sections are normative. These are:

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

1.3. Change log

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

1.3.1. Changes from version 1.0

- Substituted all occurrences of 'UKERNA' with 'JANET(UK)', reflecting the change of trading name of The JNT Association.
- *Set a date when the revised document takes effect.*
- Capitalised all RFC 2119 keywords to conform to convention.
- Substituted the 'rationale' headings with 'discussion' throughout the document, reflecting the purpose of these sections.
- Substituted instances of 'VLAN' with 'network' throughout the document to avoid the spurious differentiation between 'logical' and 'physical' networks.
- Corrected the participation requirements in section 2.1 ('Participation') to permit participation from organisations that choose not to deploy a visitor network. This was the original intention of the previous version of the document.
- Moved the discussion on logging from section 2.4 ('RADIUS Hosts') to section 2.3 ('Logging') to aid clarity.
- Removed mandatory support for ICMP responses from section 2.3 ('RADIUS Hosts') because some RADIUS implementations do not support this, and added the JANET Roaming Support Server as a possible source of ICMP requests.
- *Mandated a list of RADIUS attributes that must be forwarded by an ORPS in section 2.4 ('RADIUS hosts').*
- *Added a sub-section 2.5 ('JANET Roaming Website') to the 'Common Requirements' section; this has the effect of requiring all organisations (and not only Visited organisations) to publish a JANET Roaming website.*
- *Added requirements in section 2.5 ('JANET Roaming Website') relevant to all organisations to link to the JANET Roaming Policy and eduroam website.*
- Added a brief discussion concerning the use of anonymous and pseudonymous user names in section 3.1 ('User Names').
- Removed section 3.3 PAP Authentication and the recommendation that organisations configure their RADIUS server to authenticate PAP (Password Authentication Protocol); this being unnecessary since the use of web redirect is no longer permitted by this specification.
- Changed the EAP type specification for the test account from being a requirement to being a recommendation, section 3.4 ('Test Account'). Removed requirement for test account to be PAP authenticable and also recommended the use of either PEAP or TTLS.
- Renumbered section 3.6 ('User security awareness') to 3.5 and removed the discussion of web redirect this section; this information is redundant as the use of web redirect is no longer permitted by this specification.

- Removed the reference to a ‘local AUP’ in section 4.1 as an applicable document may not necessarily exist.
- Added a clarification in section 4.1 concerning the segregation of networks and visitors using VLANs or other techniques.
- Added a requirement in section 4.2 to explicitly prohibit the forwarding of requests from NASs other than those that conform to this specification.
- Added a requirement in section 4.2 to prohibit forwarding of realmless NAIs.
- Changed the heading of section 4.3 (‘NAS Requirements’) from ‘NAS General Requirements’.
- Clarified the appropriate uses of local authorisation or admission control in section 4.3.
- Removed section 4.10 (‘802.1X NASs’) and moved its requirements into section 4.3 (‘NAS Requirements’); 802.1X NASs are the only type permitted by this specification, as the use of web redirect is no longer permitted by this specification.
- Changed the heading of section 4.4 (‘Securing Host Network Configuration’) from ‘Securing Host Bootstrapping’ to assist understanding.
- Removed the discussion of web redirect from section 4.4 (‘Securing Host Network Configuration’); this information is redundant as the use of web redirect is no longer permitted by this specification.
- Changed the heading of section 4.5 (‘IP Forwarding’) from ‘IP Filtering’ to assist understanding.
- *Added the Network Time Protocol to the list of mandatory forwarded protocols in section 4.5 (‘IP Forwarding’).*
- *Added AFS to the list of mandatory forwarded protocols in section 4.5 (‘IP Forwarding’).*
- *Added port udp/10000 to the Cisco IPSec NAT traversal protocol’s policy in section 4.5 (‘IP filtering’). This corrects its accidental omission in the previous version of this policy.*
- *Updated the OpenVPN protocol’s policy in section 4.5 (‘IP Filtering’) to reflect the change in this protocol’s default port and transport.*
- *Added a recommendation in section 4.7 (‘JANET Roaming Website’) relevant to Visited organisations to publish the IP forwarding policies imposed on the visitor network on the JANET Roaming website.*
- *Moved some of the requirements that cover common requirements in section 4.7 (‘JANET Roaming Website’) to the new section 2.5 (‘JANET Roaming Website’).*
- Changed the heading of section 4.8 (‘SSID’) from ‘SSIDs’ reflecting this specification’s use of a single SSID.
- *Updated section 4.8 (‘SSIDs’) to require a single SSID for all tiers.*
- *Removed section 4.9 (‘WRD NASs’) as the use of web redirect is no longer permitted by this specification.*

- *Removed section 4.12 ('WEP') as the use of WEP is no longer permitted by this specification.*
- *Mandated the use of TKIP in section 4.10 ('WPA').*
- *Removed discussion of WEP in section 4.10 ('WPA') as WEP is no longer permitted by this specification.*
- *Mandated the use of CCMP (AES) in section 4.11 ('WPA2').*
- *Removed discussion of WEP in section 4.11 ('WPA2') as WEP is no longer permitted by this specification.*

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

Participation as a Visited organisation is not mandatory, although it is recommended. This permits an organisation that may be unable or unwilling to participate as a Visited organisation to participate as a Home organisation and allow its own users to roam.

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.
6. Logs **MUST** be kept for at least three months and for no longer than six months.

2.3.2. Discussion

Accurate logging is necessary for resolving technical problems and tracking abuse. A host's knowledge of the time is necessary for the production of logs that can be compared with logs maintained at other organisations. JANET(UK) offers a Network Time Protocol [4] (NTP) service [5] that can be used for synchronising the clocks of hosts.

The JANET(UK) 'Logfiles' [6] technical guide provides further information and advice regarding logging.

2.4. RADIUS Hosts

2.4.1. Requirements

7. Participants' RADIUS (Remote Authentication Dial In Service) clients and servers **MUST** comply with RFC 2865 [7] and RFC 2866 [8].
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 JRS National 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).
11. If the ORPS's RADIUS implementations support it, both the NRPS and JANET Roaming Support Server **MUST** be able to receive responses to Internet Control Message Protocol (ICMP) Echo Requests they send to participants' ORPSs.
12. The following RADIUS attributes **MUST** be forwarded by participants' ORPSs if present in RADIUS Access-Request, Access-Challenge, Access-Accept or Access-Reject messages.
 - 12.1. User-Name
 - 12.2. Reply-Message
 - 12.3. State
 - 12.4. Class
 - 12.5. Message-Authenticator
 - 12.6. Proxy-State
 - 12.7. EAP-Message
 - 12.8. MS-MPPE-Send-Key
 - 12.9. MS-MPPE-Recv-Key
 - 12.10. Calling-Station-Id
13. The following RADIUS attributes **MUST** be forwarded by participants' ORPSs if present in RADIUS Accounting messages.
 - 13.1. User-Name
 - 13.2. Acct-Status-Type
 - 13.3. Acct-Session-ID

- 13.4. Proxy-State
- 13.5. Class
- 14. Participants' ORPSs MUST log all RADIUS authentication requests exchanged with the NRPS; the following information must be recorded.
 - 14.1. The value of the user name attribute in the request.
 - 14.2. The value of the Calling-Station-Id attribute in the request.
- 15. Participants MUST log all RADIUS accounting 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 accounting session identifier.
 - 15.3. 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 JANET Roaming. A secondary ORPS should be implemented to improve the resilience of the service.

RADIUS authentication and accounting typically use ports UDP/1812 and UDP/1813 respectively. Ports UDP/1645 and UDP/1646 are deprecated, but in occasional use, and so their use is also permitted.

Detailed logging of authentication and accounting requests is necessary for problem resolution and the tracking of network abuse. Note that the JANET Roaming Policy (available from the JANET Roaming website) states that Visited organisations are responsible for all activities of visitors, and consequently it is in their interests to ensure that this logging is accurate and complete.

The IP addresses of the JRS NRPSs and Support Server may be obtained from the JANET Service Desk.

2.5. JANET Roaming Website

2.5.1. Requirements

- 16. Participants MUST publish a JANET Roaming website which must be generally accessible from the Internet and, if applicable, within the organisation to allow visitors to access it easily. The website MUST include the following information as a minimum.
 - 16.1. The text of, or a link to, the participant's acceptable use policy (AUP), where applicable.
 - 16.2. A link to the JANET Roaming Policy [9].
 - 16.3. The eduroam logo linking to the eduroam website [10].

2.5.2. Discussion

The JANET Roaming website is used to publish relevant information about the participant's JANET Roaming service to the participant's own users and visitors.

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

3. Home Organisation Requirements and Recommendations

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

3.1. User Names

3.1.1. Requirements

17. Home organisations' JANET Roaming user names **MUST** conform to the Network Access Identifier (NAI) specification (RFC 4282 [11]).
18. The realm component **MUST** conclude with participant's realm name, which **MUST** be a domain name in the global Domain Name System (DNS) that the Home organisation administers, either directly or by delegation.

3.1.2. Discussion

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

3.2. Logging

3.2.1. Requirements

19. Home organisations **MUST** log all authentication attempts; the following information **MUST** be recorded.
 - 19.1. The time that the authentication request was received.
 - 19.2. The authentication result returned by the authentication database.
 - 19.3. The reason given, if any, if the authentication was denied or failed.

3.2.2. Discussion

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

3.3. EAP Authentication

3.3.1. General Requirements

20. Home organisations **MUST** configure their RADIUS server to authenticate one or more Extensible Authentication Protocol [12] (EAP) types.
21. Home organisations **MUST** select an EAP type, or EAP types, for which their RADIUS server will generate symmetric keying material for encryption ciphers and encapsulate the keys, following section 3.16 of RFC 3580 [13], within RADIUS Access-Accept packets.

3.3.2. Recommendations

3. Home organisations **SHOULD** choose a type, or types, that fulfil all or most of the 'mandatory requirements' section of RFC 4017 [14].
 - 3.1. The EAP types TLS [15], PEAP [16], and TTLS [17] are recommended.

3.3.3. Discussion

RFC 4017 defines requirements for EAP types used on IEEE 802.11 [18] LANs. While it is recommended that Home organisations select an EAP type (or types) that fulfils as many of these requirements as possible, it is mandatory that the ‘Generation of symmetric keying material’ requirement is met, and that the keys are returned in the RADIUS Access-Accept packet.

The JANET(UK) ‘Extensible Authentication Protocol’ [19] technical sheet provides further information on EAP.

3.4. Test Account

3.4.1. Requirements

22. Home organisations **MUST** create an authenticatable test account.
23. JANET Roaming 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 JANET Roaming 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. The test account **SHOULD** be able to authenticate the EAP type(s) selected by the Home organisation; where possible, either the PEAP or TTLS types **SHOULD** be supported.
6. Other privileges **SHOULD NOT** be assigned to the test account.
7. The test account **SHOULD** be configured to allow at least five consecutive failed authentication attempts without the account being locked.

3.4.3. Discussion

A test account is required for testing and monitoring purposes by JANET Roaming Support. These credentials will be known only to JANET Roaming Support.

3.5. User Security Awareness

3.5.1. Recommendations

8. Home organisations **SHOULD** educate their users to use protocols providing appropriate levels of security when using JANET Roaming.

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 JANET Roaming does not provide any guarantees regarding the privacy of this data.

4. Visited Organisation Requirements and Recommendations

This section is concerned with the requirements pertaining to Visited organisations. JANET Roaming defines two service tiers for Visited organisations: JRS2 and JRS3. Earlier versions of this document specified a deprecated service tier called JRS1; this tier has now been removed and may no longer be used in association with JANET Roaming or eduroam brands or SSIDs.

The purpose of the tiers is to promote consistency amongst participating organisations, thereby improving the user experience and reducing the support burden on the Home organisation, while providing Visited organisations with some flexibility in the manner in which they implement the service.

The table below shows a summary of the differences between the tiers.

<i>Tier</i>	<i>IPv6</i>	<i>NAT</i>	<i>WPA</i>	<i>WPA2</i>
JRS1	Not permitted from 1 May 2009			
JRS2	May	May	Must	May
JRS3	Must	Must not	Should	Must

4.1. Network Presentation

4.1.1. Requirements

24. Visited organisations **MUST** implement one, or optionally both, of the JRS2 or JRS3 tiers.
25. Visited organisations **MUST** ensure that a non-JANET Roaming service cannot be mistaken by visitors for the participant's JANET Roaming service.
26. The word 'eduroam' **MUST NOT** be used in an SSID for a non-JRS tier.
27. Visited organisations **MUST** implement a separate network for each tier that they choose to implement. A tier's network **MUST NOT** be shared with any other tier or network service.
28. Visited organisations that provide access to a JRS tier for local users, or visitors from organisations not participating in JANET Roaming, **MUST** ensure that the user has read and agreed to the JANET Roaming Policy.
29. Visited organisations **MUST NOT** offer visitors any wireless media other than IEEE 802.11.

4.1.2. Recommendations

9. Where possible Visited organisations **SHOULD** implement JRS3 in preference to JRS2.

4.1.3. Discussion

The JRS2 tier is intended to be the standard JRS tier; it is anticipated that most participants will implement this tier initially. The JRS3 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-JANET Roaming wireless service, in addition to a JRS tier. 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 JRS tier(s).

Note that it is permissible to place local users on a non-JRS network tier, even if they have connected to an SSID bearing the name 'eduroam'; it is not permissible to do this to visitors.

Each tier is intended to operate at a known security context. Hence, sharing the visitor network with other tiers or network services is prohibited as this may degrade the security context.

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 JANET Roaming, participants are permitted to use other media, such as FastEthernet, providing that the other tier requirements are adhered to. With the same proviso, the mixing of media on the same network is also permitted.

At present this specification currently prohibits the use of non-IEEE 802.11 wireless media, such as Bluetooth, because their suitability for JANET Roaming has not yet been adequately explored. These media may be permitted in a future revision of this specification if interest in their use is expressed.

4.2. RADIUS Forwarding

4.2.1. Requirements

30. Visited organisations **MUST** forward RADIUS requests originating from JANET Roaming Network Access Servers (NASs) and containing user names with unknown realms via an ORPS to an NRPS.
 - 30.1. RADIUS Access-Requests must be addressed to port UDP/1812.
 - 30.2. RADIUS Accounting-Requests must be addressed to port UDP/1813.
31. Visited organisations **MUST NOT** forward RADIUS requests containing user names without a realm.
32. Visited organisations **MUST NOT** forward requests that have originated from NASs that do not conform with the requirements of this specification.
33. 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 does not administer.
34. 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 administers (either directly, or by delegation).
35. Visited organisations **MUST NOT** otherwise forward requests to other JANET Roaming participants.

4.2.2. Recommendations

10. Visited organisations **SHOULD** configure their ORPS to fail-over between the NRPS servers in the event that a NRPS fails to respond to a RADIUS request.
 - 10.1. 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).

4.2.3. Discussion

JANET Roaming is part of the eduroam confederation, which consists of organisations holding domain names derived from many of the top level Domain Name Service (DNS) [20] 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.

4.3. NAS Requirements

4.3.1. Requirements

36. NASs MUST implement IEEE 802.1X [21] authentication.
37. 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.
38. 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.
39. A NAS port MUST NOT connect more than one user.
40. Visited organisations MUST deploy NASs that include the following RADIUS attributes within Access-Request packets.
 - 40.1. The supplicant's MAC address within the Calling-Station-ID attribute.
 - 40.2. The NAS's IP address within the NAS-IP-Address attribute.

4.3.2. Discussion

Each visitor must have a unique port on a NAS that supports IEEE 802.1X. It is not permissible to have two or more users on the same NAS port, as this reduces the security context because they are able to communicate with each other without authenticating to the NAS. Note that this restriction prohibits the use of some gateway devices that provide IEEE 802.1X authentication to multiple users over a single NAS port.

The JANET 'IEEE 802.1X' [22] 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 and the tracking of network abuse.

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

11. Visited organisations SHOULD configure the network to prevent a visitor from masquerading as an authorised Dynamic Host Configuration protocol (DHCP) [23] 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

41. 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.

- 41.1. IPv6 Tunnel Broker NAT traversal: UDP/3653;TCP/3653 egress and established.
- 41.2. IPsec NAT traversal: UDP/4500 egress and established.
- 41.3. Cisco IPsec NAT traversal: UDP/10000; TCP/10000 egress and established.
- 41.4. PPTP: IP protocol 47 (GRE) egress and established; TCP/1723 egress and established.
- 41.5. OpenVPN: UDP/1194; TCP/1194 egress and established.
- 41.6. NTP: UDP/123 egress and established
- 41.7. SSH: TCP/22 egress and established.
- 41.8. HTTP: TCP/80 egress and established.
- 41.9. HTTPS: TCP/443 egress and established.
- 41.10. LDAP: TCP/389 egress and established.
- 41.11. LDAPS: TCP/636 egress and established.
- 41.12. IMSP: TCP/406 egress and established.
- 41.13. IMAP4: TCP/143 egress and established.
- 41.14. IMAP3: TCP/220 egress and established.
- 41.15. IMAPS: TCP/993 egress and established.
- 41.16. POP: TCP/110 egress and established.
- 41.17. POP3S: TCP/995 egress and established.
- 41.18. Passive (S)FTP: TCP/21 egress and established.
- 41.19. SMTPS: TCP/465 egress and established.
- 41.20. Message submission: TCP/587 egress and established.
- 41.21. RDP: TCP/3389 egress and established.
- 41.22. VNC: TCP/5900 egress and established.
- 41.23. Citrix: TCP/1494 egress and established.
- 41.24. AFS: UDP/7000 through UDP/7007 inclusive egress and established.

4.5.2. Recommendations

12. Visited organisations MAY implement arbitrary IP filtering of packets addressed to other hosts on the Visited organisation's own network.
13. Visited organisations SHOULD provide visitors with unimpeded access to JANET, and *vice versa*, where local policy permits.

4.5.3. Discussion

An important aim of JANET Roaming is to provide visitors with unimpeded access to JANET. 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.

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

42. Visited organisations deploying application or 'interception' proxies on the visitor network MUST publish this fact on their JANET Roaming website.
43. 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

14. Visited organisations SHOULD NOT deploy application or 'interception' proxies on the visitor 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. JANET Roaming Website

4.7.1. Requirements

44. In addition to the requirements detailed in section 2.5, Visited organisations' JANET Roaming websites MUST state:
 - 44.1. Sufficient information to enable visitors to identify and access the service; at a minimum this must include the locations covered and their JRS tier.
 - 44.2. Where applicable, the information specified in section 4.6 regarding application and interception proxies.

4.7.2. Recommendations

15. Visited organisations **SHOULD** ensure that their JANET Roaming website is accessible using small form-factor devices such as PDAs.
16. 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

45. A broadcast SSID of 'eduroam' **MUST** be used for all JRS tiers.

4.8.2. Discussion

Windows XP is unable to authenticate against a non-broadcast SSID offering IEEE 802.1X where another broadcast SSID is also visible.

4.9. Network Addressing

4.9.1. Requirements

46. The JRS3 tier **MUST NOT** make use of NAT.
47. The JRS3 tier **MUST** allow routing of IPv6 on the visitor network.
48. Visited organisations **MUST** allocate IPv4 addresses to visitors using DHCP.
49. Visited organisations **MUST** log the IPv4 addresses allocated to visitors and the corresponding MAC addresses.
50. Visited organisations **MUST** log NAT address mappings, if used as part of a JRS2 tier implementation.

4.9.2. 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.

IPv6 is required for the JRS3 tier. 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.

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

4.10. WPA

4.10.1. Requirements

51. The JRS2 tier **MUST** implement WPA with the use of the TKIP algorithm.

4.10.2. Recommendations

17. The JRS3 tier SHOULD implement WPA with the use of the TKIP algorithm.

4.10.3. Discussion

WPA is a specification from the WiFi Alliance that implements a subset of IEEE 802.11i [24]. 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.

WPA is mandatory for the JRS2 tier. WPA is also recommended for the JRS3 tier, to allow it to support WPA clients without compromising on security (WPA2 specifies a WPA/WPA2 mixed mode).

4.11. WPA2

4.11.1. Requirements

52. The JRS3 tier MUST implement WPA2 with the use of the CCMP (AES) algorithm.

4.11.2. Recommendations

18. The JRS2 tier MAY implement WPA2 with the use of the CCMP (AES) algorithm.

4.11.3. Discussion

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

WPA2 is optional for the JRS2 tier, because many stations do not support WPA2 at present.

WPA2 is mandatory for the JRS3 tier, as it contributes towards a higher security context.

5. Appendices

5.1. Appendix I – Summary of Requirements

5.1.1. Common requirement

1.	Participating organisations MUST observe the requirements set out in section two of this document.	6
2.	Participants that choose to participate as a Home organisation MUST observe the requirements set out in section 3 of this document.....	6
3.	Participants that choose to participate as a Visited organisation MUST observe the requirements set out in section 4 of this document.....	6
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.	6
5.	Every log entry MUST state the date and time it was logged, derived from a reliable time source.....	7
6.	Logs MUST be kept for at least three months and for no longer than six months.	7
7.	Participants’ RADIUS (Remote Authentication Dial In Service) clients and servers MUST comply with RFC 2865 [7] and RFC 2866 [8].....	7
8.	Participants’ RADIUS clients’ and servers’ clocks MUST be configured to synchronise regularly with a reliable time source.....	7
9.	Participants MUST deploy at least one ORPS (organisational RADIUS proxy server).	7
10.	Participants’ ORPSs MUST be reachable from the JRS National 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).	7
11.	If the ORPS’s RADIUS implementation support its, both the NRPS and JANET Roaming Support Server MUST be able to receive responses to Internet Control Message Protocol (ICMP) Echo Requests it sends to participants’ ORPSs.	7
12.	The following RADIUS attributes MUST be forwarded by participants’ ORPSs if present in RADIUS Access-Request, Access-Challenge, Access-Accept or Access-Reject messages.....	7
12.1.	User-Name	7
12.2.	Reply-Message.....	7
12.3.	State	7
12.4.	Class.....	7
12.5.	Message-Authenticator	7
12.6.	Proxy-State.....	7
12.7.	EAP-Message.....	7
12.8.	MS-MPPE-Send-Key.....	7
12.9.	MS-MPPE-Recv-Key	7
12.10.	Calling-Station-Id	7
13.	The following RADIUS attributes MUST be forwarded by participants’ ORPSs if present in RADIUS Accounting messages.....	7
13.1.	User-Name	7
13.2.	Acct-Status-Type	7
13.3.	Acct-Session-ID.....	7

13.4.	Proxy-State.....	8
13.5.	Class.....	8
14.	Participants’ ORPSs MUST log all RADIUS authentication requests exchanged with the NRPS; the following information must be recorded.	8
14.1.	The value of the user name attribute in the request.	8
14.2.	The value of the Calling-Station-Id attribute in the request.	8
15.	Participants MUST log all RADIUS accounting requests exchanged with the NRPS; the following information must be recorded.	8
15.1.	The value of the user name attribute in the request.	8
15.2.	The value of the accounting session identifier.....	8
15.3.	The value of the request’s accounting status type.....	8
16.	Participants MUST publish a JANET Roaming website which must be generally accessible from the Internet and, if applicable, within the organisation to allow visitors to access it easily. The website MUST include the following information as a minimum.....	8
16.1.	The text of, or a link to, the participant’s acceptable use policy (AUP), where applicable.	8
16.2.	A link to the JANET Roaming Policy [9].....	8
16.3.	The eduroam logo linking to the eduroam website [10].	8

5.1.2. Home organisation requirements

17.	Home organisations’ JANET Roaming user names MUST conform to the Network Access Identifier (NAI) specification (RFC 4282 [11]).	9
18.	The realm component MUST conclude with participant’s realm name, which MUST be a domain name in the global Domain Name System (DNS) that the Home organisation administers, either directly or by delegation.	9
19.	Home organisations MUST log all authentication attempts; the following information MUST be recorded.....	9
19.1.	The time that the authentication request was received.	9
19.2.	The authentication result returned by the authentication database.	9
19.3.	The reason given, if any, if the authentication was denied or failed.....	9
20.	Home organisations MUST configure their RADIUS server to authenticate one or more Extensible Authentication Protocol [12] (EAP) types.	9
21.	Home organisations MUST select an EAP type, or EAP types, for which their RADIUS server will generate symmetric keying material for encryption ciphers and encapsulate the keys, following section 3.16 of RFC 3580 [13], within RADIUS Access-Accept packets.....	9
22.	Home organisations MUST create an authenticatable test account.	10
23.	JANET Roaming 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 JANET Roaming Support informed as soon as possible.	10
5.	The test account SHOULD be able to authenticate the EAP type(s) selected by the Home organisation; where possible, either the PEAP or TTLS types SHOULD be supported..... Error! Bookmark not defined.	

5.1.3. Visited organisation requirements – common to all JRS tiers

24. Visited organisations MUST implement one, or optionally both, of the JRS2 or JRS3 tiers..... 11

25. Visited organisations MUST ensure that a non-JANET Roaming service cannot be mistaken by visitors for the participant’s JANET Roaming service..... 11

26. The word ‘eduroam’ MUST NOT be used in an SSID for a non-JRS tier..... 11

27. Visited organisations MUST implement a separate network for each tier that they choose to implement. A tier’s network MUST NOT be shared with any other tier or network service. 11

28. Visited organisations that provide access to a JRS tier for local users, or visitors from organisations not participating in JANET Roaming, MUST ensure that the user has read and agreed to the JANET Roaming Policy. 11

29. Visited organisations MUST NOT offer visitors any wireless media other than IEEE 802.11..... 11

30. Visited organisations MUST forward RADIUS requests originating from JANET Roaming Network Access Servers (NASs) and containing user names with unknown realms via an ORPS to an NRPS. 12

30.1. RADIUS Access-Requests must be addressed to port UDP/1812..... 12

30.2. RADIUS Accounting-Requests must be addressed to port UDP/1813. 12

31. Visited organisations MUST NOT forward RADIUS requests containing user names without a realm. 12

32. Visited organisations MUST only forward requests that have originated from NASs that conform with the requirements of this specification..... 12

33. 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 does not administer. 12

34. 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 administers (either directly, or by delegation). 12

35. Visited organisations MUST NOT otherwise forward requests to other JANET Roaming participants. 12

36. NASs MUST implement IEEE 802.1X [21] authentication..... 13

37. 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..... 13

38. 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. 13

39. A NAS port MUST NOT connect more than one user..... 13

40. Visited organisations MUST deploy NASs that include the following RADIUS attributes within Access-Request packets..... 13

40.1. The supplicant’s MAC address within the Calling-Station-ID attribute. 13

40.2. The NAS’s IP address within the NAS-IP-Address attribute. 13

41. 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. 14

41.1. IPv6 Tunnel Broker NAT traversal: UDP/3653;TCP/3653 egress and established..... 14

41.2.	IPSec NAT traversal: UDP/4500 egress and established.....	14
41.3.	Cisco IPSec NAT traversal: UDP/10000; TCP/10000 egress and established....	14
41.4.	PPTP: IP protocol 47 (GRE) egress and established; TCP/1723 egress and established.....	14
41.5.	OpenVPN: UDP/1194; TCP/1194 egress and established.	14
41.6.	NTP: UDP/123 egress and established	14
41.7.	SSH: TCP/22 egress and established.	14
41.8.	HTTP: TCP/80 egress and established.	14
41.9.	HTTPS: TCP/443 egress and established.	14
41.10.	LDAP: TCP/389 egress and established.	14
41.11.	LDAPS: TCP/636 egress and established.....	14
41.12.	IMSP: TCP/406 egress and established.	14
41.13.	IMAP4: TCP/143 egress and established.	14
41.14.	IMAP3: TCP/220 egress and established.	14
41.15.	IMAPS: TCP/993 egress and established.	14
41.16.	POP: TCP/110 egress and established.	14
41.17.	POP3S: TCP/995 egress and established.....	14
41.18.	Passive (S)FTP: TCP/21 egress and established.....	14
41.19.	SMTPTS: TCP/465 egress and established.....	14
41.20.	Message submission: TCP/587 egress and established.	14
41.21.	RDP: TCP/3389 egress and established.....	14
41.22.	VNC: TCP/5900 egress and established.	14
41.23.	Citrix: TCP/1494 egress and established.	14
41.24.	AFS: UDP/7000 through UDP/7007 inclusive egress and established.	14
42.	Visited organisations deploying application or ‘interception’ proxies on the visitor network MUST publish this fact on their JANET Roaming website.	15
43.	If an application proxy is not transparent, the Visited organisation MUST also provide documentation on the configuration of applications to use the proxy....	15
44.	Visited organisations’ JANET Roaming websites MUST state:	15
44.1.	Sufficient information to enable visitors to identify and access the service; at a minimum this must include the locations covered and their JRS tier.....	15
44.2.	Where applicable, the information specified in section 4.6 regarding application and interception proxies.....	15
45.	A broadcast SSID of ‘eduroam’ MUST be used for all JRS tiers.	16
48.	Visited organisations MUST allocate IPv4 addresses to visitors using DHCP...	16
49.	Visited organisations MUST log the IPv4 addresses allocated to visitors and the corresponding MAC addresses.	16

5.1.4. Visited organisation requirements – JRS2 specific

50.	Visited organisations MUST log NAT address mappings, if used as part of a JRS2 tier implementation.	16
51.	The JRS2 tier MUST implement WPA with the use of the TKIP algorithm.	16

5.1.5. Visited organisation requirements – JRS3 specific

46.	The JRS3 tier MUST NOT make use of NAT.....	16
47.	The JRS3 tier MUST allow routing of IPv6 on the visitor network.....	16
52.	The JRS3 tier MUST implement WPA2 with the use of the CCMP (AES) algorithm.	17

5.2. Appendix II - Summary of recommendations

5.2.1. Common recommendations

1. Participants SHOULD observe the recommendations set out in this document.....6
2. Participants SHOULD deploy a secondary ORPS.8

5.2.2. Home organisation recommendations

3. Home organisations SHOULD choose a type, or types, that fulfil all or most of the ‘mandatory requirements’ section of RFC 4017 [14].9
- 3.1. The EAP types TLS [15], PEAP [16], and TTLS [17] are recommended.9
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.10
6. Other privileges SHOULD NOT be assigned to the test account.10
7. The test account SHOULD be configured to allow at least five consecutive failed authentication attempts without the account being locked.....10
8. Home organisations SHOULD educate their users to use protocols providing appropriate levels of security when using JANET Roaming.10

5.2.3. Visited organisation recommendations

9. Where possible Visited organisations SHOULD implement JRS3 in preference to JRS2.11
10. Visited organisations SHOULD configure their ORPS to fail-over between the NRPS servers in the event that a NRPS fails to respond to a RADIUS request. ...12
- 10.1. 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).12
11. Visited organisations SHOULD configure the network to prevent a visitor from masquerading as an authorised Dynamic Host Configuration protocol (DHCP) [23] server or router.13
12. Visited organisations MAY implement arbitrary IP filtering of packets addressed to other hosts on the Visited organisation’s own network.15
13. Visited organisations SHOULD provide visitors with unimpeded access to JANET, and *vice versa*, where local policy permits.15
14. Visited organisations SHOULD NOT deploy application or ‘interception’ proxies on the visitor network.....15
15. Visited organisations SHOULD ensure that their JANET Roaming website is accessible using small form-factor devices such as PDAs.....16
16. Visited organisations MAY publish the IP forwarding policies imposed on the visitor network.16
17. The JRS3 tier SHOULD implement WPA with the use of the TKIP algorithm....17
18. The JRS2 tier MAY implement WPA2 with the use of the CCMP (AES) algorithm.17

5.3. Appendix III – Glossary

<i>Term</i>	<i>Definition</i>
802.11	See IEEE 802.11.
802.1X	See IEEE 802.1X.
AAA	Authentication, Authorisation, Accounting.
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.

<i>Term</i>	<i>Definition</i>
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	An organisation representing a collection of NRENs, mainly European, that promotes inter-NREN roaming.
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 organisation	An organisation with affiliated users that can authenticate them when they attempt to authenticate at a Visited 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.
JANET(UK)	JANET(UK) manages the operation and development of JANET, the UK's education and research network.
JANET Roaming Service	The JANET(UK) managed service that this document provides the technical specification for.
JRS	See JANET Roaming Service.
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.

<i>Term</i>	<i>Definition</i>
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 RFC2486 [27].
Network Access Server (NAS)	A router or bridge that provides network access to a locally attached network for authenticated supplicants.
NREN	National Regional Education Network.
NRPS	National RADIUS Proxy Server. A host managed by JANET(UK) that forwards packets between JANET Roaming participants' ORPSs and the eduroam top-level RADIUS proxies.
ORPS	Organisational RADIUS Proxy Server. A host managed by a participant that forwards RADIUS packets between the NRPS 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, authorization, 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.

<i>Term</i>	<i>Definition</i>
SSID	See Service Set Identifier.
TERENA	See Trans European Research and Networking Association.
Trans-European Research and Networking Association (TERENA)	TERENA carries out technical activities and provides a platform for discussion to encourage the development of computer networking infrastructure for the European research community (see [28]).
Visited organisation	An organisation that provides authenticated visitors with access to a visitor LAN.
WAG	See Wireless Advisory Group.
WAP	See Wireless Access Point.
Wireless Advisory Group	A group which provides advice and dissemination of information on wireless networking technologies to the JANET community, as well as guidance to JANET(UK) on work requirements in the wireless area.
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 WiFi 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 WiFi Alliance. WPA2 is a more complete profile of IEEE 802.11i than is WPA.

5.4. Appendix IV - Bibliography

- 1: GÉANT2 JRA5, GÉANT2 eduroam service, <http://www.geant2.net/server/show/nav.1977>
- 2: JANET(UK), JANET Roaming website, <http://www.ja.net/roaming>
- 3: S. Bradner, RFC2119 - Key words for use in RFCs to Indicate Requirement Levels, 1997
- 4: David L. Mills, RFC 1305 - Network Time Protocol (Version 3), 1992
- 5: JANET(UK), JANET NTP service, <http://www.ja.net/services/ntp>
- 6: JANET(UK), JANET Logfiles technical guide, <http://www.ja.net/documents/publications/technical-guides/logfiles.pdf>
- 7: C. Rigney, S. Willens, A. Rubens, W. Simpson, RFC2865 - Remote Authentication Dial In User Service (RADIUS), 2000
- 8: C. Rigney, RFC2866 - RADIUS Accounting, 2000
- 9: JANET(UK), JANET Roaming Policy v2, 2007
- 10: Eduroam, Eduroam website, <http://www.eduroam.org>
- 11: B. Aboba, M. Beadles, J. Arkko, P. Eronen, RFC4282 - The Network Access Identifier, 2005
- 12: B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, H. Levkowitz, Ed., RFC3748 - Extensible Authentication Protocol (EAP), 2004
- 13: P. Congdon, B. Aboba, A. Smith, G. Zorn, J. Roese, RFC3580 - IEEE 802.1X Remote Authentication Dial In User Service (RADIUS) Usage Guidelines, 2003
- 14: D. Stanley, J. Walker, B. Aboba, RFC4017 - Extensible Authentication Protocol (EAP) Method Requirements for Wireless LANs, 2005
- 15: B. Aboba, D. Simon, RFC2716 - PPP EAP TLS Authentication Protocol, 1999
- 16: Ashwin Palekar, Dan Simon, Glen Zorn, S. Josefsson, Protected EAP Protocol (PEAP), 2003
- 17: Paul Funk, Simon Blake-Wilson, EAP Tunneled TLS Authentication Protocol Version 0 (EAP-TTLSv0), 2005
- 18: 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
- 19: JANET(UK), Extensible Authentication Protocol, <http://www.ja.net/documents/publications/factsheets/065-eap.pdf>
- 20: P. Mockapetris, RFC1034 - Domain names - concepts and facilities, 1988
- 21: IEEE Computer Society, Port-Based Network Access Control, 2004
- 22: JANET(UK), IEEE 802.1X, <http://www.ja.net/documents/publications/factsheets/064-ieee.802.1x.pdf>
- 23: R. Droms, RFC 2131 - Dynamic Host Configuration Protocol, 1997
- 24: IEEE Computer Society, Medium Access Control (MAC) Security Enhancements, 2004