Published on *Jisc community* (https://community-stg.jisc.ac.uk)

Implementing eduroam Roadmap - Part 2

On this page sections 10 - 15:

See Part 1 for sections 1 - 9: [1]

See Part 3 for sections 16 - 22: [2]

Part 2

9. Firewall Configuration to Permit RADIUS Servers to Work with NRPS

The next step is to enable your RADIUS service to communicate with the national RADIUS

Proxy servers. RADIUS uses UDP and so there is a requirement for the ports specified below to be open on your firewall. UDP communication is needed to all three NRPS. The NRPS also perform ICMP probes to your ORPS, as does the eduroam(UK) Support server. By exception, Cisco ACS systems with CSA hardening reject ICMP and so TCP probes on port 2002 can be used instead.

Firewall requirements for ORPS-NRPS/Support operation:

a) The organisational firewall must be configured to permit the following protocols and port numbers from the three eduroam(UK) NRPSs to the ORPS(s):

- UDP/1812 inbound and outbound (used for authentication)
- UDP/1645 inbound, only if your ORPS requires this (deprecated)
- ICMP
- ICMP must also be permitted for eduroam New Support server 195.195.131.204 2001:630:1:7:5bd:5f3e:bb1c:6f27

Note that FreeRADIUS can under extreme load burst proxied auth requests to ports other than 1812. FreeRADIUS 2 used to use UDP/1814 in these circumstances but FR 3 uses ephemeral ports now. There may be some circumstances in which you would need to open additional UDP ports on your firewall, but the Tech Spec specifies that auth requests sent to the NPRS MUST be via port 1812.

The addresses of the NRPS:

Roaming0	194.82.174.185	2001:630:1:128::185	
Roaming1	194.83.56.233	2001:630:1:12a::233	
(Roaming2	194.83.56.249	2001:630:1:129::249	Roaming 2 is currently out of production)

The address of the eduroam(UK) Support server:

New Support server	195.195.131.204	2001:630:1:7:5bd:5f3e:bb1c:6f27	
Old Support server	193.60.199.62	2001:630:1:5::62	(not required at present)

b) The organisational firewall and/or ORPS firewall must be configured to allow fragmented UDP packets to pass, without any restriction on packet size, for the above servers. This is because certain EAP methods (EAP-TLS) and RADIUS server implementations result in the generation of very large packets (due to the certificate length) and it is common for such packets to get fragmented by routers during transit. It is vital to the RADIUS exchange that these fragments are not discarded. Whilst it may be technically possible for the default maximum RADIUS packet size to be adjusted at the Home site/IdP, (reducing the packet size will reduce the possibility of fragmentation by a router,) due to overseas IdPs being outside UK authority and possible capability limitations of some RADIUS servers, it would not be sensible us make RADIUS packet length recommendations. Instead, the eduroam(UK) policy focusses on firewall rules such that **any** UDP packet to or from the NRPS must be permitted without fragmentation/size restriction.

[Hint - If you are using Solaris ipf firewall the config script can be written to pass fragments using the keep frag keyword

If you do want to restrict packet length (MTU) and are using Microsoft NPS, (particularly if you are using EAP-TLS) - there is some guidance at TechNet https://technet.microsoft.com/en-us/library/cc755205%28v=ws.10%29.aspx [3].

Testing Port 1812 firewall transit and NAT/PAP if applicable: you can verify that port 1812 is open through your firewall and any NAT/PAT translation (if applicable) is working by using the PAP authentication test on the Support server together with packet capture on your RADIUS server (eg tcpdump for linux/BSD/unix or Wireshark on Windows). You will also be able to see the requests logged on your RADIUS server when you run the PAP tests. For info on how to run the test, jump to part 2 section 15 [4] of this guide.

Nb. This is the only use for PAP in edruoam; it is not used in production. Once you have configured production EAP methods as described later in this guide, there are further tests on Support server which can be of help.

10. RADIUS server proxying configuration and attributes filtering

In this section:

- Addition of NRPS as RADIUS clients
- Configure Realm Handling, Proxying and Load Balancing
- FreeRADIUS Example Configuration - proxy, client and foreign realm handling with unlang
- Special note for Microsoft NPS Configuration - setting the Framed-MTU attribute in Roaming User Network Policy
- Testing your Configuration - shared secrets check; authentication against local database; remote authentication
- Configure Peering with orther RADIUS servers on your network
- Configure Attribute Filtering
- Configure Injection of Operator-Name Attribute (FreeRADIUS, Radiator, Aruba ClearPass, latest Cisco ACS/ISE only)
- Configure Rejection of Malformed Usernames
- FAQs/Resources

10.1 Configure Peering with NRPSs

This step is to complete the peering of your ORPS with the NRPS by setting the NRPS as clients of your ORPS

To complete the process of peering your ORPS with the NRPS you must add all three NRPS as RADIUS clients on all of your ORPS systems (hint - edit clients.conf and proxy.conf files). Roaming0.ja.net, roaming1.ja.net and roaming2.ja.net (194.82.174.185 ; 194.83.56.233 ; 194.83.56.249) must have full authentication and accounting passes - allowed as clients on your ORPS.

If you use hostnames rather than IP addresses in your proxy configuration (FreeRADIUS: proxy.conf) it is recommended that you add the hostnames and IP addresses of the NRPS to the hosts file rather than relying on your ORPS doing a DNS lookup. This eliminates one potential issue - and ensures that the ORPS are able to send auth requests even if there's a problem with DNS.

The NRPS clients configuration must be set to use UDP ports 1812/1813 (authentication and accounting). The NRPS will not **listen** on anything other than the proper RADIUS ports 1812 and 1813. If your ORPS needs to use ports 1645/46 (inbound), these should also be configured - the NRPS will send on these if you have set the configuration so, as detailed in section 9 above.

The shared secrets with the NRPS are generated by the Support web site, as described above.

Accuracy is essential when transcribing the shared secrets to the configuration files. It should be remembered that these are used independently to validate and encrypt client (NRPS remote authentication) and proxying (visitor authentication forwarding from ORPS) connections. An error in one of the shared secrets can lead to confusing problems such as i) remote authentication working whilst visitor authentication fails ii) unreliable performance due to authentication failure occuring when one NRPS is utilised whilst successful authentication is achieved through the others.

The following applies to Microsoft NPS and IAS implementations only - it is essential for these systems. When setting up the NRPS as clients in Win2008 NPS it is essential to check that the Vendor Name for the three NRPS is set to ‘RADIUS standard’ and not ‘Ascend Communications’ in the NPS/RADIUS clients and servers/RADIUS clients configuration tree in the Server Manager. Open Server Manager, navigate down Roles/Network Policy and Access Services/NPS/RADIUS Clients and Servers/RADIUS Clients. The RADIUS clients pane will display the IP Address and Vendor Name (Device Manufacturer) that has been set. Device Manufacturer should be ‘RADIUS Standard’.

In the case of IAS, even if the Client-Vendor name is correctly set in the NRPS client properties to RADIUS Standard, Access-Requests containing Operator-Name will still be dropped. The solution is a little more involved and it is necessary to modify an IAS database file as below. It is however essential that MS IAS sites carry out this fix at the earliest opportunity.

1. Stop the IAS Service
2. Make a backup copy of c:\windows\system32\ias\dnary.mdb
3. Open c:\windows\system32\ias\dnary.mdb in MS Access
4. Open the 'Attributes' table
5. Scroll down to attribute number 126
6. Change the Name to Operator-Name
7. Change the Syntax to String
8. Close Access, and start IAS

The dnary.mdb file can be copied to another machine for editing if you do not have Access on your IAS server.

These instructions and the background to this requirement are described in the following Janet Advisory:

Janet Advisory: MS IAS and NPS Operator-Name RADIUS attribute issue (Nov 2010) - notification of critical issue affecting participants that have implemented Microsoft IAS and NPS ORPS - urgent action required.

Resources:

- eduroam wiki - Radiator RADIUS Client Definition [5]
- eduroam.org wiki - Microsoft IAS RADIUS Client Definition [6]
- Running eduroam on NPS with Windows 2008 R2 Enterprise [7] (SURFnet draft doc - nb contains SURFnet-specific screenshots)
- eduroam.org wiki - FreeRADIUS Client Definition [8]
- 'FreeRADIUS Beginner's Guide' book by Dirk van der Walt; Packt Publishing ISBN 978-1-849514-08-8

10.2 Configure Realm Handling, Proxying, RADIUS server timeouts and Load Balancing

This step is to configure your ORPS to handle auth requests originating from your network APs/controllers: forwarding Access-Requests from Visitors to the NRPS and (if applicable) forwarding Access-Requests from local users to your local authentication system.

The next stage is to configure the handling of RADIUS Access-Request packets from your network NAS systems (APs, WLCs and [if you support wired .1X connection] switches) by your ORPS. The aim is to handle Access-Request packets arising from your users authentication requests locally while Access-Requests arising from visiting users need to be forwarded to the NRPS servers. How you go about achieving this is dependent on the RADIUS platform you have deployed. FreeRADIUS and Radiator use unlang script language/PERL and in the case of FR, virtual servers which are dedicated to particular tasks and which can be tuned for best performance, whilst Microsoft NPS and Cisco ACS/ISE require policies to be defined and configuration carried via GUI.

Authentication of your own users should be considered as a separate logical process from Access-Request packet handling/'proxying'. This is covered later in section 13.

To save having to revisit this part of your configuration at a later stage, it is worthwhile tackling the issue of dealing with badly-formed usernames during this setup stage. Due to the huge number of users of eduroam and explosive growth over recent years, this is an important topic. Dealing with badly formed usernames applies to both local authentication of your own users and forwarding of auth requests for visitors. The object of filtering invalid realms is covered in the separate advisory document Filtering of Invalid Realms [9]. How put this into practice with FreeRADIUS is covered below in section 10.3 and for Microsoft NPS the Microsoft NPS 2008R2 config to avoid bad usernames flooding NRPS [10] document and in the eduroam(UK) NPS Implemention Guide to be published shortly.

If using FreeRADIUS it is recommended you review our FreeRADIUS Demystified seminar material [11]. [Configuration will include editing your proxy.conf file to define your local realm and editing the authorize section of radiusd.conf to program the proxying logic. More details in section 10.3 below.] When setting up a FreeRADIUS server we'd recommend you run the server in full debug mode (freeradiusd -X or radiusd -X depending on whether it was installed by APT or from source) to enable you to see exactly what is going on for each packet and the decisions/checks the server is making as you develop the configuration.

How requests are handled and how different RADIUS server modules should authenticate and authorise the users must be configured.

Points to consider:

a) It is a requirement that ALL users (home users and visitors) authenticating via eduroam MUST have a realm component in their username (ie must be of the form ' userID@camford.ac.uk [12]') and that the Visited site realm handling logic drops any authentication request without a realm name in the outer id. This is to avoid a situation where your users have used a simple username eg. 'fred' to authenticate whilst connecting to eduroam at your organisation and then find that they cannot gain authentication when visiting another eduroam site. The problem would be that the Visted site ORPS will not recognise the user name and should drop it, but even if it did forward the Access-Request to the NRPS, the NRPS will not know where to forward the request to and so will drop it, returning an Access-Reject including explantory text. Do NOT permit authentication based on a simple username - insist that the username contains @realm.

b) Consideration should be given as to how both "outer" stage 1 identities and "inner" stage 2 identites are handled. You should **not** permit proxying of inner ID off to other organisations in cases where the inner ID realm is not your organisation - such authentication attempts should be allowed to fail. (E.g. Your RADIUS server handles an authentication request for outerID user@myorganisation.ac.uk [13], but during the auth process encounters an innerID of user@camford.ac.uk [14] - your ORPS must drop this auth request).

c) It is essential that your ORPS does not forward an authentication for a user from your own realm or a sub-realm to the NRPS. That would create a potential authentication loop as the NRPS would rightly return the request to your ORPS. Because such authentication loops are highly resource-hungry this situation would create a threat to the eduroam service. The NRPS have anti-auth-loop logic which drops such loop-forming requests, which protects against this threat - but please note that sending auth-loop triggers are explicitly prohibited by the Technical Specification.

d) (Advisory applicable only to FreeRADIUS and Radiator) - it is possible to set up your ORPS to be too "open" with regard to forwarding authentication requests, which can make interpretation of logs very difficult. A unsatisfactory situation can arise if your ORPS is configured to forward requests based on inner identities in addition to forwarding based on the mandatory outer ids. The default on FreeRADIUS is too open and should be closed down. By default Radiator is fine, but it is possible to set up undesirable forwarding based on inner id.

e) Only error-free authentication requests should be forwarded to the NRPS. So for example if your ORPS receives a RADIUS packet with a bad EAP-Authenticator then that packet should be dropped at your ORPS. Bad EAP-Authenticators can arise if internal NAS systems on your network (APs and WLCs) have incorrect shared secrets with your ORPS. If the NRPS receives an Access-Request containing a bad EAP Message-Authenticator, the packet will be dropped and an error entry will be made in the NRPS log. This is potentially a very serious situation since your systems could flood the NRPS with bad packets - which will result in us applying a block to your ORPS.

f) The order in which your ORPS communicates with the three NRPS should be considered. Many participants are tempted to order the three NRPS in the order: roaming0, roaming1, roaming2. The effect of this would be that roaming0 becomes the most heavily loaded of the three national proxies. In order to ensure the best responsiveness for your ORPS and to help avoid overloading any particular NRPS, it is recommended that you order the NRPS in your proxy configuration randomly.

g) Load balancing of communications with the NRPSs should be set up. However the method used must be such that all RADIUS conversation in relation to any one particular authentication event is directed through only one NRPS for the duration of the conversation. Problems arise if proxy state and conversation sequence do not tally at the NRPS.

Radiator 3.1 and up, MS IAS, NPS, Cisco Secure ACS and FreeRADIUS 2.x all have good EAP load balancing capability, but older software, such as FreeRADIUS 1.x, must only be used in 'fail over' mode rather than 'load balance' (ie. use fail_over in proxy.conf, not round_robin).

h) RADIUS server timeout should be set to ensure that authentication requests forwarded to the NRPS (for onwards forwarding to your visitors' home ORPSs) is sufficiently long to allow a response to be provided. Bear in mind that some visitors may be from distant eduroam federations and that several RADIUS hops may be involved. A timeout of 30 seconds is recommended. So taking the example of Microsoft NPS, the following settings are suggested:

Number of seconds without response before request is considered dropped: 30

Max number of dropped requests before server is identified as unavailable: 5

Number of seconds between requests when server is identified as unavailable: 30

i) **It is essential that your ORPSs do not mark all of the NRPS as 'dead' should no reply be received from the NPRS when handing off visitors' authentication requests to the NRPSs for onward authentication by the visitors' Home ORPS.** There are logical reasons why the NRPS may not reply to your ORPS and whilst you should configure fail-over between the NRPSs in case of genuine NRPS unavailability, potentially serious communications breakdown can occur if your ORPS marks the NPRSs as dead for the wrong reason.

Remember it is not the NRPS that authenticate your visitors, it is the Home sites. The NRPS simply acts as proxy and waits for a response from the Home site. This can take some time, especially if the visitor is from outside the UK. It should also be noted that some RADIUS implementations (e.g. Microsoft NPS) behave in an unhelful manner if they receive authentication requests they have difficulties with. If they recieve a request for an unknown user or if the request contains an unknown attribute, rather than respond with an Access-Reject, they simply drop the request and remain silent. The NRPS keeps the connection open, waiting for a reply, tying up NRPS resources and your ORPS recieves no response from the NRPS. The NRPS do retry the remote Home server a second time, but if there is no further response, the next Home ORPS is tried. NRPSs only act as proxies, cannot act as EAP end points and so cannot formulate Access-Rejects containing reason for failure messages. They will only forward error messages returned in RADIUS packets from the legitimate remote Home site.

Since your ORPS only knows about its immediate neighbours, i.e. the NRPSs, it may appear that the NRPS has not responded to a proxied authentication request. If your ORPS marks the NRPSs as unresponsive, zombie or dead, a serious communication breakdown can develop. The problem is that the NRPS is not dead, it is simply waiting for a response from the users' home server. So if your ORPS stops talking to the NRPS it was in dialogue with, when the NRPS sends an Access-Request for one of your roaming users and your ORPS does not respond, **your** ORPS will be marked as dead. (Due to hierarchical nature of RAIDUS communications, the NRPS are entitled to make this decision, you OPRSs are not).

You must configure your ORPS to avoid rogue behaviour - i.e. it is essential that your ORPSs do not mark all of the NRPS as 'dead' should no reply be received from the NPRS when forwarding visitors' authentication requests. If your RADIUS server supports Status-Server (FreeRADIUS and Radiator) you should set up your ORPS to use that.

10.3 FreeRADIUS Example Configuration - proxy, client and foreign realm handling with unlang

We have put together an example configuration of a FreeRADIUS ORPS (both v 1.1.x and 2.x) here: example FreeRADIUS ORPS configuration on eduroam Support server [15]

The first section covers configuration of the NRPS servers as proxy authenticatprs and clients.

About a third of the way down there is script for the authorize stanza in your proxy.conf file for your default virtual server to:

a) enforce use of full userID@realm [16] username format

b) reject bad usernames against a sequence of common error criteria, returning reason for rejection in the reply-message

c) check for properly formed usernames in auth requests and only for valid forms, detect your local realm and hand off to local realm processing

d) hand off auths for non-local realms to eduroam realm processing

10.4 Special Note for Microsoft NPS Configuration - Setting the Framed-MTU Attribute in Roaming User Network Policy

By default NPS uses a maximum size of 1500 (was 2000) bytes for its datagrams. If it is sending a certificate (whose size may exceed this), the Ethernet packet created will probably be fragmented and this may result in the datagram to be lost in transit where packet fragmentation is rejected (this is why we specify you must NOT configure reject fragments at your firewall). If this happens, the EAP interaction will never complete. This causes NPS to log a discard for your roaming user authentication, for some reason claiming that the incoming packet was incorrectly formatted. Even if the client sends a Framed-MTU attribute itself, NPS will ignore it. However, if you set the Framed-MTU attribute in the Network Policy involved, NPS will use the value you specify for its own packets.

[The author of this tip notes: 'We were seeing this problem initially with responses to the test authentication requests that the NRPSs send every few minutes. I got the details from a Cisco article (http://www.cisco.com/c/en/us/support/docs/lan-switching/8021x/118634-technote-eap-00.html [17]). Since implementing the change, I've noticed that authentication attempts from a number of clients which were failing previously are now working.']

How to set the Framed-MTU attribute size in Microsoft NPS:

From the NPS console, double-click Policies, click Network Policies, and then in the details pane double-click the policy that you want to configure - refer to our NPS config guide for the policy that forwards Visitor authentication requests to the NRPSs.

In the policy Properties dialog box, click the Settings tab.

In Settings, in RADIUS Attributes, click Standard. In the details pane, click Add. The Add Standard RADIUS Attribute dialog box opens.

In Attributes, scroll down to and click Framed-MTU, and then click Add. The Attribute Information dialog box opens.

In Attribute Value, type a value equal to or less than 1344. Click OK, click Close, and then click OK.

10.5 Special Note for NPS Configuration - Tuning NPS for authentication with eduroam

https://community.jisc.ac.uk/library/network-and-technology-service-docs... [18]

10.6 Testing your Configuration

Once the ORPS(s) have been configured, authentication can be tested using the test tools on the eduroam Support web site as described in section 12.

Shared secrets check. In scenarios involving multiple ORPSs, it is advisable to test each ORPS independently for correct configuration. Shared secrets can be checked by simply running a command line test on each of the ORPS. Note that whilst FreeRADIUS, Radiator and MS IAS/NPS include utilities for cleartext password based authentication methods such as PAP, **this is no longer supported by the eduroam(UK) infrastructure**, so please do not attempt to use radtest, radpwtst or NTRadPing.

a) If you have not hooked your Wi-Fi service in to your RADIUS server, the simplest test involves using a command line tool to try to send Access-Request packets to the NRPS for forwarding to the eduroam Support ORPS for a test user belonging to the eduroam(UK) realm. (This is a command line variation of the standard visitor authentication simulation test - see section 12 below). Nb As specified in section 5 above, you **must** register a test user account complete with password for your site on the Support server. You should also create a test user account with the registered credentials as a local account on your RADIUS server or an account in your user database). Remember, any changes your make to your config on eduroam Support can take up to an hour to take effect.

Test tools (linux and Windows): http://techgenix.com/testing-monitoring-tools-radius-servers/ [19]

NTRadPing (PAP/CHAP test only - **do not attempt to use this!**): https://support.secureauth.com/hc/en-us/articles/360019651812-How-To-Tes...

[20]. Support server no longer supports plain PAP authentication.

Radius Test: https://radiustest.software.informer.com/download/ [21]

eapol_test is included in wpa_supplicant which is an opensource supplicant that can be acquired from http://w1.fi/wpa_supplicant/ [22]

The eapol_test commands would be:

```
eapol_test -c<test.conf> -aroaming0.ja.net -p1812 -s<shared secret
for roaming0>
```

```
eapol_test -c<test.conf> -aroaming0.ja.net -p1812 -s<shared secret
for roaming1>
```

```
eapol_test -c<test.conf> -aroaming0.ja.net -p1812 -s<shared secret
for roaming2>
```

See https://www.systutorials.com/docs/linux/man/8-eapol_test/ [23]

For hints on how to build the test.conf file see https://www.systutorials.com/docs/linux/man/5-wpa_supplicant.conf/ [24]

(Radpwtst for Radiator may include PEAP/EAP alternatives to PAP for the more advanced user.)

b) If you have peered your Wi-Fi controller/AP to the RADIUS server you can simply use the test account credentials to try to send authentication requests for the user <your realm>@eduroam.ac.uk to the NRPS

Authentication tests against your local realm user database / test auth requests from remote sites In order to carry out this test you must have a test user account on your site with a valid password (eg. a local account on the RADIUS server or an account in your user database) and registered it on the eduroam Support server as specified in section 5. You then have a variety of options for testing authentication at your realm - using the remote eduroam Support server or locally from (one of) your ORPS. The tests described below involve interaction with the NPRS, you can however use radtest locally against a specific host.

The eduroam Support server has a remote user test feature for ORPS in normal 'production' mode - see section 12.

If you wish to run authentication tests involving the NRPS from (one of) your ORPS you must first set the target ORPS as a 'test-development' server in the eduroam infrastructure. This can be done via the relevant RADIUS proxy servers page on the eduroam Support server. With this setting, ONLY packets with 'test' prefixing your realm name will be sent to your ORPS. This facility is detailed in section 12; Testing a new ORPS within eduroam Infrastructure before bringing it into production use. CAUTION - there is a danger that auth-loops can be created, so it is essential that the local test user account is valid and that you use credentials accurately. At the end of your test session, you must check your logs to ensure that no auth-loop has been initiated.

If you (temporarily) configure the test ORPS forwarding policy to send all access-requests with realm ('@xxx') suffixes to the NRPS, then when you use 'testuser@test.yourrealm [25]' with radtest, the NRPS will process the request and send the access-request back to your ORPS. (Nb. if you have a group of ORPSs then this request could be sent to ANY **one** of the individual servers since the NRPS sends to the first ORPS in its list that it finds is not busy). Nevertheless the three lines of radtest commands are useful to verify that the ORPS can talk to all three NRPS - ie that there are no bad secrets and no firewall problems! If you do have multiple ORPSs you could always turn off the other ORPSs while doing each test - which would guarantee that only the ORPS being tested would be sent the return access-request. This would verify that the ORPS under test could be reached from each NRPS in turn).

Assuming that the test account can be authenticated using PAP, the FreeRADIUS command would be:

```
Radtest testuser@test.your_realm <password> roaming0.ja.net 1812
<shared secret for roaming0>

Radtest testuser@test.your_realm <password> roaming1.ja.net 1812
<shared secret for roaming1>

Radtest testuser@test.your_realm <password> roaming2.ja.net 1812
<shared secret for roaming2>
```

10.7 Configure Peering with other RADIUS servers on your network

If you choose to implement multiple organisation RADIUS proxy servers for resilience or performance/load sharing, you will have to configure peering between them.

10.8 Configure Attribute Filtering

Frequently organisations make use of attributes within RADIUS packet during the Access-Request / Challenge and Accounting exchanges to check user/machine parameters or to control how users are given access to the network. Such exchanges are frequently of local relevance only and can cause problems during remote authentication attempts. Filtering of all but the most essential RADIUS attributes from the returning packets should therefore be implemented to avoid the local access point at the Visited site receiving attributes it doesn't know how to handle.

Once you have configured attribute filtering, you can test your filter by selecting the 'Poisonous Access-Accept packets' option for the Visitor Authentication Simulation test - which will result in the returned Access-Accept containing a set of attributes that are known to cause problems. See section 15 for further details about the Visitor Auth Simulation test and this feature.

Hint, for FreeRADIUS ORPS - you can determine what attributes are being sent in Access-Request packets by running your server in debug mode or you can run radmin to see what attributes you are sending to the NRPS. Alternatively you could packet capture and then look at the packets in Wireshark.

First off though, the following is the set of attributes required (at a minimum) to support eduroam, as listed in the Technical Specification. These **must NOT** be filtered out:

RADIUS Access-Request or Access-Challenge message attributes:

1. User-Name
18. Reply-Message
24. State
25. Class
31. Calling-Station-ID
33. Proxy-State
79. EAP-Message
80. Message-Authenticator
    MS-MPPE-Send-Key
    MS-MPPE-Recv-Key
89. Chargeable-User-Identity
126. Operator-Name

RADIUS Accounting messages:

1. User-Name
25. Class
33. Proxy-State
40. Acct-Status-Type
44. Acct-Session-ID

This list has been determined following a small number of incidents involving roaming eduroam users being unable to connect at certain institutions (both here in the UK and elsewhere) owing to over-restrictive attribute filtering. Please note that implementation of the list is likely to become a mandatory feature of eduroam.

How to set up attribute filtering? Hint for FreeRADIUS ORPS sites - in your pre-proxy section activate filtering:

```
pre-proxy {

    attr_filter.pre-proxy
```

Then in attrs.preproxy set your attributes. Something like:

```
DEFAULT

    Service-Type == Framed-User,

    Service-Type == Login-User,

    Login-Service == Telnet,

    Login-Service == Rlogin,

    Login-Service == TCP-Clear,

    Login-TCP-Port <= 65536,
    Framed-IP-Address == 255.255.255.254,
    Framed-IP-Netmask == 255.255.255.255,
    Framed-Protocol == PPP,
    Framed-Protocol == SLIP,
    Framed-Compression == Van-Jacobson-TCP-IP,
    Framed-MTU >= 576,
    Framed-Filter-ID =* ANY,
    Reply-Message =* ANY,
    Proxy-State =* ANY,
    EAP-Message =* ANY,
    Message-Authenticator =* ANY,
    MS-MPPE-Recv-Key =* ANY,
    MS-MPPE-Send-Key =* ANY,
    MS-CHAP-MPPE-Keys =* ANY,
    State =* ANY,
    Session-Timeout <= 28800,
    Idle-Timeout <= 600,
    Calling-Station-Id =* ANY,
    Called-Station-Id =* ANY,
    Operator-Name =* ANY,
    Chargeable-User-Identity =* ANY,
    Port-Limit <= 2
```

Make sure you properly test any changes.

For more information on this topic see:

- List of RADIUS Attributes [26]
- RADIUS Attributes [27]
- RADIUS Attribute Filtering with Microsoft IAS and NPS [28] - the role of attribtues during authentication and VLAN assignment; why do we need to configure attribute filtering; the issue with MS IAS and NPS; how to set up filtering with IAS and NPS

- Improving reliability of Microsoft NPS as an authentication provider for eduroam [29]
- Attribute Screening for Access Requests on Cisco Network Access Server [27]

10.9 Configure Injection of Operator-Name Attribute (FreeRADIUS and Radiator only)

If you are deploying a FreeRADIUS, Radiator, Aruba ClearPass or Cisco ACS v5.4, you should configure your system to inject the Operator-Name attribute, correctly formed for your organisation, into Access-Request packets forwarded to the NRPS. The background, rationale and one method of achieving this are documented in Advisory: Injection of Operator-Name attribute (Aug 2011) [30].

10.10 Configure Rejection of Malformed Usernames

Sending Access-Request packets to the national proxy infrastructure with malformed 'bad' usernames, more particularly those with errors in the realm component, is bad practice; definitely not good-neighbourly. Due to the prevalence of misentered usernames in laptops and mobile phones and in the case of the latter, the 'auto-correct' feature of the phone software compounds this problem, the NRPS are bombarded with Access-Requests that will never result in successful authentications. Instead, the finite resources of the NRPS become tied up waiting for responses from the Home ORPS or from the eduroam.org ETLRs in the case of non-existent non-UK realms. To avoid the above situation you should configure your ORPS to drop authentication attempts by clients with bad usernames. Bad usernames are essentially those that do not conform to 'username@FQDN [31]' - the formal description can be found in RFC 4282, which is largely correct.

To avoid the above, FreeRADIUS depoyments should utilise the Policy engine. There are now numerous examples included in the FreeRADIUS config. It is also possible to avoid the above situation is described at:www.wireless.bris.ac.uk/netcomms/eduroam-realm-checks.conf [32].

For Microsoft NPS and IAS this is described at: Microsoft NPS 2008R2 config to avoid bad usernames flooding NRPS [33].

NB. There is nothing that can be done at present to avoid the RADIUS infrastructure from being hit by Access-Requests from users who have left their organisation but still have eduroam credentials configured in their devices. User education to remove eduroam configuration from devices when they leave is the best current solution.

10.11 Resources/FAQs

- Complying with the Technical Specification [34]
- Inter-NREN Roaming Infrastructure & Service Support Cookbook [35] (pdf) (produced and published by GEANT2)
- Configuration examples and hints for FreeRADIUS on eduroam Support Website [36]
- eduroam.org guide: Setting up FreeRADIUS server for Visited service [37]
- Advisory: Filtering bad realms from auths sent to the NRPS [38]

Troubleshooting Microsoft IAS as a RADIUS server and as a RADIUS proxy

This link to the MS TechNet site should be useful:

- Microsoft TechNet IAS Troubleshooting [39]

Is it possible to authenticate EAP-PEAP against Novell Directory Services?

While it is not possible to authenticate EAP-PEAP against the default non-reversible hash used in NDS, it is now possible to configure a "Universal Password" in NDS which stores users' passwords in a reversibly encrypted format. This will permit the authentication of EAP-PEAP against NDS through RADIUS servers such as FreeRADIUS and Radiator.

How do you configure FreeRADIUS against Novell eDirectory?

Novell has produced documentation on configuring FreeRADIUS against eDirectory:

- http://www.novell.com/documentation/edir_radius/index.html [40]

Are there any example configurations for Radiator available?

We currently don't have any direct cut'n'paste for Radiator that is clearly available for any site due to the uniqueness of each site requirement (backend authentication and such).

However, Radiator supplies many example configuration file snippets and templates.

eg ntlm_eap_multi.cfg which is a simple config which handles Radius PAP, CHAP, MSCHAP and MSCHAPV2 and also handles the outer and inner requests for TTLS and PEAP. In this case, the <AuthBy NTLM> sub-handler is doing the work. Of course this is only suitable for Active Directory. If sites are using passwords or eDirectory etc then the requirements will be different.

Also appendix A.2 of the Geant2 Roaming Infrastructure Service and Support Cookbook [35] provides useful information on configuring the ORPS server software.

Are there any example configurations for FreeRADIUS available?

We don't have any direct cut'n'paste configurations for FreeRADIUS that would be suitable for all sites due to the uniqueness of each site requirement (backend authentication etc).

However there are some hints and tips on the eduroam Support website [36] and there is some useful information in the following case study, which is a practical description of how University of Bristol implemented and complies with the Technical Specification using FreeRADIUS in an AD environment: A Case Study in Complying with the Technical Specification [34].

Also appendix A.2 of the Geant2 Roaming Infrastructure Service and Support Cookbook [35] provides useful information on configuring the ORPS server software.

FreeRADIUS integration with Active Directory

The received way of setting up FreeRADIUS to authenticate users against Active Directory is to use Samba/winbind/ntlm_auth:

FreeRADIUS Active Directory Integration Howto - from FreeRADIUS Wiki [41]

University of Bristol implemented FreeRADIUS in an AD environment, the following case study contains useful information: A Case Study in Comlying with the Technical Specification [34].

How do I change the IP address of our ORPS? (Is there a procedure we need to go through?)

You need simply to use the https://support.roaming.ja.net [42] eduroam support site. Go to your ORPS configuration page and select your ORPS, change the name of the RADIUS server and press [Update RPS]. Check that the passphrase does not change (it should not). The final step is to remove the old ORPS entry and add the new one. The passphrase will be different then. The changes are propagated to the NRPS on the hour.

11. Wi-Fi Service and Establishment of a VLAN/Network Service for eduroam

eduroam Wi-Fi service

The steps involved in establishing an eduroam Wi-Fi service are:

- Enabling 802.1X on your Access Points or Wireless LAN Controllers
- Peering APs/WLC with your ORPS (ORPS are RADIUS servers to APs and APs are RADIUS clients of ORPS)
- Set up radios and wireless LAN - RF bands to be used for each standard, define WLANs, enable WPA2/AES cipher
- Setup eduroam SSID
- eduroam VLAN setup
- Configure authenticated user connection policy - VLAN connection/dynamic VLAN assignment
- Tune EAP timers, RADIUS server timeout and other WLAN parameters

Most organisations provide eduroam over a Wi-Fi service although eduroam may alternatively or in addition be provided over wired infrastructure. Wi-Fi is typically the 'front-end' by which most users would prefer to connect, since this supports the laptop, tablet and smartphone devices that are most popular with users.

Many organisations have used the deployment of eduroam to simplify their wireless network offering. This can result in reduced management overhead and improved overall Wi-Fi performance and can be achieved by combining eduroam as the primary ESSID with multiple dynamically assigned VLANs as described below, together with a further small number of ESSIDs e.g. for an open captive portal network for first time users to provide access to device setup utilities or for a guest network for non-eduroam visitors.

To establish an eduroam Wi-Fi service, you need to configure the organisation's APs to broadcast the eduroam SSID, the APs need to be set to use 802.1X/AAA-RADIUS-authentication and be defined as clients of the RADIUS server. Then the APs need to be configured to forward authentication requests from the Wi-Fi devices associating to the eduroam SSID to your RADIUS server(s). Upon receipt of an validated authenticated request (an Access-Accept) the APs must connect the device to your **eduroam network**, described below.

If you want to use dynamic VLAN assignment as described below (assigning users to specific VLANs based on information received from the RADIUS server) then the APs must be configured to do this. (Other activities performed by the APs include exchange keying material (initialisation vectors, public and session keys, etc.) with client systems to prevent session hijacking).

Resources:

- eduroam.org wiki - Wi-Fi network set up guide for implementing eduroam Visited services [43] (highly recommended - very thorough!)
- WLAN Network Infrastructure [44] - Geant Best Practice Guide (2011)
- Using eduroam as the single primary SSID [45]
- Cisco WLCs Wi-Fi tuning tips for eduroam [46]

eduroam network

Visited organisations must implement one (or more) dedicated network/VLAN(s) to provide eduroam network services. All eduroam networks must comply with the eduroam(UK) Tech Spec (access to the Internet permitting use of (at least) the defined key ports and protocols - see Firewall section). Any eduroam network/VLAN must not be shared with any other network service. Authenticated Visitors must be connected to such an eduroam network service.

Most participating organisations permit their own users to connect via the organisation's eduroam Wi-Fi service. If this is not permitted, this must be clearly stated on the organisation's eduroam Service Information web page. Organisations may connect local users to the mandatory Visitors' eduroam network service, but alternatively may connect them to a more appropriate local network. This can be achieved through 'dynamic VLAN assignment' (which is the more efficient alternative to the fixed SSID-VLAN mapped solution). Such local networks may be used to for example satisfy the following requirements:

- provide access to local resources that the organisation wishes to be accessed only by its own users/specific groups of users
- provide a security environment required for local users/specific groups of users
- enable local users connecting their own personal devices to be connected onto an 'untrusted network'
- provide a remedial network environment for devices requiring AV updates, OS-patches etc.

Detailed information about how to set up dynamic VLAN assignment is beyond the scope of this guide, but essentially involves configuring your RADIUS server to return a value in the relevant attribute in the Access-Accept based on the policy you define for the particular user or user-group. The AP needs to be configured to act upon the attribute value and to connec the device to the appropriate VLAN. There are many guides available on the Internet, one of which is Allied Telesyn's How To user 802.1X VLAN Assignment [45].

Nb. The minimum set of open ports and protocols for eduroam network services defined in the eduroam(UK) Tech Spec does NOT apply to non-eduroam network services that a participating organisation may choose to connect local users to.

Requirements for eduroam network/VLANs:

- The Wi-Fi service that connects to the eduroam network service must use a broadcast SSID of 'eduroam' (**which must be lowercase**)
- DHCP must be employed to allocate IP addresses
- Only IEEE 802.1X is permitted for the eduroam network; no form of WRD/captive portal is permitted, although you may implement this on other networks such as device setup and remediation networks
- IEEE 802.1X NASs must support symmetric keying using keys provided by the Home organisation within the RADIUS Access-Accept packet
- Only a single user is permitted per NAS port except where 'thin client'/controller-based systems are employed
- IPv4 addresses must be allocated to visitors using DHCP
- The IPv4 addresses allocated to visitors and the corresponding MAC addresses must be logged
- NAT address mappings, if used must be logged
- Routing of IPv6 on the eduroam visitor VLAN ideally should be supported
- NAT is permitted
- WEP must not be implemented on the eduroam Wi-Fi service that connects to the eduroam network service
- TLS interception proxies/filters must not be employed on the eduroam network service for visitors

Visited organisations may implement IPv4 and IPv6 filtering between the visitor VLAN and other external networks, providing that this permits the forwarding protocols detailed in the Firewall Configuration section.

Resources:

- eduroam.org wiki - Wi-Fi network set up guide for Visited services - Aruba, Cisco, Meru, Trapeze, wired [43]
- eduroam.org wiki - Configuring request forwarding in FreeRADIUS (proxy.conf) [47]
- eduroam(UK) Technical Specification [48]
- Deploying MS IAS with VLANs [49]

?12. Firewall Configuration to Support eduroam Network Service

If not done already, your organisational firewall must now be made ready for the eduroam Visitors network service.

An important aim of eduroam is to provide visitors with unimpeded access to the Internet, not least because this maximises the probability of a visitor's applications working as expected. The Tech Spec therefore requires that at least the core list of protocols listed in the talble below must be permitted. You may of course open additional ports and protocols if your local policy is more liberal.

Note, if member organisations wish to absolutely ensure that their own users, when roaming, have or a wider range of ports/specific additional ports available than the minimum listed, they could provide their users with a (supported) VPN service through which the home site could control the availability of required ports and protocols.

Similarly, the Visited service providing organisation need only comply with the list for their eduroam visitor network. If you connect your own users (through your eduroam Wi-Fi service) to an alternative network service more appropriate for local users, you are **not** required to adhere to the minimum list (and you may be more restrictive or more open).

One approach worth considering is to offer a fairly open Visitied service network with just the ports and protocols suggested in the following document blocked and also SMTP/port 25 blocked https://community.jisc.ac.uk/library/janet-services-documentation/blocking-lan-service-ports [50]. Your own users when at home could be connected to a network service compying with your policy for local users.

Mandatory Open Ports and Protocols:

Passive (S)FTP:	TCP/21	egress and established
SSH:	TCP/22	egress and established
IPv6 Tunnel Broker Service:	IP protocol 41	egress and established
PPTP:	IP protocol 47 (GRE) and TCP/1723	egress and established
ESP:	IP protocol 50	egress and established;
AH:	IP protocol 51	egress and established
HTTP:	TCP/80	egress and established
POP:	TCP/110	egress and established
NTP:	UDP/123	egress and established
IMAP4:	TCP/143	egress and established
IMAP3:	TCP/220	egress and established
LDAP:	TCP/389	egress and established
IMSP:	TCP/406	egress and established
HTTPS:	TCP/443	egress and established

ISAKMP: and IKE:	UDP/500	egress
LDAPS:	TCP/636	egress and established
SMTPS:	TCP/465	egress and established
Message submission:	TCP/587	egress and established
IMAPS:	TCP/993	egress and established
POP3S:	TCP/995	egress and established
OpenVPN:	UDP 1194 and TCP 1194	egress and established
Citrix:	TCP/1494	egress and established
SQUID Proxy	TCP/3128	egress and established
RDP:	TCP/3389	egress and established
IPv6 Tunnel Broker NAT traversal:	UDP/3653 and TCP/3653	egress and established
IPSec NAT traversal:	UDP/4500	egress and established
VNC:	TCP/5900	egress and established
AFS:	UDP/7000 through UDP/7007 inclusive	egress and established
HTTP Proxy:	TCP/8080	egress and established
Cisco IPSec NAT traversal:	UDP/10000 and TCP/10000	egress and established

You may have additional ports and protocols open as permitted by your local policies.

The above list is subject to change, so you should refer to the current published eduroam(UK) Technical Specification, which provides the definitive listing.

13. RADIUS server configuration for Home service - interoperation with user database

Configure Authentication of Preferred EAP Types

Home organisations must configure their RADIUS server (eg.edit the eap.conf file) to authenticate one or more EAP (Extensible Authentication Protocol) types as specified in the Technical Specification.

Interoperation with User Database

For each home realm authentication request handled by the ORPS, the RADIUS server generally has to interrogate the user database (LDAP, NDS, AD). The interoperation of the RADIUS server with the backend user database is often the most problematic part of implementing 802.1X. Whilst there are a number of well known techniques and software combinations, since each institution's environment is unique, detailed guidance about this is beyond the scope of this overview.

A note on the use of anonymous outer identities: the majority of the most often depolyed EAP methods (PEAP/MSCHAPv2, EAP-TTLS/*, EAP-FAST) use a two-stage authentication process (EAP-TLS is certificate based and is not a two-stage process):

- the first stage uses the realm component only of the 'outer identity' username to enable the client to be connected to the appropriate authenticator (identity username = userID@realm [16])
- the second stage uses the cryptographically protected 'inner identity' username for the actual authentation of the user (and the authentication server actually uses the userID and is not normally concerned with the realm component of the username that is presented)

Note that RFC 4282 permits the use of anonymous outer identities the aim of which is the better preservation of privacy for your users. Therefore the RADIUS server configuration of a Home service should permit the use of anonymous/blank userID in the outer identity, ie the value the user inputs when enabling 'Enable Identity Privacy'/ 'Anonymous identity' and the RADIUS server configuration of a Visited service MUST permit the use of anonymous/blank userID.

A note for Microsoft NPS server deployments: see p51 on https://community.jisc.ac.uk/system/files/257/eduroam%28UK%29%20Microsof... [51] - when configuring the Connection Request Policy for your roaming users be sure to tick 'Override network policy authentication settings’ and Add the EAP Type of 'Microsoft: Protected EAP (PEAP)'.

More in depth advice on configuring RADIUS-database interaction is available in various documents:

- Connecting FreeRADIUS to AD and LDAP User Database [52] - Geant Best Practice guide (2013)
- eduroam(UK) Microsoft NPS Configuration Guide [53]
- Aruba Wireless Controller and ClearPass Configuration guide [54] - Geant Best Practice (2016)

A note on FreeRADIUS with LDAP based systems: the authentication handling flow is as follows - after the prefix module has run, the 'Stripped-User-Name' attribute gets populated with the userID part of the username (e.g. 'a123467'/'fred.smith') - you then use that in your LDAP configuration (ie %{Stripped-User-Name}) with the relevant CN/DN/ON that you require in LDAP.

Tip: when setting up a FreeRADIUS server we'd recommend you run the server in full debug mode (freeradiusd -X or radiusd -X depending on whether it was installed by APT or from source) to enable you to see exactly what is going on for each packet and the decisions/checks the server is making as you develop the configuration.

A word on the format of user names: when migrating to an 802.1X authenticated network, it is often tempting to permit simple usernames to continue to be authenticated for users on the home campus rather than requiring a full username including a realm element to be used. Since an eduroam username must include a realm component, the Tech Spec now requires that the username should always include the realm component, even for eduroam networks for local users only and for users who might be thought to not roam to other eduroam sites.

It is particularly important to not permit simple userID-only usernames to be used in single-SSID eduroam networks where 'eduroam' is used for both guest users and local users.

By requiring that the full 'userID@organisation.ac.uk [55]' type credentials are used, you can ensure that the same credentials are used by users both on the home network and when roaming. Thus problems associated with use of incorrect creadentials can be avoided. For the user, there is no confusion and after the first time that the credentials are entered into the supplicant, there is no additional work involved resulting from the adoption of this policy.

Configure RADIUS server to reject PAP requests from the NRPS

Historical note (PAP tests are no longer generated from the NRPS): PAP is useful to have configured against a local test account during the early stages of service implementation. However, once you have used it to test port 1812 transit and NAT/PAT if applicable, since there will be no production PAP traffic, you should confgure your RADIUS server to reject any PAP requests coming from the NRPSs.

Configure load balancing if deploying multiple RADIUS servers servicing your WLAN

If you are deploying multiple RADIUS servers to service your WLAN, think about how you are going to share the load evenly between these and your failover mechanisms.

A note on working with usernames in Microsoft NPS Windows 2008R2

Many organisations implement eduroam in an existing MS Windows network environment where usernames are stored in AD in a simple userID form without a realm component (or in some cases the realm component doesn't match the eduroam realm, e.g. eduroam realm = @camford.ac.uk but AD realm = @ad.camford.ac.uk). For eduroam authentication, usernames must be in the form userID@realm [16], therefore a means must be found of presenting the username in a form that can be successfully authenticated. (In the mismatching realms case, the eduroam realm needs to be made authenticatable). In IAS and earlier NPS versions, a perfectly workable solution has hitherto been to simply strip the realm component by using for example the find-replace rule in the Connection Request policy which is the standard Find “(.*)@(.*)” Replace “$1”. This however is no longer possible in later versions of NPS.

In NPS Windows2008R2 and later, whilst you can implement the above, the results is authentication fails even though the actual realm stripping seems to work - the stripped username is found in the AD, but still the authentication fails, (almost as if the password is wrong). Interestingly you could even strip the original .ac.uk type realm component (e.g. @camford.ac.uk) and replace it with a local one (e.g. @ad.camford.ac.uk or @camford.local) that matches a valid username in AD, but the result would be the same.

This is because in Windows 2008R2 Microsoft decided to change the way that NPS deals with realms. In 2008R2 a stripped realm no longer passes EAP security requirements and thus the stripping of a User-Name always results in an authentication failure.

The fix for this is to do one of the following:

1) Configure the realm stripping rules on the front-end NPS server to modify the identity in the Access-Request and then forward the request to a second NPS server for authentication OR just send the Access-Request to a second (earlier release) Microsoft RADIUS server (older NPS or even ancient IAS box) to do the stripping and authentication.

2) The recommended solution is to add your eduroam realm as another global UPN to your AD so you don't need to strip the realm in the first place. (What is UPN? https://apttech.wordpress.com/2012/02/29/what-is-upn-and-why-to-use-it/ [56])

3) Use a different RADIUS server platform!

Set up logging

Logging on the ORPS must be set up in accordance with the Technical Specification. All transactions with the NRPS, including some mandatory attributes, must be logged and records held for at least 3 months, with a recommended maximum of 6 months (subject to your own policies).

RADIUS Accounting

RADIUS Accounting is not required by eduroam(UK) but some overseas countries do use Accounting information inside their own borders for various reasons. Since eduroam Europe Operations does not interfere with forwarded Accounting packets, ORPS at Home service organisations may receive accounting records from their own users when they roam to a non-UK hotspot for which RADIUS Accounting has been turned on. Note that the number and content of attributes in the Accounting packets varies greatly due to the underspecification in RFC2866; you can not rely on any single Accounting attribute being present. The best option is for your to simply discard Accounting packets which cannot be correctly understood by your RADIUS server.

Visited sites should turn off RADIUS Accounting.

Resources:

- Technical Specification [57]
- Complying with the Technical Specification
- Inter-NREN Roaming Infrastructure & Service Support Cookbook [35] (pdf) (produced and

published by GEANT2)

- eduroam.org guide: Setting up Various RADIUS servers for Home service [58]
- Connecting FreeRADIUS to AD and LDAP User Database [52] - Geant Best Practice guide (2013)
- Aruba Wireless Controller and ClearPass Configuration guide [54] - Geant Best Practice (2016)
- Clarification of Policy and Tech Spec Wording - Visitor Activity Logging

?14. DNS Name Server Configuration - NAPTR record

All(*) participants providing a Home (IdP) eduroam service **should** ensure that the DNS zone relating to their realm contains a NAPTR record (Name Authority Pointer) enabling the NRPS to be indirectly defined as hosts for radsec services via SRVs. (*****)With the exception of .ac.uk participants using Windows Server 2003 as their DNS server (since this does not support NAPTR records - Windows 2008 R2 is fine). This ensures improved authentication performance for your users when using eduroam outside of the UK.

It should be noted that it is **mandatory** for organisations using non-.uk realm names (e.g. camford.edu and camford.org to configure NAPTR records in their DNS zones and so such organisations must ensure that their DNS name server supports NAPTR records. This is because top-level international RADIUS routing for 'special' top level domain names is now achieved using RadSec DD.

The background, rationale and method of achieving insertion of NAPTR records are documented in Advisory: Improving Efficiency of International Authentication through utilisation of RadSec at National Level [59]

Source URL: https://community-stg.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-2

Links
[1] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-1
[2] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-3
[3] https://technet.microsoft.com/en-us/library/cc755205%28v=ws.10%29.aspx
[4] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-2
[5] https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-Clients
[6] https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-ConfiguringremoteRADIUSservers
[7] http://www.surfnetters.nl/paul/nps-eduroam-01.pdf
[8] https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-Clientdefinition
[9] https://community.jisc.ac.uk/library/janet-services-documentation/filtering-invalid-realms
[10] http://community.jisc.ac.uk/library/janet-services-documentation/microsoft-nps-2008r2-config-avoid-bad-usernames-flooding-nrps
[11] https://community.jisc.ac.uk/groups/eduroam/document/nws-40-freeradius-demystified
[12] mailto:userID@camford.ac.uk
[13] mailto:user@myorganisation.ac.uk
[14] mailto:user@camford.ac.uk
[15] https://support.roaming.ja.net/?q=node/30

[16] mailto:userID@realm
[17] http://www.cisco.com/c/en/us/support/docs/lan-switching/8021x/118634-technote-eap-00.html
[18] https://community.jisc.ac.uk/library/network-and-technology-service-docs/microsoft-nps-improving-reliability-authentication
[19] http://techgenix.com/testing-monitoring-tools-radius-servers/
[20] https://support.secureauth.com/hc/en-us/articles/360019651812-How-To-Test-RADIUS-Using-NTRadPing
[21] https://radiustest.software.informer.com/download/
[22] http://w1.fi/wpa_supplicant/
[23] https://www.systutorials.com/docs/linux/man/8-eapol_test/
[24] https://www.systutorials.com/docs/linux/man/5-wpa_supplicant.conf/
[25] mailto:testuser@test.yourrealm
[26] http://www.freeradius.org/rfc/attributes.html
[27] http://www.cisco.com/en/US/products/ps6350/
[28] https://community.jisc.ac.uk/library/janet-services-documentation/radius-attribute-filtering-microsoft-ias-and-nps
[29] https://community.jisc.ac.uk/groups/eduroam/article/improving-reliability-microsoft-nps-authentication-provider-eduroam
[30] https://community.jisc.ac.uk/library/janet-services-documentation/advisory-injection-operator-name-attribute
[31] mailto:username@FQDN
[32] https://www.wireless.bris.ac.uk/netcomms/eduroam-realm-checks.conf
[33] https://community.jisc.ac.uk/library/janet-services-documentation/microsoft-nps-2008r2-config-avoid-bad-usernames-flooding-nrps
[34] https://community.jisc.ac.uk/library/janet-services-documentation/case-study-complying-technical-specification
[35] http://www.eduroam.org/downloads/docs/GN2-08-230-DJ5.1.5.3-eduroamCookbook.pdf
[36] https://support.roaming.ja.net/?q=node/25
[37] https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-SetupofeduroamSPRADIUSservers
[38] https://community.jisc.ac.uk/library/janet-services-documentation/advisory-filtering-invalid-realms-auth-requests-sent-nrps
[39] http://technet2.microsoft.com/WindowsServer/en/library/1d497af2-be8a-4e9f-a586-e01bff1862d01033.mspx?mfr=true
[40] http://www.novell.com/documentation/edir_radius/index.html
[41] http://wiki.freeradius.org/FreeRADIUS_Active_Directory_Integration_HOWTO
[42] https://support.roaming.ja.net
[43] https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-eduroamSP
[44] https://services.geant.net/sites/cbp/Knowledge_Base/Wireless/Documents/gn3-na3-t4-wlan-infrastructure.pdf
[45] http://www.alliedtelesis.co.uk/media/fount/how_to_note_alliedware/c613-16051-00-A.pdf
[46] https://community.jisc.ac.uk/groups/wireless-admin/document/wireless-options-cisco-wlcs
[47] https://wiki.geant.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-Requestforwarding
[48] https://community.jisc.ac.uk/library/janet-services-documentation/janet-eduroamuk-technical-specification
[49] http://technet.microsoft.com/en-us/library/cc757645%28v=WS.10%29.aspx
[50] https://community.jisc.ac.uk/library/janet-services-documentation/blocking-lan-service-ports
[51]
https://community.jisc.ac.uk/system/files/257/eduroam%28UK%29%20Microsoft%20NPS%20Configuration%20Guid
[52] https://services.geant.net/sites/cbp/Knowledge_Base/Wireless/Documents/gn3-na3-t4-freeradius-db.pdf
[53] https://community.jisc.ac.uk/groups/eduroam/document/eduroamuk-microsoft-nps-configuration-guide
[54] https://services.geant.net/sites/cbp/Knowledge_Base/Wireless/Documents/cbp-79_guide_to_configuring_eduroam_using_the_aruba_wireless_controller_and_clearpass.pdf

[55] mailto:userID@organisation.ac.uk
[56] https://apttech.wordpress.com/2012/02/29/what-is-upn-and-why-to-use-it/
[57] https://community.jisc.ac.uk/library/janet-services-documentation/janet-eduroam-technical-specification
[58] https://confluence.terena.org/display/H2eduroam/How+to+deploy+eduroam+on-site+or+on+campus#Howtodeployeduroamon-siteoroncampus-SetupofseveralpopularRADIUSservers
[59] https://community.jisc.ac.uk/blogs/eduroam/article/advisory-improving-efficiency-international-authentication-through-utilisation