Implementing eduroam Roadmap - Part 2

Page updated 24/04/2025

On this page sections 8 - 10:

8. Firewall configuration to permit RADIUS servers to work with NRPS
9. RADIUS server configuration; ORPS shared secrets; registration via Support Server - for Visited service
10. RADIUS server proxying to support a Visited Service and attributes filtering

See Part 1 for sections 1 - 7: [1]

1. Concepts and terminology
2. Deciding your service type and planning your eduroam implementation
3. Choose RADIUS server platform and plan connectivity for ORPS
4. Joining eduroam(UK) and selecting your realm
5. The eduroam Support Server website; input organisation/site details, realm name, test account
6. Install your RADIUS Server (ORPS)
7. Acquire server certificate for ORPS/NAS

See Part 3 for sections 11 - 16: [2]

11. RADIUS Server configuration to support Home user authentication when roaming and on campus; and attributes filtering
12. Wi-Fi service and establishment of a VLAN/network service for eduroam
13. Firewall configuration to support eduroam network service
14. RADIUS server software configuration for Home service / interoperation with user database
15. DNS Name Server Configuration - NAPTR record
16. Test facilities on eduroam Support Server / Visitor Test / Testing a new ORPS

See Part 4 for sections 17 - 23: [3]

17. RADIUS server log keeping and interpretation of logs
18. Monitoring your own service
19. Setting up user devices - 'onboarding users'
20. Q.A. test of your eduroam implementation
21. Promote eduroam at your organisation - your eduroam web site
22. Keep your configuration details data on the eduroam Support server up to date
23. Planning Ahead and Developing your eduroam Implementation

Part 2

Section 7 continued:

Self-signed certs/private Certification Authority (CA) or commercial server certs?

Private CA signed certificates/self-signed certificates - It is generally accepted that use of private CA signed server certificates represents best practice, with self-signed server certificates offering a good alternative. This is not to say that commercial CA certificates are inferior or result in an insecure solution - they are perfectly fine when coupled with correct device setup i.e. with server certificate validation enabled and the same condition applies where private CAs/self-signed certs are employed!

Since a private CA should be extremely difficult for a malign agent to gain access to and to create rogue certificates or for self-signed certificates to be stolen and copied, the use of private certificates means that should a malign agent set up an impostor RADIUS server, since that server will not posess a trustworthy certificate (not issued by the 'expected' authority) it should be more easily identified as an imposter and the user's authentication should not proceed. So use of a private CA does partially mitigate the potential threat of a 'man in the middle' exploit - but see below (*)'Misconfigured clients'.

Man in the middle exploit - To trick users into interacting with an imposter RADIUS server the malign agent would need to set up a rogue access point broadcasting the eduroam SSID, with an imposter RADIUS server masquerading as your ORPS - which could be made believable by using a server certificate acquired from the same CA as your legitimate ORPS. This would allow the impostor RADIUS server to support TLS based interaction in situations where the client 'just trusted' the RADIUS server - i.e. where it does not do server certificate validation, including checking the name on the certificate. The client device, trusting the spoofed ORPS then will then go on to send username and password thereby allowing harvesting of credentials and after the rogue AP has provided the device with a network connection, man-in-the-middle interception of network traffic. The use of private CA certificates reduces the risk, but does not eliminate it.

(*) Misconfigured clients still represent a risk - Unfortunately there is, we believe, still widespread practice of connecting to eduroam using inadequately set up client devices, including those doing 'trust on first use', (so certificate validation including certificate name validation is not performed). It is essential that device setup is included for corporately managed devices or that some form of device setup provising is employed for corporate devices and is made available for users' own devices - such as the eduroam CAT system in conjunction with the geteduroam App.

Use of self-signed server certificate - This is a certificate which is signed with its own private key. Whilst it cannot be stolen or copied, since there is no root certificate used for the signature this means that you cannot pre-install trust for it on devices - you will need to rely on users to 'click accept' when the certificate alert pops up. This represents poor practice as it conditions users to ignore such alerts - reducing device security. Additionally, having a self-signed cert means that when it expires it you will need to replace it and reconfigure all client devices - but by having a long expiry date you can balance this effort against the effort of replacing a commercial server certificate (such as can be supplied through Jisc's Certificate Service

[4]) on your ORPS.

If you have the necessary expertise to set up a private Certification Authority and issue server certificates you will be able to negate the risk of your ORPS being masqueraded by a credentials harvesting rogue. Use of private CA signed certificates will of course require the CA certificate to be distributed to user's devices and trust of the CA to be pre-configured. But by using CAT, the effort of CA cert distribution and client device reconfiguration can be minimised.

A further benefit of using a private CA is that you will be able to construct a certificate chain without intermediate CA certificates. This results in fewer bytes to be transmitted inside the EAP conversation and hence fewer EAP round-trips and thus faster authentication.

Note: If you are using Microsoft Windows Server Certfication Authority - the implementation of the X509v3 Extension: Basic Constraints in Windows Certification Authority appears to contain a bug which results in certificate validation (and hence authentication) failure with **Android 12** when the technically accurate recommendations set out in https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+consider... [5] are strictly followed.

*From December 2021 onwards, when creating your server certificate CSR and following section 8 of the guide eduroam(UK) NPS guide, p31, on the Extensions tab, under Basic Constraints you should **NOT** tick the 'Make the basic constraints extension critical' box and **NOT** tick the 'Enable this extension' box.*

Commercial CA server certificates - services from a public CA have their plus points! It is recognised that many organisations lack the time or resources to produce self-signed certificates and to manage the distribution of these to client devices, and whilst this is our best practice recommendation, use of commercial server certificates (e.g. through Jisc's Certificate Service) makes for a perfectly acceptable solution!

If you decide not to use your own CA for signing certificates, most RADIUS servers will work without difficulty using certificates issued by both public certification authorities and intermediate certification authorities such as those issued through the Jisc Certificate Service [4] (which supplies certificates from a tba Certification Authority at very favorable pricing). (Historical note: with the old MS Internet Authentication Server, particular was needed in configuring the server because by default it assumed that the certificate was issued directly from a root certification authority known by the supplicant. No problems with NPS though).

Server certificate hints

Take care when preparing the CSR for your ORPS(s)!

Certificate type - you need an X.509v3 certificate, ideally Organisation-Validated (OV) or Domain-Validated (DV). Choose multi-domain SSL to keep your options open. SHA-256 is the recommended secure hash algorithm for the signing of the server certificate. The public key should be at least 2048 bits and ideally 3072. Only extended key usage (TLS Web Server Authentication) certificates should be used - not to be confused with Extended Validation (EV) certificates. There is no benefit in the use of an EV certificate and in fact there have been reports of difficulties with ChromeOS. (OV Certs can be acquired more speedily too!)

Whilst the Common Name (CN) does not have to match the host name of the ORPS in DNS (the CN is just 'a name' and the RADIUS server is not a web server) it is best practice to use a fully qualified domain name as the CN for reasons of maximum compatibility with devices.

There should be no spaces in the CN.

The SubjectAlternativeName:DNS parameter in the Certificate field should not be empty - the CN and SubjectAlternativeName:DNS must have the same value and must match exactly including upper/lower case. The CN should not be a wildcard name (e.g. *.camford.ac.uk).

If you deploy multiple ORPS servers, since there is no technical requirement for each server to have a different certificate, it is recommended you use one certificate, imported into all your ORPSs, thereby avoiding issues of support and client configuration/certification. The certificate will have just the one CN component in the Subject field - and that is usually a server name, e.g. eduroam.ORPS1.camford.ac.uk. Note that by using just one CN this will allow you to increase the number of ORPSs in your cluster in the future if required by importing a further copy of the certificate. Note that you can use multiple certificates if you wish, but each certificate will need a unique CN/subjectAltName pair.

The certificate should include a CRL Distribution Point extension and the URL needs to be valid and publicly accessible. In addition, some devices require that the BasicConstraint extension has CA:FALSE set, marking the certificate as being not a CA (the extension should also be marked as critical).

Resources:

- Certificates in eduroam [6]
- **EAP Server Certificate Considerations** **[5]** - highly recommended (almost mandatory) reading from the eduroam Europe documentation wiki
- Understanding Server Certificate Validation [7] - video stream of Kevin Koster's presentation to NWS
- Factsheet: Introduction to Server Certificates [8]
- Jisc Certificate Service [9] - lowest cost QuoVadis CA server certificates
- Using certificates issued through the Jisc Certificate Service with Microsoft IAS [10]
- Microsoft technical article: Certificate Requirements when using EAP-TLS or PEAP with EAP-TLS [11]
- TechRepublic paper - Self-sign a RADIUS server for secure PEAP or EAP-TTLS authentication [12]
- Generating self-signed certificates for use with Windows IAS using OpenSSL: Generating Windows IAS PEAP & LDAPS certificates using OpenSSL. [13]
- Generating self-signed certificates using OSC(Radiator)'s CATool™ for linux/unix: OSC CATool home page. [14]
- Advisory: Supporting Windows Mobile 8 Certificate Validation [15]
- Advisory: MD5 certificate types deprecated in favour of SHA-1 for RADIUS server [16]

FAQs:

Can I use the Janet Certificate Service to provide certificates for my RADIUS servers?

Yes - the Jisc Certificate Service [17] works fine with the most popular RADIUS servers; FreeRADIUS, Radiator, Microsoft NPS and Cisco ISE and will provide you with a small number of server certificates free of charge - suitable for use with EAP-PEAP and EAP-TTLS methods.

Historical notes:

From April 2015 - c.2020, the service provided Sectigo (Comodo) certificates. Prior to that Comodo certificates using the TERENA SSL intermediate CA and thence chained to Comodo.)

The use of intermediate CA certificates is considered to be more secure than root CA type. The result of this however was that if you intended to use Microsoft Internet Authentication Service (IAS/NPS) with Janet Certificate Service, a degree of skilful configuration was required. A technical guidance sheet which details this is available: Using Certificates Issued by the Jisc Server Certificate Service with Microsoft Internet Authentication Service.

The difficulties with MS Internet Authentication Service stemmed from the fact that it did not send the full certificate chain during EAP-PEAP negotiation. Consequently, in order to use MS IAS with Janet CS certificates (or any other certificate not issued directly from a certification authority (CA) known by the supplicant), it is essential to:

1. Ensure that you include the correct extensions in the certificate

2. Configure IAS to include the certificate in its list of known certificates.

This issue originally came to light through problems experienced in attempting to use certificates issued by the Janet Certificate Service with the Windows XP supplicant. All certificates issued by the JCS are signed as from an intermediate CA; but any 802.1X supplicant, including the one native to XP, will **not** be able to validate certificate chains derived from intermediate CAs from Microsoft IAS because IAS does not send the full chain in the ServerHello during the TLS handshake in Phase 1 of EAP-PEAP.

So if you intend to use Microsoft IAS, your options are:

1. Use a commercially-supplied certificate that will 'chain directly' to a root CA 'known' by your supplicants.

2. Use a certificate that uses an intermediate CA, but be very careful and thorough in your configuration of IAS. Refer to the technical guide - Using certificates issued by the Jisc Certificate Service with MS IAS [18]. [10]

3. Manage your own private CA.

Nb. Microsoft NPS users must use SHA256 certificates, which the JCS QuoVadis certificates are! "In late 2013, Microsoft announced that SHA1 certificates will not be accepted in Windows after January 2017. At that time, QuoVadis changed its default issuance of SSL to SHA256." https://support.quovadisglobal.com/kb/a429/changes-to-security-indicators-in-the-chromium-browser-affecting-sha1-ssl-certificates.aspx?KBSearchID=34148 [19]

How do I get and install a commercial server certificate for use with MS IAS?

- MS IAS - obtaining and installing a VeriSign WLAN Server Certificate for EAP-PEAP (MSCHAPv2) [20]

Can I use a self-signed certificate for my RADIUS server?

Yes. EAP methods that use TLS, such as EAP-PEAP and EAP-TTLS, require the use of a server certificate to authenticate the RADIUS server to the supplicans.

This certificate may be derived from a local self-signed certificate authority (CA), or purchased from a commercial CA. The advantages and drawbacks of both of these are listed below.

Benefits of a certificate from a self-signed CA:

- No need to purchase a certificate from a commercial vendor.
- Provides a slight security benefit by making it harder for a user to misconfigure their supplicant in an insecure way. (The use of a certificate from a commercial CA combined with a failure by the supplicant to validate the CN of the certificate makes a MITM attack feasible, where the attacker simply acquires a certificate from the same CA).

Benefits of a certificate from a commercial CA:

- No need to distribute the CA's root certificate to each client.

Note: some RADIUS implementations, such as Radiator and FreeRADIUS, provide a certificate from a self-signed CA for testing purposes. Under no circumstanances should this certificate be used in a production environment.

Resources:

- See links in Resources section above

8. Firewall configuration to permit RADIUS servers to work with NRPS

The next step is to ensure that your RADIUS service will be able to communicate with the national RADIUS Proxy servers through your firewall.

RADIUS communication is based on the User Datagram Protocol (UDP). In early RADIUS deployments port 1645 was utilised, but RFC 2865 officially assigned port number 1812 and this is the port that RADIUS servers listen on in eduroam. Therefore your firewall must be configured to allow UDP communication with all of the eduroam (UK) National Roaming Proxy Servers.

The NRPS also perform ICMP probes to your ORPS, as does the eduroam(UK) Support server. This is to check for and monitor basic network connectivity. By exception, Cisco ACS systems with CSA hardening reject ICMP and so TCP probes on port 2002 can be used instead.

a) Firewall configuration to allow UDP for ORPS-NRPS RADIUS/ICMP for Support server :

Firewall configuration - the firewall protecting your ORPSs must be configured to permit RADIUS communication between the three eduroam(UK) NRPSs and your ORPS(s) using the following protocols on the port numbers indicated:

- UDP/1812 inbound and outbound (used for authentication)
- ICMP
- ICMP must also be permitted for eduroam New Support server 195.195.131.204 2001:630:1:7:5bd:5f3e:bb1c:6f27

IP Addresses of the NRPS:

- Roaming0 193.63.195.58 2001:630:1:133::58
- Roaming1 193.63.195.34 2001:630:1:132::34
- Roaming2 193.63.195.50 2001:630:1:133::50

The address of the eduroam(UK) Support server:

- New Support server 195.195.131.204 2001:630:1:7:5bd:5f3e:bb1c:6f27

Network Address Translation - if your ORPS is connected via an internal network with private addressing and so has a private IP address, the NATing must be fixed and your firewall rules will need to be carefully configured to permit inbound and outbound access via the NAT. Note that as far as the eduroam(UK) NRPSs are concerned, the public IP address that is resolved from your ORPS FQDN is the IP address of the ORPS. We don't know anything about what goes on beyond that public IP.

Host/Server firewall - it should be remembered that servers themselves may have firewalls/ACLs. For servers that sit behind corporate firewalls this seems overly complicated, but if you haven't built the ORPS server yourself or you are inheriting a system it is worth checking for a local firewall - particularly if troubleshooting a problem.

Historical notes: old implementations of RADIUS used UDP/1645 inbound and you would only permit inbound on this port if your ORPS required this (1645 was deprecated may years ago since this conflicts with the 'datametrics' service). Nb. Old eduroam Support server was at 193.60.199.62 2001:630:1:5::62 (no longer required).

FreeRADIUS note - 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 various random ports now. There might be some circumstances in which you may need to open additional UDP ports on your firewall, **however the eduroam(UK) NRPS will only accept authentication requests sent on port 1812** - as stated in the Technical Specification: auth requests sent to the NPRS MUST be via port 1812.

b) Firewall configuration to not reject fragmented UDP packets:

To eliminate a potential cause of problems, your firewall should be configured to allow UDP packets from the NRPSs without any restriction on packet size or fragmentation state. This is because certain EAP methods (EAP-TLS) and RADIUS server configurations result in the generation of very large RADIUS messages and UDP packets (due to the length of user/server certificates) and it is common for such packets to be fragmented by routers during transit. It is vital to the RADIUS exchange that these fragments are not discarded - a RADIUS exchange may comprise a dozen or more messages each of which may consist of multipe UDP packets and since UDP is connectionless, the loss of a single packet will result in the whole authentication attempt having to be re-started from the beginning.

Firewall discard/reject fragmented UDP packets rule:

- No not apply reject (allow UDP fragment packets)

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

It is technically possible with some RADIUS implementations, in the RADIUS IdP config., to adjust the default maximum UDP packet size to be used for the RADIUS exchange, thereby reducing the possibility of fragmentation by routers in the transmission path. However, due to capability limitations of some RADIUS servers and overseas IdPs being outside UK authority, it would not be sensible for us to 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.

c) RADIUS server configuration to managing UDP packet size - this may need to be done after configuration of RADIUS servers/policies:

Whilst this guide recommends configuring firewalls to not reject UDP packet fragments, it cannot be guaranteed that all UK member organisations will configure their firewalls in this way, so your users roaming to a site where the firewall rejects fragmented UDP may experience authentication problems. The chances of experiencing difficulties increases the further your users roam, particularly outside of the UK where eduroam(UK) has no influence over deployments. In addition, the more data links and routers that the user's authentication packets have to traverse before reaching your RADIUS server, the greater the possibility is that fragmentation will be applied and fragmentation-unfriendly routers will be encountered. So the aim should be to reduce the chances packets being fragmented en-route to/from your RADIUS server - and this can be achieved by reducing the negotiated size of the UDP packets.

The default maximum transmission unit (MTU) size that a number of RADIUS servers and clients use for EAP payloads is 1500 bytes, but this size of payload results in the maximum size Ethernet frame and consequently a high risk of being fragmented by routers as it traverses multiple links in the path. There are exceptions to this - Cisco ISE has a fixed 1,002 byte maximum. It is therefore recommended that you check the value your RADIUS server is using and adjust it to a reasonable value if possible. With some RADIUS servers this is pre-set at a modest size and is not adjustable. But on others, the MTU can be changed.

How to adjust the MTU - for RADIUS there is the Framed-MTU attribute which is defined in RFC 2865, but "This Attribute indicates the Maximum Transmission Unit to be configured for

the user, when it is not negotiated by some other means (such as PPP). It MAY be used in Access-Accept packets. It MAY be used in an Access-Request packet as a hint by the NAS to the server that it would prefer that value, but the server is not required to honor the hint." Neither the Cisco ISE nor the Microsoft NPS RADIUS servers take any notice of any Framed-MTU attribute recieved from a client device in an Access-Request!

Microsoft NPS - the default maximum transmission unit (MTU) used for EAP payloads is 1500 bytes. Whilst NPS ignores Framed-MTU in an Access-Request from a client, you can add a Framed-MTU attribute and set its value ***via the Network Policy that is handling the authentication of your users*** - and that Framed-MTU will be used by NPS to manage the size of the packets sent back to your remote user. The Microsoft documentation suggests setting a value of 1344 or lower. Suggested value - 1100.

- Go to Network Policies and in the Details pane double-click the policy that you want to configure (e.g. local authentication)
- 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. (Suggested value: 1100) Click OK,
- Click Close, and then click OK.

See: https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-np-configure#configure-the-eap-payload-size [21]

(Old TechNet reference: https://technet.microsoft.com/en-us/library/cc755205%28v=ws.10%29.aspx [22])

Aruba ClearPass - the default value of default maximum transmission unit (MTU) is 1100. This should be fine in most cases. You can modify the relevant 802.1X Authentication Profile using the WebUI. Select your users profile and change the settings for the parameter Framed MTU. This sets the framed MTU attribute sent to the authentication server. Click Pending Changes. and in the Pending Changes window, select the check box and click [Deploy changes].

Cisco ISE - you do not need to worry about trying to adjust the EAP payload size, indeed, it is not possible to change the maximum packet size. ISE always tries to send e.g. EAP-TLS fragments (usually Server Hello with Certificate) that are 1002 bytes long (although the last fragment is usually smaller). Even if a client should send a Framed-MTU attribute in an Access-Request it will not be honoured. It is not possible to reconfigure ISE to send larger EAP fragments.

d) 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 visitor simulation authentication test on the Support server, with eapol_test, optionally together with packet capture on your RADIUS server (eg tcpdump for linux/BSD/unix or Wireshark on Windows). eapol_test is now available (courtesy of eduroam(UK)) as a Windows executable. When you run the visitor authentication tests you

will also be able to see the requests logged on your RADIUS server and also there will be entries in the Support server RADIUS logs view. For info on how to run the test, jump to part 2 section 15 [23] of this guide.

Nb. Once you have configured RADIUS forwarding and EAP authentication methods as described in the next section and section 13 respectively, you will be able to make use of the further authentication/certificate tests on Support server - which, if they are successful prove that you have UDP/1812 enabled.

9. RADIUS server configuration; ORPS shared secrets; registration via Support Server - for Visited service

In this step you will add your ORPS to the NRPS RADIUS configuration as a Client and add the NRPS to your ORPS RADIUS config as remote RADIUS servers/Authenticators - this readies your ORPS to support a Visited service which requires sending authentication requests to the NRPS

Adding your ORPS into the eduroam infrastructure to support Visited service interaction: (Not applicable to Home-only deployments - which make no provision for visitors). You now need to peer your ORPS(s) with the NRPSs so that RADIUS messages can be exchanged for eduroam visitors to your campus. (Wi-Fi/network configuration is covered in section 12 below). Configuration of your ORPS for the support of a Home service for your roaming users is detailed in section 11, but you may combine the RADIUS peering operations at this stage if you wish.

With respect to setting up a Visited service, since a there are two ends of a RADIUS conversation there are two operations:

1. Addition of your ORPS to the RADIUS clients configuration of the NRPSs - so the NRPS accept RADIUS packets from your ORPS
2. Addition of the NRPS to the RADIUS proxy/authentication servers (remote/external RADIUS servers) configuration of your ORPSs - so your ORPS can send RADIUS packets to the NRPS

The first operation is completed by you registering your ORPS via the eduroam(UK) Support Server portal. Your ORPS details will be added to the NRPS configuration file and that will be uploaded to the NRPSs at the next hourly configuration refresh. RADIUS server peering requires mutual trust and this is achieved through the use of shared secrets. In eduroam(UK) each NRPS-ORPS pair shares an alphanumeric key. The shared secrets for the NRPS are generated when you click on the [Add server] button to begin the registration process. You will need to copy each share secret and paste this into your RADIUS server configuration.

As stated in section 6, your ORPS needs to have a public facing IP address and a fully qualified domain name i.e. an address record in DNS. Your ORPS will be configured in the NRPS clients and AuthBy tables with their IP addresses, but you need to provide us with the FQDNs. This reduces scope for error, facilitates IPv4 and v6 support and enables you to change the IP address in the future with a single click and [Save] on Support Server. (To change IP address, update your A record in DNS and then trigger a lookup for the new IP address by clicking in the address field - remember to click [Save] at the bottom of the panel).

9.1 Adding your first ORPS via Support Server Portal and Acquire your Shared Secrets

Log in to Support Server: via https://support.eduroam.uk/login [24]

Click on the 'Configure' tab.

In the green 'RADIUS servers' panel click on the [Add server] button. A popup box will appear which will enable you to add the necessary details of your ORPS and you will see the unique shared secrets that are generated when the form is opened. You will need to copy each shared secret and paste this into your RADIUS server configuration for each of the NRPSs.

Entered your required settings - see able below. When complete and you have clicked on the 'Save' button at the bottom of the form, the details will be added to the ORPS config file on Support and at the next hourly NRPS config update, will be propagated to all three NRPS. Therefore new additions and subsequent ORPS status changes can take up to one hour to take effect! The updated configuration is loaded into the NRPS in the order: Roaming0, Roaming2 then Roaming1, with there being a few minutes between RADIUS reloads to ensure continuity of service.

Enter ORPS configuration details required:

IP connectivity		
Fully qualified domain name:	The fully qualified domain name of the RADIUS proxy server. You cannot use the IP address	This field is mandatory. Be sure to update your DNS zonefile to include the server and think about the TTL which will be important if you ever change the IP address
The IPv4 and IPv6:	These are automatically populated	Support server performs DNS lookup when you click on the address field. (Facilitates IP address change of your ORPS if you ever need to - simply update the DNS A record and refresh the Support server IP lookup and Save).

Authentication port:	Default value is 1812	This field is mandatory. The NRPSs listening on this port for authentication requests from your ORPS. For legacy reasons you have the option to change the RADIUS communication port, but strongly advise use of the default 1812. The only alternative port allowed is 1645
RADIUS settings		
Copy shared secrets:	Relevant when you register multiple ORPS: Default is 'none' i.e. new unique secrets. You can choose an existing ORPS to copy the secrets from	When you have an existing ORPS you have the option to copy shared secrets from that ORPS. This is useful with clustered servers if all members of a cluster need to have the same shared secrets. To prevent accidents, you cannot change the shared secrets for an existing server, but you can certainly delete and recreate it with new or copied secrets
Shared secrets:	Cut and paste into your config for the NRPSs	You need these to configure your ORPS to authenticate against the NRPS
Authenticate requests (role of your ORPS):	Default is Client only (sends auth requests to NRPS). Tick if this ORPS is an authenticator too (processes auth requests)	For Visited service this box can be left unticked. The server will be set as a Client only and will only be able to forward authentications for your visiting users to the NRPS. If this ORPS will be supporting a Home service and will authenticate requests from your roaming users you must tick this box.

Test and development:	Tick to set ORPS as test/dev	Select this if you have a live service and the server you are adding is for testing only and should not handle production traffic. The NRPS will then only forward test realm traffic to it. The test realm is in the format of test.yourrealm.tld and does not need to exist in DNS
Disabled:	Tick to set ORPS as inactive	If you mark a server as disabled it will be removed from the NRPS configuration, however all settings and the shared secrets will be kept on the support server so they can be reinstated later
Server information		
Server (host)name:	Short name	A short name for this server which should be unique within your own set of ORPSes
Server operating system:	Choose from drop down list	This data allows us to tailor the options you see in this portal and assists us in supporting your system both in response to support requests and pro-actively
Operating system version:	Enter OS s/w version	As above
RADIUS software name:	Choose from drop down list	As above
Software version:	Enter RADIUS s/w version	As above

When complete, click on [Save].

You will see the new ORPS listed in the 'In production' box in the RADIUS servers panel - unless you ticked 'Test and development'. By clicking on this or any other ORPS you create, the the details will be displayed in a popup box. You can view the shared secrets and edit the ORPS settings and details. You must hit the [Save] button if you wish to save any changes.

Note that you may see a 'Status server' tick box when the edit ORPS popup is displayed. You should only see this option if your platform supports it. If you have configured status server on your ORPS you should tick this box. Support Server will then check that the it gets a status

server response from your ORPS. Since enabling status server without it actually being operational on your ORPS would prevent service, you cannot enable this setting without a successful test outcome (if the test fails the box is de-selected).

Your ORPS will be added to the NRPS client configuration on the next scheduled update. This occurs approx 6 minutes past the hour every hour.

Notes:

- **Status-Server:** If your ORPS supports it and you wish the NRPS to use Status-Server to check the operational status of your ORPS, tick the box. Status-Server packets very helpfully allow a RADIUS server to determine whether or not another server is alive should no response be received to Access-Request packets. Some RADIUS platforms (FreeRADIUS, Radiator, radsecproxy) support this - if yours does then opting to use this will be beneficial. For further information see: Status-Server Advisory [25]. **Nb. This function was suspended (Sept 2016) on Support Server v 1 and is planned to be reintroduced in Support Server v2.**
- **Test/Development:** Relevant to organisations which already have an operational service and wish to peer a new additional OPRS with the national proxies. Servers marked as test/dev will not receive production **or** eduroam test/monitor traffic; only 'anyuser'@test.'your_realm' traffic will be sent to the test/dev ORPS. This enables you to carry out your own testing - which you must initiate through your production ORPS.
- **Note that there is no Accounting port field:** (The port that the RADIUS server is listening on for Accounting requests). The NRPS no longer accepts Accounting packets and the value of the port for Accounting messages is in any case fixed. Your ORPS must not

9.2 Add the NRPS as remote RADIUS proxy servers/authenticators on your ORPS - for Visited service

ORPS side peering - To complete the process of peering your ORPS with the NRPS (for a Visited service) you must add all three NRPS as RADIUS servers on all of your ORPS systems. (The process of peering for a Home service is covered in section 11).

Configuration details are different for each RADIUS software platorm, generally entail i) defining each remote RADIUS server ii) defining a remote RADIUS group iii) adding the servers to the group iv) setting the weighting/fail over order. You should use the IP addresses as follows, but you may use hostnames: roaming0.ja.net (194.82.174.185) ; roaming1.ja.net (193.63.195.34) ; roaming2.ja.net (193.63.195.50).

Your remote RADIUS servers configuration for the NRPSs must be set to use UDP ports 1812 (authentication). The NRPS will not **listen** on anything other than the proper RADIUS port 1812. 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.

RADIUS Accounting is no long supported on the NRPS; your ORPS must not send Accounting packets to the NRPS. The NRPS do not support CoA (Change of Authorization) - if relevant this would be applicable only internally to your network.

The shared secrets for your configuration for the NRPS are generated by the Support server

when you register your ORPS by clicking on [Add server] as described above in 9.1. Accuracy is essential when transcribing the shared secrets to the configuration files/config fields. The secrets entered separately in your ORPS configuration for both remote RADIUS servers/authenticators and for RADIUS clients. The secrets in each config setting are used independently to validate messages for both visitor authentication (forwarding to NRPS) and roaming user authentication (in-bound from NRPS) connections. An error in any one of the shared secret entries 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.

'Proxying' - We will complete the configuration or your ORPS to actually forward authentication requests from your visitors to the NRPS in section 10 below

Hints

Microsoft NPS:

i) Under (NPS) - Templates Management > Shared Secrets > New RADIUS Shared Secret Template - template name=roaming0 (1) (2), select Manual, enter secret from Support server.

ii) Under (NPS) - RADIUS Clients and Servers (folder) > Remote RADIUS Server Groups > 'New' to create a new group, name it e.g. 'NRPS', and [Add] the NRPS IP addresses for all three NRPS; click on Authentication/Accounting tab, select Shared Secrets template, tick 'Request must contain message authenticator attribute', untick 'Forward network access server notifications to this server' [OK]; click on Load Balancing tab and set Load Balancing 33; set timeouts and backoff as per 10.2 (e) below. See section 14 p45 of [26]NPS guide [27]).

Aruba ClearPass: RADIUS Proxy Service configuration comprises five elements: definition of Proxy Targets; a Service Rule including definition of conditions; inclusion of Proxy Targets; selection of proxying scheme; excluding Accounting requests.

Rather than use Authentication Sources - which you would do via Configuration > Authentication > Sources, instead:

i) Define each NRPS as a RADIUS Proxy Target - Navigate to Configuration > Network > Proxy Targets, then click on ‘Add’. The 'Add Proxy Target pop-out box will open. Enter the requisite informatation (select 'RADIUS' as the protocol option) and click [Save]. Do this for all three NPRS (roaming0.ja.net, roaming1.ja.net and roaming2.ja.net).

ii) Create a RADIUS Proxy Service - Navigate to Configuration > Services, then click on 'Add'. On the 'Service' tab: Type - select 'RADIUS Proxy'. Name - enter a logical name (e.g. 'eduroam-outbound'/'proxy eduroam visitors to eduroam').

The conditions that must be met for the Service to be applied can be defined in the Service Rule section - this will be configured in section 10 below.

iii) Specify which remote RADIUS servers to forward authentication requests to. Click on the Proxy Targets tab. Proxy Targets - using the 'Select to Add' dropdown, add all three NRPSs as defined in the Proxy Targets definition step above.

iv) Proxying Scheme - select the 'Load Balance' option rather than 'Failover'.

v) Accounting Requests: Untick the ‘Enable proxy for accounting requests’ box

Nb. You can define the RADIUS attributes to be filtered out from Access-Challenge/Accept replies from the NRPS if you wish.

Click [Next]

Click the Enforcement tab

You can apply Enforcement parameters as required.

Click on the [Save] button

FreeRADIUS: edit proxy.conf. Nb. If you use hostnames rather than IP addresses in your proxy configuration 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).

```
home_server roaming0 {
        ipaddr = <193.63.195.58>
        secret = <secret>
        status_check = status-server
        response_window = 30                (default 5)
        check_interval = 10
        check_timeout = 5
}

home_server roaming1 {
        ipaddr = <193.63.195.34>
        secret = <secret>
        status_check = status-server
        response_window = 30                (default 5)
        check_interval = 10
        check_timeout = 5
}

home_server roaming2 {
        ipaddr = <193.63.195.50>
        secret = <secret>
        status_check = status-server
        response_window = 30                (default 5)
        check_interval = 10
        check_timeout = 5
}
```

Cisco ISE:

i) Administration > Network Resources > External RADIUS Servers > +Add. Include all three NRPS devices.

ii) Administation > Network Resources > RADIUS Server Sequences and create a 'RADIUS Server Sequence'. On the General tab, provide a name for the NRPSs sequence (e.g. 'Proxy to eduroam NRPS') and enter descriptive text.

Via User Selected Service Type, from the 'Available' box select the three NRPSs, roaming1, roaming2, roaming0. Note that there does not appear to be a load balancing option other than the sequential fail-over mode. Note that the 'Remote accounting' tick box must NOT be unticked.

Click on the 'Advanced Attribute Settings' tab. Under 'Advanced Settings', the Strip options must NOT be ticked.

Under 'Continue to Authorization Policy' TICK 'On Access-Accept, continue to Authorization Policy'. Click [Save].

Setting up your ORPS to actually forward/proxy RADIUS authentication requests is covered in section 10.

9.3 Adding a Second/any Further ORPS

- Register additional ORPS
- Firewall/router configuration
- Shared secrets for additional ORPS
- Applying the same secrets as existing ORPS (clusters/Cisco ISE)
- Test/dev feature

Register additional ORPS: additional ORPS can be added to the clients config of the NRPS by following the same steps as described above. It is now quite common practice for organisations to deploy multiple ORPSs, which they may do for resilience or load sharing or during migration to a new data centre or to a cloud platform. You can add as many ORPS as you wish.

Once an ORPS has been added the NRPSs will automatically communicate with it. NRPS send all traffic to the first ORPS in their config list until it stops responding, the NRPS then try the next ORPS in the list. The order of preference is the order which the ORPS were added to the Support server. (*Feature not supported on Support Server 2 - If you want any particular ORPS to be your primary server, set the 'High priority' option on its config on the Support server, as indicated in section 9.1. We may be able to re-introduce this in the future.)*

Firewall/router configuration: when adding additional ORPSs, the same considerations apply regarding permitting inbound/outbound UDP and ICMP as for your initial ORPS - as described in section 8 above. If your ORPSs sit on an internal private address subnet and you have implemented network address translation, be careful to check that your outbound NAT mapping is correct. Whilst Support server tests roaming user authentications for each ORPS and flags alerts if there is an issue, checking auths for Visitors from each ORPS is a manual process - and something easily overlooked when you have other functioning ORPS.

Hard-to-detect outbound NATing error - we have seen instances of outbound NATing issues whereby the ORPS source address of access-requests is the firewall's public gateway address. Since this is an address not-registered as a trusted ORPS, the requests are dropped at the NRPS and if the address cannot be resolved to your public subnet, Support server will not log the 'unknown host sending requests' in the 'Radius errors' for for you organisation.

Shared secrets for your additional ORPS: Normally every ORPS has a unique set of shared secrets for peering with the three NRPS. This is best practice and the most secure way of employing shared secrets. This remains true even in scenarios in which peered realms contain multiple RADIUS servers. When an organisation registers a second ORPS, by default a further unique set of shared secrets is generated, different from those for the first ORPS. eduroam administrators must be aware that in deployments where the ORPS form fail-over clusters you cannot simply use the original three shared secrets on both ORPSs by default.

Cloning secrets from an existing ORPS for your additional ORPS: We recognise that there are particular solutions which use and require a common shared database for all clients and so require the same shared secret for each NRPS to be used by all ORPSs. Where two ORPS are deployed in fail-over systems that use the same set of secrets for each ORPS-NRPS proxy/client config. (ie ‘secret0’ for roaming0 for both ORPSs, ‘secret1’ for roaming1 for both ORPSs, ‘secret2’ for roaming2 for both ORPSs).

When registering your second or subsequent ORPS, as described in the table in section 9.1 above, in the RADIUS settings box, from the drop down option list for 'Copy shared secrets' (default 'none'), select the existing OPRS whose shared secrets you wish to copy for your new ORPS.

If you have previously registered ORPS with different sets of shared secrets, it is not possible to retrospectively change the secrets yourself via the Support portal. However, we can on request adjust the secrets manually in the database on Support server, (ie we will duplicate the settings for one of your ORPS). If this is required, please submit a service request advising us of the ORPS that has the seed shared secrets and to which ORPS you want the seeds copied.

Test/dev feature: The Support server includes a feature to enable you to connect additional ORPS prior to bringing them into production service. This is achieved through the 'test/dev' setting described above, but full details of this feature can be found in the technical documents section - https://community.jisc.ac.uk/library/janet-services-documentation/orps-role-designation-features-eduroamuk-support-server [28]

10. RADIUS Server Proxying and Attributes Filtering to Support a Visited Service

The next step is to configure handling of authentication requests arising from visitors and forwarding these to the NRPS. This should be implemented in a good neighbourly way to avoid adversely impacting the load on the NPRS and also to ensure that your own service is not adversly affected by poorly configured Home organisations.

Visited service - Configuring your ORPS to handle local campus authentication requests from your visitors:

You will need to configure realm handling and forwarding of authentication requests from your wireless LAN from the eduroam SSID to the NRPSs. (Nb. this is not applicable to Home-only deployments - which have no local Wi-Fi component).

- Configure Realm Handling, Proxying and Load Balancing
- Configure Attribute Filtering
- Configure Rejection of Malformed Usernames
- Configure Injection of Operator-Name Attribute (FreeRADIUS, Radiator, Aruba ClearPass, latest Cisco ACS/ISE only)

10.1 Visited service - Configuring your ORPS to forward authentication requests from your visitors on campus to the NRPS

This step is to configure your ORPS to handle auth requests from network APs/controllers, from the eduroam SSID, for Visitors. Such auth requests must be forwarded to the NRPS: You need 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 configured via GUI; Aruba Clearpass requires a 'service' to be defined and configured using the GUI. The actual authentication of your own users should be considered as a logical process separate from Access-Request packet handling/'proxying'. User authentication is covered later in section 14.

Since there are so many RADIUS servers to choose from, it is beyond the scope of this guide to provide detailed instructions for all the possible solutions. Nevertheless we have produced a configuration guide for Microsoft NPS and there are links to other guidance in the resouces section. You will also find links to these in the green Library panel on the Troubleshoot page of the Support server portal.

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 - see 10.4 below. 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 [29]. 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 [30] document and in the eduroam(UK) NPS Implemention Guide to be published shortly.

Hints

Microsoft NPS: Create a Connection Policy for Visitors and if regex expression condition is matched, forward to NRPS server group.

Aruba ClearPass: RADIUS Proxy Service configuration. Navigate to Configuration > Services

and select/edit the 'eduroam-outbound'/'proxy eduroam visitors to eduroam' service as configured in section 9 above. Don't forget to click [Save] when done.

In the Service Rule panel you can specify the conditions you wish to be matched for the Service to be applied. For proxying visitor requests to the NRPS, define a condition selecting requests with usernames that have non-local realm components.

It is recommended that the eduroam-outbound service should be configured with authentication conditions that reduce the number of auth requests with 'bad usernames' being forwarded to the NRPS as per lines 1 and 2 of the following table. Service Rule: Matches ALL of the following conditions:

Type	Name	Operator	Value
Authentication	Full-Username	MATCHES_REGEX	.*@[A-Za-z0-9-]+(\.[A-Za-z0-9-]+)*(\.[A-Za-z]{2,4})$
Authentication	Full-Username	NOT_CONTAINS	@'localrealm.' (*) 3gppnetwork, @gmail, @hotmail, @yahoo, @outlook, @live.co
Connection	Src-IP-Address	BELONGS_TO_GROUP	local WLC (**)
and optionally:			
RADIUS:IETF	Name Called-Station-Id	Operator: CONTAINS	Value: eduroam (***)

(*) e.g. @camford., @student.camford., @staff.camford. ; ie @.*camford\.ac\.uk$ should work; to catch frequent misspellings of camford you would need to include the frequent mispellings explicitly.

(**) Whatever name you give to the group of your campus wireless LAN controllers/APs.

(***) Some APs append the SSID name to their MAC address in the Called-Station-Id attribute - this can be useful when configuring handling of auth requests arising from your campus network.

FreeRADIUS: The proxy.conf file is where the logic for forwarding of authentication requests from Visitors is defined. In FreeRADIUS3 the remote RADIUS servers group is called the 'home_server_pool' - authentication request from Visitors can be sent to this. The authenticating servers (remote RADIUS servers) i.e. type 'auth' that were defined as 'home servers' are added to the 'home_server_pool'. The authentication policy/service is provided through the 'realm' section of proxy.conf. This defines the realm, some options, and indicates which server pool should be used for the realm. "Realms point to server pools, and server pools point to home servers".

The fail-over/load balancing mechanism to be used is defined in the home_server_pool section . FR3.0.x published at https://github.com/FreeRADIUS/freeradius-server/blob/v3.0.x/raddb/proxy.conf [31] (login to github will be required before you can access this) provides lots of descriptive text. The default option, 'fail-over' is not the preferred solution in eduroam(UK) since this leads to the 'hammering' of one NRPS. 'Load-balance' MUST NOT be used as EAP packets for the same conversation may be sent to different NRPSs. So, select type = 'client-port-balance' or 'client-balance'.

The 'realms' section is used to create rules for forwarding authentication requests to for a 'realm'. For Visitors the 'realm' can be called e.g. 'eduroam'. Using 'auth_pool', the home_server_pool to which authentications are sent is defined. And it is essential to add the directive 'nostrip' in order to ensure that the full username is used in the outer identity when the auth request is forwarded to the 'home_server_pool'.

So, as far as handling auth requests for Visitors goes, the essential sections of proxy.conf would be similar to:

```
#Define the NRPS pool for eduroam NRPSs
home_server_pool NRPS {
        home_server = roaming0
        home_server = roaming1
        home_server = roaming2
        type = client-port-balance
}

#Define a realm for non-‘my_organisation’ eduroam users
realm eduroam {
    auth_pool = eduroam
    nostrip
}
```

If using FreeRADIUS it is recommended you review our FreeRADIUS Demystified seminar material [32]. [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.

Cisco ISE

Policy set for external eduroam visitors – create a policy and configure this to use the RADIUS Server Sequence ‘Proxy to eduroam NRPS’

Policy > Policy Sets > 'eduroam External Visitors'

And you can use the authorisation policy settings to grant permission for guest access.

10.2 Visited Service Considerations - Request Proxying, RADIUS server timeouts and Load Balancing

a) (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.

b) **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.

c) **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.

d) **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 and 3.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).

e) **RADIUS server timeout should be set sufficiently long** 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. Do not rely on the default settings. 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.

Hints

Microsoft NPS: edit RADIUS Server dialog box, select the Load Balancing tab. The following settings are suggested:

- Request timeout: Number of seconds without response before request is considered dropped (default 3). Recommended value = 30
- Retransmits: Max number of dropped requests before server is identified as unavailable. Recommended value = 5
- Server back off timeout: Number of seconds between requests when server is identified as unavailable (default 30). Recommended value = 30

Aruba ClearPass: through the Policy Manager UI:

Administration > Server Manager > Server Configuration > Service Parameters (tab)

Select 'Radius server' from the drop down list.

In the Proxy section, the following parameters can be adjusted:

- Maximum Response Delay: If the target server has not responded, specify the time delay before retrying a proxy request. (Valid range 1 – 5. Default 5 seconds). Even the maximum 5 seconds time is very aggressive. We would like CPPM to offer a 30 second request timeout, but since this is not possible using the GUI, recommended value = 5.
- Maximum Retry Counts: If the target server doesn't respond, specify the maximum number of times to retry a proxy request. (Valid range 2 – 10. Default 5). Recommended value = 5
- Maximum Reactivation Time: Specify the time to elapse before retrying a dead proxy server. (Valid range 60 – 3600. Default 120 seconds). Recommended value = 30

If you make any changes, click on the [Save] button.

Cisco ISE: (capability introduced with ISE release 2.7) the following can be adjusted (through the webUI):

- Request timeout: 'Server Timeout'/'timeout' (valid range 1 - 120). Recommended value = 30
- Retransmits: 'Connection Attempts'/'retries' (valid range 1 - 9). Recommended value = 5
- Server back off timeout: 'RADIUS Proxy Failover Expiration'/proxyDeadTimeout' (valid range 1 - 600). Recommended value = 30

f) **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 receives 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.

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://community.jisc.ac.uk/library/network-and-technology-service-docs/implementing-eduroam-roadmap-part-4
[4] http://www.ja.net/products-services/janet-connect/janet-certificate-service
[5] https://wiki.geant.org/display/H2eduroam/EAP+Server+Certificate+considerations
[6] https://community.jisc.ac.uk/library/network-and-technology-service-docs/certificates-eduroam
[7] http://webmedia.company.ja.net/content/presentations/shared/networkshop300310/koster_understandingservercertif
[8] https://community.jisc.ac.uk/library/janet-services-documentation/using-server-certificates-factsheet
[9] http://www.ja.net/services/jcs/service-overview.html
[10] https://community.jisc.ac.uk/library/janet-services-documentation/using-certificates-issued-janet-certificate-service-ms-ias
[11] http://support.microsoft.com/kb/814394
[12] http://articles.techrepublic.com.com/5100-1035-6148560.html

[13] http://www.cs.bham.ac.uk/~smp/projects/peap/
[14] http://www.open.com.au/catool/index.html
[15] https://community.jisc.ac.uk/groups/eduroam/article/windows-mobile-8-and-certificate-verification
[16] http://community.jisc.ac.uk/groups/eduroam/article/use-least-sha-1-radius-server-certificates
[17] http://www.ja.net/jcs
[18] http://community.jisc.ac.uk/library/janet-services-documentation/using-certificates-issued-janet-certificate-service-ms-ias
[19] https://support.quovadisglobal.com/kb/a429/changes-to-security-indicators-in-the-chromium-browser-affecting-sha1-ssl-certificates.aspx?KBSearchID=34148
[20] http://www.microsoft.com/downloads/details.aspx?familyid=1971D43C-D2D9-408D-BD97-139AFC60996B&displaylang=en
[21] https://docs.microsoft.com/en-us/windows-server/networking/technologies/nps/nps-np-configure#configure-the-eap-payload-size
[22] https://technet.microsoft.com/en-us/library/cc755205%28v=ws.10%29.aspx
[23] https://community.jisc.ac.uk/library/janet-services-documentation/implementing-eduroam-roadmap-part-2
[24] https://support.eduroam.uk/login
[25] https://community.jisc.ac.uk/groups/eduroam/article/status-server
[26] http://community.jisc.ac.uk/library/janet-services-documentation/microsoft-nps-configuration-guide
[27] https://community.jisc.ac.uk/library/janet-services-documentation/microsoft-nps-configuration-guide
[28] https://community.jisc.ac.uk/library/janet-services-documentation/orps-role-designation-features-eduroamuk-support-server
[29] https://community.jisc.ac.uk/library/janet-services-documentation/filtering-invalid-realms
[30] http://community.jisc.ac.uk/library/janet-services-documentation/microsoft-nps-2008r2-config-avoid-bad-usernames-flooding-nrps
[31] https://github.com/FreeRADIUS/freeradius-server/blob/v3.0.x/raddb/proxy.conf
[32] https://community.jisc.ac.uk/groups/eduroam/document/nws-40-freeradius-demystified