eduroam administrators trouble shooting flowchart

This document is intended to serve as an aid for eduroam site administrators in troubleshooting problems with the implementation of the eduroam service at RADIUS server level. The document is split into two sections: remote user authentication, addressing problems your users may be experiencing at a remote site and visitor authentication, focussing on problems faced by yourvisitors from other sites. Please note, for successful troubleshooting you must be able to tick off the conditions in the 'Prerequisites' box.

Prerequisites

- Your ORPS must be registered on the JRS Support Server. It must be correctly peered with the JRS NRPS, be defined as test/devel, must be set for authentication, and must be added using a fully canonical DNS name that can be resolved from remote sites.
- The user name and password for a valid JRS test user account on your network must be entered on the main 'JRS Configuration' page for your organisation on the JRS Support server (this option is only visible after you have added an ORPS as above).
- Your JRS compliance level must be set to at least 'Working towards...' or 'Complies with...', or certain functions will not operate. If you have (or will have) users who will roam to other eduroam sites, then you must ensure that 'Home' is in the compliance; if you have (or will have) visitors then 'Visited' must be in the compliance. Sites having or expecting to have both remote users and visitors need to ensure that 'Home' and 'Visited' are in the compliance selection.
- After registering your ORPS on the JRS Support server or making status changes, you should allow one hour to elapse in order to ensure that the configuration change has propagated to the national proxies).
- You are able to run your RADIUS server in a debug mode – or with the highest level of logging detail. To derive maximum benefit from the remote user tests, your ORPS should be running in debug mode.

Remote user authentication

Issue 1: The 'Test ICMP' function doesn't work

Comment: The JRS technical specification states that your ORPS must be 'pingable' from the 3 NRPS systems and from the JRS Support server. There is one exception to this – the Cisco Secure ACS platform when running ACS, which offers TCP port 2002 as an alternative to ICMP for use in monitoring.

Fix: Ensure that your main campus firewalls, router ACLs or host firewalls allow ICMP protocol (specifically type 8 – echo request) to your ORPS from the NRPS and JRS Support server (ACS users, ensure that TCP port 2002 is open from the JRS support server). Sites using IPv6 must ensure this true for ICMPv6 if your ORPS has an IPv6 address.

Issue 2: I have IPv4 and ICMP holes but ICMP ping test still doesn't work

Comment: If your DNS record for the ORPS has an IPv6 AAAA record then the JRS Support server will use that address in preference to the IPv4 one.

Fix: If you are using IPv6 then ensure you have full IPv6 connectivity to the 3 NRPS addresses via IPv6 and the JRS Support server via IPv6 (e.g. ping them). If you don't have IPv6 connectivity then remove the AAAA record for the server in your DNS zonefile (and wait an hour).

Issue 3: JRS Support server remote user authentication tests fail

e.g. PEAP test fails with 'EAPOL test timed out' near the bottom of the output

```
'STA 02:00:00:00:00:01: Resending RADIUS
message (id=0)
Next RADIUS client retransmit in 12
seconds
STA 02:00:00:00:00:01: Resending RADIUS
message (id=0)
Next RADIUS client retransmit in 24
seconds
EAPOL test timed out
MPPE keys OK: 0  mismatch: 1
FAILURE'
```

e.g. PAP test fails with lots of 'Sending' messages but no 'Access-Reject' or 'Access-Accept' message at the bottom.

Comment: These types of failure indicate that the RADIUS messages are not reaching your ORPS

Fix: Firewalls/ACLs need to allow UDP port 1812,1813 and 1814 from the NRPS addresses to the ORPS address. These rules may also need to be adjusted to allow UDP 1812,1813,1814 to the NRPS (depending on direction of traffic). The systems must also allow fragmented UDP packets between the NRPS and ORPS (RADIUS packets can be large – much larger than 1500 bytes and thus they will get fragmented). Verify this issue by running a packet sniffer on the RADIUS server – e.g. tcpdump (Linux), snoop (Solaris) or wireshark (nee Ethereal – Windows, Linux, BSD).

Issue 4: Test fails but packets arriving at RADIUS server

Comment: Usually messages containing words such as 'WARNING: Bad authenticator in request from ...' (RADIATOR), 'WARNING: Unprintable characters in the password ...' (FreeRADIUS), RADIUS Client Authentication Attribute not Valid (NPS).

Fix: Double-check or re-enter the shared secrets for your ORPS. Remember, they are unique for every NRPS and each ORPS (nb. in a multi-ORPS environment each ORPSusually requires a different set of secrets). The secrets are listed on each ORPS page on the JRS Support server.

Issue 5: Some tests work, some don't.

Comment: There are a range of tests on the Support server. So long as the methods that your RADIUS server supports and that your users will be using work, then that is all that matters. A visiting user will **not** be doing EAP against your RADIUS server – that will be proxied to the NRPS. (Nb. your RADIUS server must not drop unknown EAP types! This can be validated with the simulated visitor user test – see later).

Issue 6: Tests that should work fail with reject messages appearing in the logs on the RADIUS server

Comment: Configuration issue.

Fix: Use the logs to see what/where things are failing – ensure that if the RADIUS server needs to talk to a third party box (e.g. domain controller, LDAP server etc.) then all that is working. Use tools such as IAS log viewer or web-based FreeRADIUS debug aider: http://networkradius.com/freeradius.html. NB RADIATOR is a section-by-section program – it goes through the config line-by-line so ensure that the config is written in the correct order.

If at this point you are still having problems you will need to contact JSD and put in a request for JRS technical support who are able to look at the logs on the NRPS and Support server to see what the issue might be.

Visitor authentication

Note: Local visitor test issues – as per 'Simulated Visitor Authentication Test' document on http://www.ja.net./roaming (Information for JRS administrators -> Test facilities available through JRS Support Server)

You must ensure that the laptop/device is configured with the username of e.g. your_realm@eduroam.ac.uk, that it is using the password for your JRS test account (and not the password you use to access the JRS Support Server). For this test, at present, no certificate checking or RADIUS server details are required.

Wireless adds in many additional hurdles – it is sometimes best to simply use command line tools (e.g. radpwtst (RADIATOR), radtest (FreeRADIUS), eapol_test (WPA supplicant) or NTRadPing (Windows)) to check that remote authentications work. These tools have to be used on the ORPS itself.

Issue 1: Client fails to authenticate (1)

Comment: This could be for many reasons – reason 1 – PHY issue

Fix: Ensure 'eduroam' SSID is available (advertised), that the signal is good and that e.g. a local test account works.

Issue 2: Client fails to authenticate (2)

Comment: Local accounts work, but RADIUS debug/logs show the 'visitor' client failing.

Fix: Check shared secrets are correct – when the ORPS talks to the NRPS it uses its 'proxy' section. This is often a separate section in the config and will need to be populated with shared secrets (taken from the ORPS page on the JRS Support server) – Nb. these are unique per ORPS and NRPS like the 'client' section shared secrets!

Issue 3: Client fails to authenticate (3)

Comment: Local accounts work, shared secrets double checked.

Fix: Ensure that the required RADIUS attributes are allowed through any RADIUS attributes filter you may have set up (see JRS Technical Specification).