This document is intended to serve as an aid for eduroam site administrators in troubleshooting problems with 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 your visitors from other sites. Please note, for successful troubleshooting you must be able to tick-off the conditions in the 'Prerequisites' box.

### 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 firewall 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 true this 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

```
SR (00:00:00:00:00:01) sending EAPOL start message (10)
SR (00:00:00:00:00:01) sending EAPOL start message (10)
SR (00:00:00:00:00:01) sending EAPOL start message (10)
```

**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 ORPS addresses. These rules may also need to be adjusted to allow UDP ports 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 will get fragmented). Verify this issue by running a packet sniffer on the RADIUS server – e.g. tcpdump (Linux), snmp (Solaris) or wireshark (see 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 …’ (RADIUS), ‘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-NRPS environment each ORPS usually 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 test user – 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 RADIUS is a section-by-section program – it goes through the config file-by-file 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

**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 a local test access 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) – No. 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).