

# JANET Roaming Service Advisory : eduroam

## Recommendation – Injection of Operator-Name RADIUS Attribute

August 2011

### 1. Executive Summary

This advisory presents our strong recommendation to all UK eduroam participants providing a Visited service, that where technically feasible, simple configuration changes are carried out on their eduroam RADIUS servers to put into practice inclusion of visited site identification information in the authentication requests sent to the JANET national RADIUS servers.

The cost of carrying out the recommended work is zero and the effort required is minimal; however the benefits are significant. The work involved includes simple modification of some reference files and server configuration script by organisations offering a Visited eduroam service.

At present within eduroam RADIUS authentication requests do not contain Visited site identification information. Furthermore it can take several hops between RADIUS servers before a user's authentication request ultimately reaches the Home site. Consequently the system administrator at the Home site has no simple way of determining where an authentication attempt has originated. This results in the investigation of problems being more difficult than needs to be.

In order to assist system administrators engaged in the task of troubleshooting problems eduroam users may be having, specifically by making it easier to locate relevant sections in RADIUS logs and to identify problems, **JANET strongly recommends wherever possible the implementation of injection of the Operator-Name RADIUS attribute into Access-Request packets forwarded to the JANET National RADIUS Proxy servers by all RADIUS servers at organisations offering Visited eduroam services.**

A further benefit of carrying out the recommendation is that organisations will be ready for any future requirements arising from developments being explored by eduroam.org relating to the CUI RADIUS attribute – effective use of which depends on Operator-Name also being employed.

***This advisory is applicable only to FreeRADIUS and Radiator systems at present*** since MS IAS/NPS and Cisco Secure ACS do not support the IETF RFC standard describing the attribute and its utilisation. Organisations with Microsoft proxy servers should note the contents of the JANET advisory, 'Operator-Name RADIUS Attribute Issues in MS IAS and NPS,' issued November 2010. This can be found on:

[www.ja.net/services/authentication-and-authorisation/janet-roaming/documentation.html#service\\_documentation](http://www.ja.net/services/authentication-and-authorisation/janet-roaming/documentation.html#service_documentation)

#### Contents:

- [Executive Summary](#)
- [Introduction](#)
- [Background](#)
- [Technical Rationale and Business Case](#)
- [Considerations](#)
- [Implementation Instructions \(FreeRADIUS and Radiator\)](#)
- [Timescale](#)

## 2. Introduction

This advisory describes our strong recommendation to all Visited site eduroam participants in the UK, where technically feasible, to implement injection of the Operator-Name RADIUS attribute at their ORPS into all Access-Request packets forwarded to the NRPS. Therefore at present it is only applicable to organisations employing FreeRADIUS and Radiator proxy servers. Organisations with Microsoft proxy servers should note the contents of the JANET advisory, 'Operator-Name RADIUS Attribute Issues in MS IAS and NPS,' issued November 2010.

Operator-Name (O-N) is a standard RFC 5580 RADIUS attribute and can uniquely identify the owner of an 802.1X access-controlled network (e.g. by providing the visited site's realm name). The benefits to all UK eduroam organisations of introducing O-N injection fully justifies the straightforward configuration work required for its implementation - which can be carried out on FreeRADIUS and Radiator RADIUS applications. Nb. It is not at present possible to configure Microsoft IAS and NPS to inject O-N.

The background, business case and implementation instructions are included in this document. There is also a description of the JRS monitoring system that is place to check conformance and the means by which a participant's provision of this enhancement to their eduroam service will be advertised.

This advisory is applicable with immediate effect. The work involved in implementing the recommended configuration change on RADIUS servers is minimal. The recommendation will become part of the JRS eduroam Technical Specification later this year.

## 3. Background

Of the enhancements to the JANET eduroam service to improve support of roaming users, one of the most requested is a facility to identify which remote site a particular RADIUS Access-Request packet is coming from - which in practice would result in the ability to correlate users' login problems with specific remote site locations.

The primary aim of encouraging the use of the Operator-Name attribute throughout eduroam in the UK is to provide a solution to the above issue.

The inclusion of Operator-Name in the Access-Request sent to the NRPS for forwarding to the user's Home (IdP) organisation, can greatly assist the Home organisation's eduroam system administrator in identifying entries in the RADIUS logs relating to the visited site where the user actually is when attempting to troubleshoot in real time a specific problem the user is having. Furthermore, being able to identify Visited sites also greatly assists the system administrator during routine inspection of logs to check for any problems.

Of relevance to this initiative it should be noted that the injection of Operator-Name is becoming increasingly common in a growing number of European countries. There is a current GÉANT JRA3 project which is investigating the use of the Chargeable User Identifier attribute (CUI) within eduroam. To achieve a practical application, both Operator-Name and CUI information is needed. The aim is to provide the system administrator with a unique user key to identify the user, eliminating the intrinsic uncertainties in the current outer-id and MAC address identification methods. This would help when investigating cases of policy abuse. However, the scope of this advisory is limited to the injection of Operator-Name.

#### 4. Technical Rationale and Business Case

At present within eduroam, RADIUS packets are forwarded by RADIUS proxy servers to a user's home organisation based simply upon the user's outer anonymous identity (the realm name of their home organisation). Responses are returned via the chain of proxy servers to the remote site at which the user is attempting to gain authenticated network access. The RADIUS packets contain no information relating to the realm or organisation from which they were transmitted.

This is not helpful for the Home site eduroam system administrator during inspection of RADIUS server logs when attempting to troubleshoot a problem that a particular roaming user might be experiencing at a remote site; or who, in the course of routine inspection of RADIUS logs, detects an unusually large number of failed authentication attempts. The problem at present is that there is no way of correlating an entry in the server log to the realm of the organisation from which the RADIUS packet came.

By injecting the Operator-Name attribute into Access-Requests sent to the NRPS, the Visited site will greatly help the Home site system administrators in the above scenarios, and by way of return of complement, will benefit from injection of O-N at sites their users visit.

Apart from contributing towards the general improvement in the efficiency and effectiveness of troubleshooting and problem detection throughout the eduroam community, the injection of O-N can be seen as an enhancement of the quality of the eduroam service that the Visited site organisation is providing.

The provision of this feature at a Visited site will contribute towards any future rating of the eduroam service offered by a participating organisation – the injection of O-N would be an important differentiator of quality of eduroam service provision, in a similar way to offering other premium features such as IPv6, WPA2-only Wi-Fi or 'get you started' setup and remediation VLANs.

As mentioned above, there is a current GÉANT JRA3 project which is investigating the use of the Chargeable User Identifier attribute (CUI) within eduroam. To achieve a practical application, both Operator-Name and CUI information is needed. By implementing O-N injection, organisations will be ready for any future requirements arising from the JRA3 developments.

The final deciding point in favour of implementing O-N injection is that it is very simple to set up and can be achieved at zero cost.

Nb. There are already a number of eduroam organisations injecting O-N:

Aston University  
Imperial College  
London School of Hygiene and Tropical Medicine  
Loughborough University  
JANET(UK)  
National Science Learning Centre  
Nottingham Trent University  
University of Bristol  
University of Lincoln  
University of London.

Help freely is available for any organisation uncertain as to the details of what is involved, either from local mentor institutions or through the usual JRS Support service.

## 5. Considerations

- Alternative ways of providing visited realm information
- Consequences for user privacy
- eduroam system administrator work effort required
- RADIUS packet size increase, affect on firewalls
- RADIUS attributes filtering
- RADIUS log files
- Impact on JRS Technical Specification
- Monitoring/test of O-N injection
- Advertisement of enhanced Visited site feature to the eduroam community
- Technical capability of various RADIUS platforms to inject O-N

### Alternatives

JANET has considered various ways of providing site information using alternative attributes, but the conclusion has been reached that Operator-name is the most satisfactory mechanism.

### User Privacy

We have also considered the consequences of injecting Operator-Name and the implications for user privacy. The conclusion is that this would add no further information than could be gleaned through other mechanisms. The relationship between the user and parent organisation and the expectations of the users are such that it is reasonable for the parent organisation to record the O-N attribute in the RADIUS logs, which in any case are retained for a limited period only.

### Implementation Effort

The amount of work involved for system administrators in introducing O-N injection has been weighed up against the benefits to the eduroam community. Configuration guides have been put together as detailed below and the effort now required to implement the changes is minimal.

### RADIUS Packet Size

There are few technical considerations; any use of RADIUS attributes increases the RADIUS packet size. This could potentially have the effect of increasing the degree of UDP packet fragmentation which could result in problems with misconfigured firewalls. However a number of other attributes are already in use within eduroam, so the increase in packet size due to inclusion of O-N will be minimal. In any case, guidelines for configuration of firewalls are already included in JRS eduroam implementation guides and so firewalls should be properly configured already to not reject fragmented UDP packets.

### Attribute Filtering and Logging

The second technical note is that at the RADIUS attributes filtering level within ORPS, the Operator-Name attribute should NOT be filtered out. Ensuring that this is the case should be a trivial matter for system administrators. A related issue is that the Operator-Name value should be recorded in the RADIUS log files. Again this is a simple measure which should take very little time to accomplish.

### JRS Tech Spec

There is nothing in the current JANET Roaming Technical Specification that prevents immediate adoption of O-N injection by Visited sites. There are nevertheless various changes to the Specification that will be extremely helpful in ensuring that the recommended measures are widely adopted and effective. The requisite changes to the JRS Technical Specification will be introduced shortly, however there is no reason for organisations wishing to introduce O-N injection to wait for these changes to become effective.

### Testing and Monitoring

Since it is feasible that mistakes could be made in implementing O-N injection and we attach considerable importance to this initiative, something we would like to see universally adopted (where possible), a means of testing that organisations have been successful in introducing it was considered necessary. Therefore a test (monitoring) system has been set up.

The JRS Support Server is now able to detect the inclusion and accurate composition of O-N for each registered realm during simulated visitor test authentications – which may be run ad-hoc by participants or as part of a service monitoring system. The ‘JRS Configuration’ web page, which the JRS Technical Contact at each participating organisation has access to, presents the status of O-N injection via the JRS Minor Issues panel. Where an organisation is not injecting Operator-Name (or is injecting a malformed O-N), the administrator will see the prompt, ‘You are not sending Operator-Name attribute from you ORPS’; successful O-N injection results in the message, ‘Congratulations, we have detected Operator-Name attribute '1your\_realm' from your ORPS.’

It should be noted that if an organisation has more than one ORPS sending visitor test Access-Requests to JRS Support, then obviously both RADIUS servers should be configured to inject O-N. If one ORPS injects O-N whilst the other does not, the JRS Support Minor Issues panel will flip between indicating successful O-N injection and a negative result.

### Advertisement of enhanced Visited site feature

Injection of Operator-Name is viewed as a significant service enhancement and so some means of advertising the adoption of this recommendation by organisations to the eduroam community was required. Using the results from the above monitoring system, a new field has been added to the sites data that is published on the JANET ‘where you can use eduroam’ map and downloadable spreadsheet sites listing. The information (no O-N injection, yes O-N injection, error in O-N injection) is also available to eduroam.org to incorporate into their comprehensive database of eduroam sites details.

### Technical capability of various RADIUS platforms to inject O-N

An issue arises regarding the technical capability of various RADIUS platforms to inject O-N, which has caused some difficulties. As advised previously, Microsoft IAS and NPS RADIUS implementations contain a flaw due to the inclusion of pre-RFC5580 values for attribute 126 in the attribute dictionaries and the consequent behaviour of the servers when in receipt of RADIUS packets containing (properly formed) O-N attributes - in cases where the server was configured to peer with specific RADIUS client vendors. In such cases the servers simply marked (and logged) the correctly formed packet as ‘malformed’ and rejected it with no return response to the originating RADIUS client. There is a further issue with Microsoft IAS and NPS. At present there is no way for O-N to be injected into packets for forwarding to the NRPS. Whilst this situation may be corrected in future releases of NPS, this is unlikely to be the case for IAS.

In addition to the problems related to Microsoft IAS and NPS, at the present time, we have no verified configuration for the Cisco Secure ACS 4.2 or 5.1 platforms and so cannot recommend O-N injection for these.

***In view of the above, we are therefore limiting this advisory to a strong recommendation for FreeRADIUS and Radiator systems only.***

## 6. Implementation

### Applicability

At the present time it is only possible to implement injection of Operator-Name using the FreeRADIUS and Radiator RADIUS platforms.

### Accurate Composition of Operator-Name Attribute

There are many ways that the name of the network operator can be composed within the Operator-Name attribute. In eduroam, organisations are identified by their realm names, which is one of the naming conventions defined with RFC 5580 (registered domain name). The other naming conventions include: TADIG codes; Mobile Country/Mobile Network Codes; and ITU Carrier Codes. To identify the naming convention in use, the Operator-Name attribute contains a Namespace ID field. This is followed by the actual operator-name data.

To use registered domain name, the Namespace ID must be set to 'REALM', which is defined as '1'. This must be prefixed to your actual realm name. Therefore, for an organisation whose realm name is 'myorganisation.ac.uk', the Operator-Name is '1myorganisation.ac.uk' .

### Dictionary Files in Free RADIUS

Certain dictionary files in FreeRADIUS contain Attribute 126 definitions that are at variance with the IETF definition of Attribute 126 being Operator-Name, which has certain implications:

- dictionary.usr defines 'Multi-Link-Flag' as Attribute 126
- dictionary.ascend defines 'X-Ascend-Temporary-Rtes' as Attribute 126

Prior to version 2.1.9 there were other offending dictionaries\*, but these were corrected in FreeRADIUS 2.1.9 onwards. [In recent versions, the format of the dictionary files has been changed such that VSAs are now encoded in blocks between 'BEGIN-VENDOR *vendor\_name*' and 'END-VENDOR *vendor\_name*'. If an attribute definition of Attribute 126 is between such block denominators, it is a VSA 126, not an IETF Attribute 126 - which means it does no harm.]

\*Versions of FreeRADIUS 2.1.8 and earlier contained dictionary files with non-IETF definitions of Attribute 126: dictionary.acme, dictionary.alvarion, dictionary.ericsson, dictionary.ern, dictionary.huawei, dictionary.itk, dictionary.lucent.

All versions of FreeRADIUS will operate normally if a server receives an Access-Request containing O-N without these dictionaries being corrected (unlike MS IAS and NPS). However O-N will be truncated or incorrectly formatted and the server will not process the attribute correctly. Also O-N data in your logs (which you should set up for recording O-N) will be meaningless. Furthermore, without the modifications described below, a server will not inject O-N using the correct format. It is hoped that this problem will be remedied in next version of FreeRADIUS (2.2.0).

## **FreeRADIUS 2.x Configuration Changes**

There are a number of ways of implementing Operator-Name injection. The following describes one simple method which, it should be noted, injects O-N into requests forward to ALL RADIUS proxies (i.e. including any that are not part of the JRS infrastructure).

1. Correct the dictionary definition of Attribute 126. An elegant solution is to make a one line addition to your [/usr/local]/etc/raddb/dictionary file to correctly define the attribute. This is better than editing individual dictionary files (or the main dictionary file to comment out the line which imports the offending files) because if a reinstallation of FreeRADIUS is ever carried out, the dictionaries in [usr/local]/share/freeradius/ would get over-written, so the changes would have to be reapplied.

Add the following line at the end of your [usr/local]/etc/raddb/dictionary file:

```
ATTRIBUTE Operator-Name 126 string
```

2. Set attribute filters to pass O-N. If you are using the attribute filter system then edit \$RADDB/attr and \$RADDB/attrs.pre-proxy and add the following to your filters to AND from the NRPS systems:

```
Operator-Name =* ANY
```

3. Inject O-N into outgoing Access-Requests. The aim is to add this attribute to outgoing packets that are heading to the NRPS. However you MUST NOT replace the attribute if the packet is coming from the NRPS (since it should contain an O-N attribute inserted by a Visited site!)

The simplest way to do this is to add the following 'unlang' to the pre-proxy section of your FreeRADIUS configuration – the section that prepares for forwarding requests to the NRPS:

```
update proxy-request {
    Operator-Name := "1myorganisation.ac.uk"
}
```

```
e.g. pre-proxy {
    update proxy-request {
        Operator-Name := "1camford.ac.uk"
    }
    [rest of your local configuration here]
}
```

4. Verify that your configuration changes have been successful. (Important!)

Access-Request packets going to the NRPS should now contain the 'Operator-Name' attribute correctly composed in RFC 5580 format for your realm. You can check this by running the server in debugging mode using radiusd -X.

You must validate successful injection of O-N. Perform a 'simulated visitor test' (\*) and check the 'JRS Minor issues' panel on your JRS Configuration web page on JRS Support. If the JRS Support Server detects that Access-Requests from your ORPS contain O-N, the status of the 'JRS Minor issues' panel on your JRS Configuration web page will indicate this by showing, "Congratulations, we have detected Operator-Name attribute '1myorganisation.ac.uk' from your ORPS."

5. Finally, modify your RADIUS logs to record the O-N attribute value for incoming Access-Requests.

## **Radiator 4.x Configuration Changes**

1. Edit your dictionary file(s) - no included files, barring the RFC 5580 file or section, should have Attribute 126 (offending lines are Ascend-Temporary-Rtes, USR-Number-of-Link-Timeouts and Ascend-Route-Preference).
2. Inject O-N into outgoing Access-Requests. In your main configuration file, go to the final section where you send requests to the NRPS systems (this is usually your last handler) and add the following into the handler:

AddToRequest Operator-Name=1myorganisation.ac.uk

(e.g. AddToRequest Operator-Name=1camford.ac.uk)

If you want to ensure that no overwriting occurs (for example in cases where you have set the Operator-Name on an internal RADIUS server) then use this instead:

AddToRequestIfNotExist Operator-Name=1myorganisation.ac.uk

3. Verify that your configuration changes have been successful. (Important!)

If you now run Radiator with a debug level of 4, you should see the O-N attribute being sent to the NRPS.

You must validate successful injection of O-N. Perform a 'simulated visitor test' (\*) and check the 'JRS Minor issues' panel on your JRS Configuration web page on JRS Support. If the JRS Support Server detects that Access-Requests from your ORPS contain O-N, the status of the 'JRS Minor issues' panel on your JRS Configuration web page will indicate this by showing, "Congratulations, we have detected Operator-Name attribute '1myorganisation.ac.uk' from your ORPS."

4. Finally, modify your RADIUS logs to record the O-N attribute value for incoming Access-Requests.

### **(\*) Simulated Visitor Test**

Since eduroam is an integral part of the essential authentication service for both visitors and own organisation users at remote sites, all organisations offering eduroam should be carrying out live service monitoring - any problems being flagged up for priority action. The JRS simulated visitor test can form part of this, showing that visitors to your organisation can authenticate via the JRS/eduroam infrastructure. To do this you simply need to add 'realm.ac.uk'@eduroam.ac.uk (and use your JRS-registered test account password) to the RADIUS test function of your chosen monitoring platform, be it NAGIOS, SolarWinds, IEA Radlogin or a home-developed system. For the purpose of validating your successful implementation of O-N injection (or troubleshooting!) you can run a one-off simulated visitor test using FreeRADIUS radtest or Radiator radpwtst.

The simulated visitor test is documented at:

[http://www.ja.net/services/authentication-and-authorisation/janet-roaming/implementing-jrs.html#visitor\\_test](http://www.ja.net/services/authentication-and-authorisation/janet-roaming/implementing-jrs.html#visitor_test)

## **7. Timescale**

It is recommended that the above configuration changes are scheduled into RADIUS system administrator work as soon as possible.

The requisite changes to the JRS Technical Specification will be introduced shortly however there is no reason to wait for these changes.

Ed Wincott  
JANET Roaming Service Manager  
JANET(UK)