RADIUS Attribute Issues regarding RFC5580 (Operator-Name and others) with several RADIUS servers (including Microsoft IAS and NPS)

The advisory is based on the JANET Roaming Service Advisory (*Operator-Name RADIUS Attribute Issues with MS IAS and NPS*) issued in November 2010.

Background

A growing number of eduroam® Service Providers are including the *Operator-Name* RADIUS attribute when sending Access-Request authentication packets to their federation-level RADIUS servers (FLR) for forwarding to the user's responsible eduroam Identity Provider.

Operator-Name is a standard RFC5580 RADIUS attribute and can uniquely identify the owner of an access network (e.g. the Service Provider realm name). Including it in the Access-Request is encouraged because this greatly assists in user support given by the eduroam Identity Provider. Being able to identify entries in the RADIUS logs relating to the Service Provider where the user is located helps when inspecting logs during routine problem identification analysis or for real-time troubleshooting a specific problem for a user.

Issue

A problem has been identified with Microsoft IAS (Internet Authentication Service) on Windows Server 2003 and NPS (Network Policy Server) on Windows Server 2008. It is possible that all Access-Requests containing RFC5580 attributes will be dropped if IAS and NPS have been misconfigured to set the type of client incorrectly to *Ascend Communications* (the setting's name is *RADIUS Clients Vendor Name* in IAS and *Client Vendor type* in NPS). In the case of IAS (additional to the configuration change), a dictionary file fix also needs to be applied for RFC5580 attributes.

This problem means that if you are an eduroam Identity Provider using one of these Microsoft products, your users may **not** be able to gain network connection when visiting other eduroam sites. You are requested to check your IAS and NPS configurations as detailed below. In addition, regarding IAS you must carry out a simple database file modification.

This issue is of concern because a user’s inability to gain network connection when visiting other eduroam sites will only be detected if the user reports a problem and the Service Provider and Identity Provider begin an investigation; or if the events log is regularly inspected by the Identity Provider.

Explanation of Problem

Microsoft built into the IAS/NPS product the capability for it to be configured such that remote access policies can be based on the client vendor’s attribute. In the RADIUS client’s properties configuration window there is an option to select the *Vendor Name* (or in the case of IAS*, Client-Vendor*). This results in the relevant dictionary being loaded.

The root of the problem is a naming clash between the values in IAS/NPS RADIUS attribute dictionaries and standard RFC 5580 usage. *Operator-Name* has a standard attribute number of 126 and is a string. Historically, 126 has also been used by other vendors (such as Ascend) for their own purposes.

Unfortunately, attribute 126 has ended up being defined as a 32 bit (4-character) integer in IAS/NPS dictionaries. After a dictionary containing a clashing entry for attribute 126 is loaded, Windows IAS/NPS expects a 4-octet integer value as a value of attribute 126. Sites sending *Operator-Name* as a string will most likely use a value of length other than 4. Upon receipt of such an attribute, Windows observes attribute definition mismatch and drops the RADIUS packet.

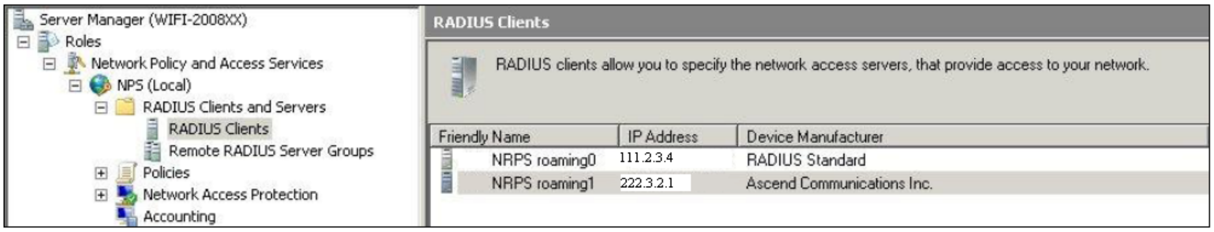
The user’s authentication attempt then fails and the Service Provider's RADIUS server receives nothing in return to explain why the attempt has failed. The NAS (AP) with which the user is associating may or may not get a response from the RADIUS server, depending on whether it has been configured to send Access-Reject when the proxied request times out. The user simply experiences a failed authentication attempt. However the problem can be identified by an entry in the Events log of the Identity Provider's RADIUS server (*malformed radius packet received)*.

MS NPS Check/Fix

In the case of NPS, the conflicting attribute will not be enabled if *RADIUS Standard* has been selected as the Vendor Name. Attribute 126 will be correctly recognised and your eduroam Identity Provider will process Access-Requests containing *Operator-Name*.

The solution for NPS in Win2008 is to check that the Vendor Name for your federation's FLR server is set to *RADIUS Standard* and not to *Ascend Communications* in NPS/RADIUS Clients and Servers/RADIUS Clients in the Server Manager configuration tree. Open Server Manager, navigate down Roles/Network Policy and Access Services/NPS/RADIUS Clients and Servers/RADIUS Clients.

The RADIUS Clients pane displays the IP Address and Vendor Name (Device Manufacturer) that has been set. Device Manufacturer should be *RADIUS Standard*. Figure 1 shows configurations for the federation's FLR servers; roaming1 is incorrect and roaming0 is correct.

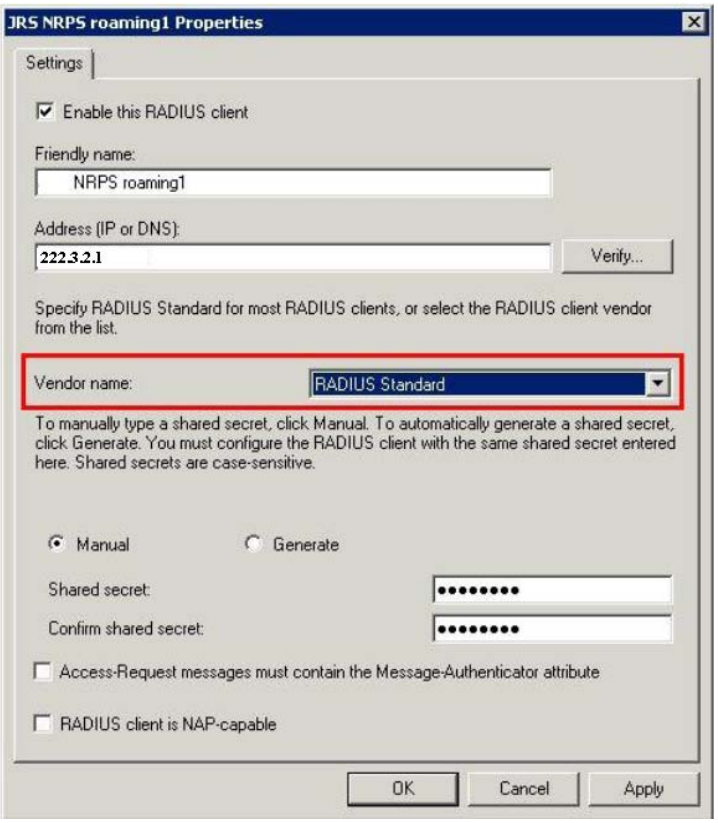

Server Manager (WIFI-2008XX)
Roles
Network Policy and Access Services
NPS (Local)
RADIUS Clients and Servers
RADIUS Clients
Remote RADIUS Server Groups
Policies
Network Access Protection
Accounting
RADIUS Clients

RADIUS clients allow you to specify the network access servers, that provide access to your network.

Friendly Name	IP Address	Device Manufacturer
NRPS roaming0	111.2.3.4	RADIUS Standard
NRPS roaming1	222.3.2.1	Ascend Communications Inc.

Figure 1: Radius Clients configuration

If the Device Manufacturer is not set to *RADIUS Standard*, right click on the client (e.g. the federation's FLR server roaming0) and select Properties. A dialogue box opens. Set Vendor name to *RADIUS Standard*, click *OK* and quit.



JRS NRPS roaming1 Properties

☑ Enable this RADIUS client

Friendly name: NRPS roaming1

Address (IP or DNS): 222.3.2.1

Specify RADIUS Standard for most RADIUS clients, or select the RADIUS client vendor from the list.

Vendor name: RADIUS Standard

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

● Manual ○ Generate

Shared secret: •••••••••

Confirm shared secret: •••••••••

☐ Access-Request messages must contain the Message-Authenticator attribute

☐ RADIUS client is NAP-capable

Figure 2: roaming1 Properties window

MS IAS Fix

In the case of IAS, even if the Client-Vendor name is correctly set in the client properties to *RADIUS Standard*, Access-Requests containing *Operator-Name* will be dropped.

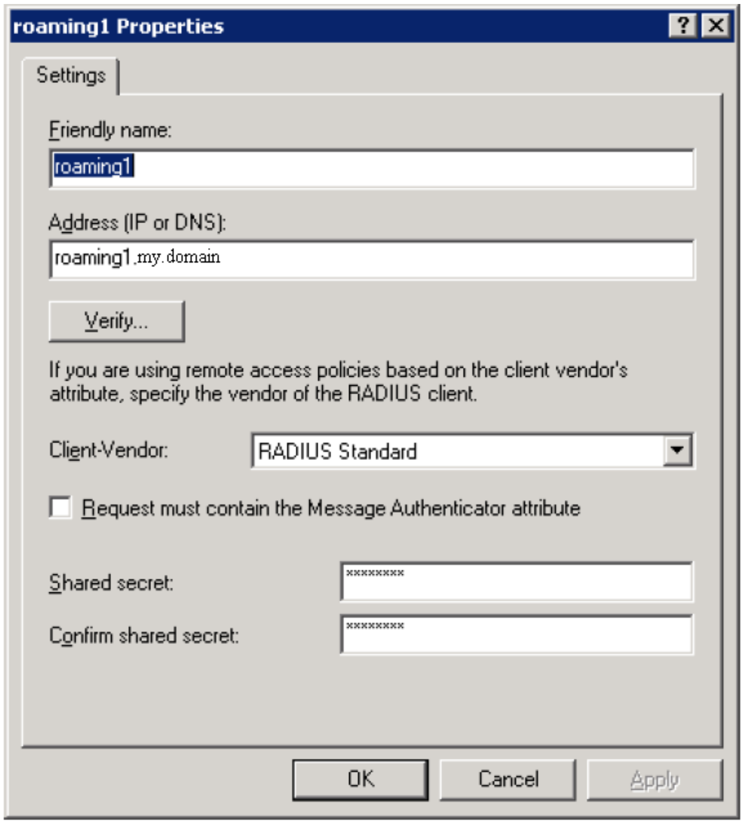
The solution is a little more involved and it is necessary to modify an IAS database file as follows. **It is essential that MS IAS sites carry out this fix at the earliest opportunity.**

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

Attribute number	Name	Syntax
126	Operator-Name	String

Table 1: Name and syntax values

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



roaming1 Properties

Friendly name: roaming1

Address (IP or DNS): roaming1.my.domain

If you are using remote access policies based on the client vendor's attribute, specify the vendor of the RADIUS client.

Client-Vendor: RADIUS Standard

□ Request must contain the Message Authenticator attribute

Shared secret: *********

Confirm shared secret: *********

Figure 3: MS IAS RADIUS Client Properties window

Consequences

The use of *Operator-Name* is fairly widespread in eduroam in Europe, and its use is endorsed in the eduroam community. Other RFC5580 attributes may also appear sporadically, depending on NAS equipment. An IAS/NPS misconfiguration can affect any given eduroam user whose Identity Provider has not fixed its IAS/NPS configuration. Consequently this MS IAS/NPR issue represents a significant problem. **We request that you carry out the recommendations above at your earliest opportunity.**

Note: Once the above has been carried out, your system will be enabled to **not** deny service to your users when visiting organisations where Operator-Name insertion is implemented. For those system administrators who would like to implement Operator-Name insertion at their own site, regrettably (following extensive investigations), our conclusions are that neither IAS nor NPS can be configured to insert *Operator-Name* themselves. Therefore you will not be able to add this valuable functionality using IAS/NPS. We will be addressing this issue with Microsoft.

Other RADIUS Servers

Attribute definition clashes are known to occur in many popular RADIUS servers. For some implementations, most notably Radiator, FreeRADIUS and radsecproxy, the clashes (if any) do not lead to as severe problems as with IAS and NPS. The only consequence observed so far is that the content of the *Operator-Name* attribute may become garbled.

Besides IAS and NPS, the implementation Navis RADIUS is also known to be problematic. Instructions for fixing Navis RADIUS' dictionary are available on request.

If you are using a RADIUS server implementation which is not mentioned in this advisory, we advise you to investigate the consequences of RFC5580 attributes and contact your federation operator, if necessary.

Acknowledgements in Original Advisory

Many thanks to James Hooper from the University of Bristol and Phil Mayers from Imperial College for identifying and providing a fix for this problem.

https://www.wireless.bris.ac.uk/netcomms/ias-radius/

Acknowledgements

Many thanks to Ed Wincott, JANET Roaming Service Manager, for making this advisory available to the whole eduroam community.