JANET Roaming Service Advisory : eduroam
Operator-Name RADIUS Attribute Issues with MS IAS and NPS
November 2010

Background

A growing number of Visited site eduroam organisations are including the **Operator-Name** RADIUS attribute when sending Access-Request authentication packets to the NRPS for forwarding to the user's home organisation. Operator-Name is a standard RFC5580 RADIUS attribute and can uniquely identify the owner of an access network (e.g. the visited site realm name). Including it in the Access-Request is to be encouraged because this greatly assists in user support by the Home organisation. Being able to identify entries in the RADIUS logs relating to the visited site where the user actually is greatly assists when inspecting logs during routine problem identification analysis or for real time troubleshooting of a specific problem a user is having.

Issue

A problem has been identified with Microsoft IAS on Windows Server 2003 and NPS on Windows Server 2008. It is possible that all Access-Requests containing the Operator-Name attribute will be dropped if IAS and NPS have been misconfigured to have RADIUS Clients Vendor Name/Client Vendor type set as 'Ascend Communications' and in the case of IAS a dictionary file fix also needs to be applied.

This problem means that if you are a Home site 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 and in the case of IAS you must carry out a simple database file modification.

This issue is of concern because the above situation will only be detected if a frustrated user reports a problem and the Visited site and the Home site begin an investigation or the Events log is regularly inspected at the Home organisation. We have however carried out a test to identify organisations at risk.

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'. Hence in the RADIUS clients properties configuration window you have the option to select the Vendor Name (or Client-Vendor: in the case of IAS). This results in the relevant dictionary being loaded by Windows.

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 is standard attribute number 126 and is a string. Historically, 126 has also been used by other vendors (e.g. Ascend) for their own purposes, and unfortunately attribute 126 has ended up being defined as a 32 bit (4 character) integer in IAS/NPS dictionaries. If after a dictionary containing a clashing entry for attribute 126 is loaded, Windows receives an access-request packet containing attribute 126 as a string (which will be the case for all sites sending Operator-Name using FreeRADIUS and Radiator ORPS), it flags up a type clash and drops the RADIUS packet.

The user's authentication attempt therefore fails and the Visited site ORPS receives nothing back explaining why the attempt has failed. The NAS (AP) the user is associating with may or may not get a response from the ORPS 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. A "malformed radius packet received" log entry is however made in the Events log of the Home site ORPS, which you should be able to identify.

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 ORPS will process Access-Requests containing Operator-Name.

The solution for NPS in Win2008 is to check that the Vendor Name for the three NRPS is set to 'RADIUS standard' and not 'Ascend Communications' in the NPS/RADIUS clients and servers/RADIUS clients configuration tree in the Server Manager. Open Server Manager, navigate down Roles/Network Policy and Access Services/NPS/RADIUS Clients and Servers/RADIUS Clients.

The RADIUS clients pane will display the IP Address and Vendor Name (Device Manufacturer) that has been set. Device Manufacturer should be 'RADIUS Standard'. This screenshot shows an incorrect configuration for roaming1.
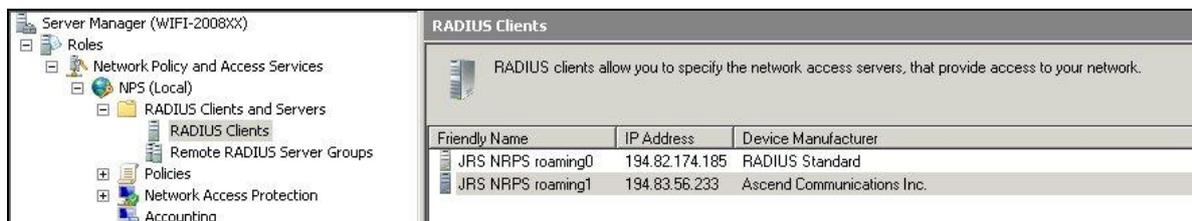
If the Device Manufacturer is not 'RADIUS Standard', right click on the client (roaming0, roaming1 and roaming2) and select Properties. A dialogue box will open and you can set Vendor name to RADIUS Standard. OK and quit.
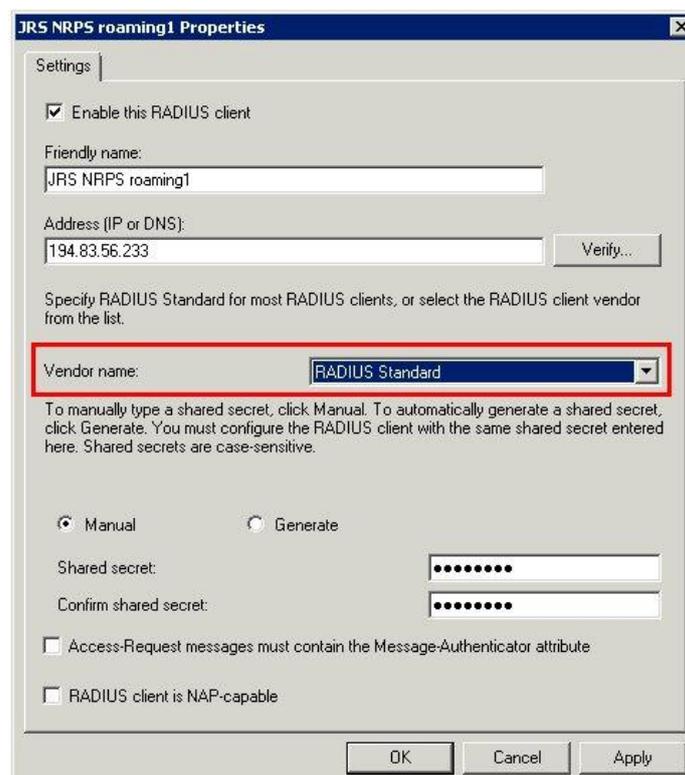
MS IAS Fix

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

The solution is a little more involved and it is necessary to modify an IAS database file as below. It is however **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** to **Operator-Name**
7. Change the **Syntax** to **String**
8. Close Access, and start IAS

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

File	Date	Size	md5sum
dnary.mdb (before-edit)	2007-02-18, 11:00	294912	c81613ae3ccd57eaec68645d8cdd033f
dnary.mdb (AFTER-edit)	-	303104	292675ae20c9fccfa6d07b632947ba24

Screen shot of MS IAS RADIUS Client properties box:

Consequences

Since relatively few UK sites at present send Operator-Name, this is not yet a widespread problem for users roaming within the UK, despite there being some 34 participants that have registered IAS/NPS ORPS (with recent IAS/NPS joiners yet to register their ORPS). However the use of Operator-Name is more widespread in Europe so will be affecting users roaming to sites overseas. Furthermore we would like to encourage (and in the future mandate where possible) more widespread use of Operator-Name in the UK. Consequently this MS IAS/NPR issue represents a significant problem.

We therefore request that you carry out the recommendations above at your earliest opportunity.

Nb. 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 taking this issue up with Microsoft.

Acknowledgements

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

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

Ed Wincott
JANET Roaming Service Manager
JANET(UK)

November 2010