Configuración de IAS para eduroam

Referencia	--
Fecha	06/05/2011-23/05/2011
Autores	Evangelino Valverde
Revisores	[Nombre y apellidos de los revisores]
Destinatarios	Administradores del servicio eduroam en la comunidad RedIRIS
Descripción	Este documento describe la configuración del servidor IAS para gestionar la autenticación de usuarios de eduroam.
Palabras clave	RADIUS, IAS, Servicio de Autenticación de Internet, Wi-Fi, eduroam

1 Introducción

El objeto de este texto es documentar la configuración del servidor RADIUS de Microsoft para el servicio eduroam. Las políticas de esta configuración estarán preparadas para admitir configuraciones para otros ámbitos (por ejemplo VPN) sin que entren en conflicto con las de eduroam.

2 Escenario y solución propuestas

Se propone el escenario típico de una institución académica en la que existen distintos colectivos que deben/pueden ser tratados de forma diferenciada:

- **Alumnos**. Estudiantes de la propia institución.
- **PDI**. Personal Docente e Investigador de la propia institución.
- **PAS**. Personal de administración y servicios de la propia institución.
- **Invitados**. Usuarios procedentes de otras instituciones o locales no comprendidos en ninguno de los colectivos anteriores.

La solución propuesta para este escenario consiste en:

- Ubicar a cada uno de los colectivos en una LAN inalámbrica distinta, de forma que puedan aplicarse políticas específicas para cada colectivo a nivel de filtrado, gestión de ancho de banda, etc.
- Emplear **PEAP** con **EAP-MSCHAP v2** como método de autenticación en los suplicantes 802.1x.

3 Requisitos previos

Antes de comenzar a ejecutar las indicaciones de esta guía, se deben cumplir las siguientes condiciones:

1. Disponer de un servidor **Windows 2003 con IAS** instalado, integrado en el dominio Windows de la organización. Si la instalación cuenta con más de 50 clientes RADIUS (puntos de acceso o controladoras, dependiendo de la arquitectura) es necesaria la versión **Enterprise** de Windows 2003.

4 Organización de los grupos de seguridad del dominio para eduroam

La organización de grupos propuesta es la siguiente:

- **Eduroam.PAS**: Grupo de usuarios pertenecientes al colectivo PAS.
- **Eduroam.PDI**: Grupo de usuarios pertenecientes al colectivo PDI.
- **Eduroam.Alumnos**: Grupo de usuarios pertenecientes al colectivo Alumnos.
- **Eduroam.bloqueados**: Grupo de usuarios locales (de cualquier colectivo) a los que se les deniega el acceso por algún incidente de seguridad pendiente de resolver.
- **Eduroam**: Eduroam.PAS + Eduroam.PDI + Eduroam.Alumnos + <Otros grupos>

5 Organización de VLANs

Los clientes de cada colectivo serán ubicados en una VLAN distinta, con un identificador numérico al que nos referiremos como <Nº VLAN colectivo>.

6 Configuración paso a paso del servidor RADIUS

Esta configuración se ha llevado a cabo sobre un servidor con Windows Server 2003 R2 Enterprise Edition.

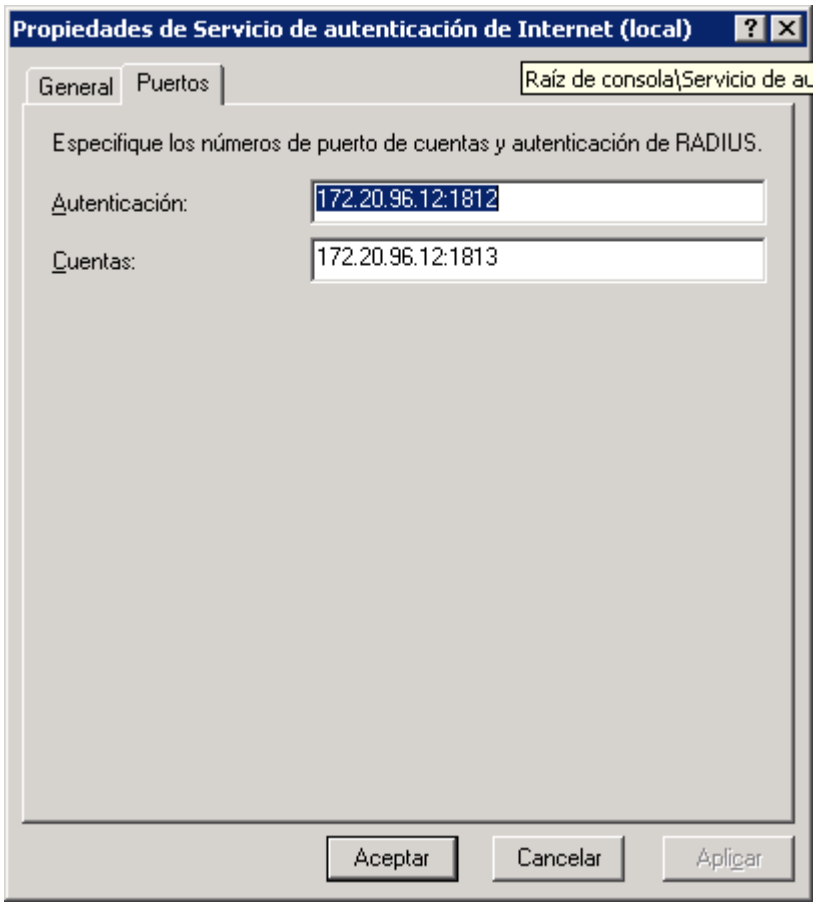
La configuración de los clientes RADIUS por rango de direcciones IP (independientemente del número) obliga a disponer de Windows 2000 o 2003 en versiones Enterprise.

6.1 Instalación del certificado del servidor RADIUS

Para que los suplicantes 802.1x puedan autenticar al servidor, es necesario instalar el certificado <**radius>.<organización>.<tld>** que luego será configurado en las opciones de protocolo EAP.

6.2 Configuración del servicio

- Seleccionar *Inicio -> Herramientas administrativas -> Servicio de autenticación de Internet -> Registrar servidor en Active Directory -> Aceptar.* Comprobar que pertenece al grupo de Servidores IAS de Active Directory.
- Seleccionar *Inicio -> Herramientas administrativas -> Servicio de autenticación de Internet -> Propiedades*. En la solapa *General* asegurarse de que se registran todos los eventos. En la solapa *Puertos* especificar los puertos 1812 para autenticación y 1813 para Cuentas. Si se trata de una máquina con varias direcciones IP, se debe indicar la dirección IP por la que se desea escuchar las peticiones RADIUS y por donde se envían las respuestas (pueden darse inconsistencias en caso de que no se indique).



6.3 Configuración de clientes RADIUS

Añadimos como clientes RADIUS toda la electrónica de red:

- Seleccionar Inicio -> Herramientas administrativas -> Servicio de autenticación de Internet -> clientes RADIUS -> Nuevo cliente RADIUS:
  - *Nombre descriptivo*: Electrónica de red
  - *Dirección del cliente*: <IP del cliente>. En las versiones Enterprise se puede indicar un rango dando una dirección IP en formato CIDR (<IP subred>/<nº bits de máscara>).
  - *Cliente proveedor*: RADIUS estándar
  - *Secreto compartido*: <secreto compartido RADIUS>
  - Desmarcar *La solicitud debe contener el atributo autenticador del mensaje*.

Ahora añadimos como clientes RADIUS los servidores RADIUS Nacionales de RedIRIS, lo que permitirá autenticar a usuarios en itinerancia:

- **radius.rediris.es**, con el secreto compartido indicado por RedIRIS.
- **radius2.rediris.es**, con el secreto compartido indicado por RedIRIS.

6.4 Registro de acceso remoto

Seleccionar *Inicio -> Herramientas administrativas -> Servicio de autenticación de Internet -> Registro de acceso remoto -> Archivo local -> Propiedades*:

- En la pestaña *Configuración*:

- *Registrar la siguiente información*: marcar todas.

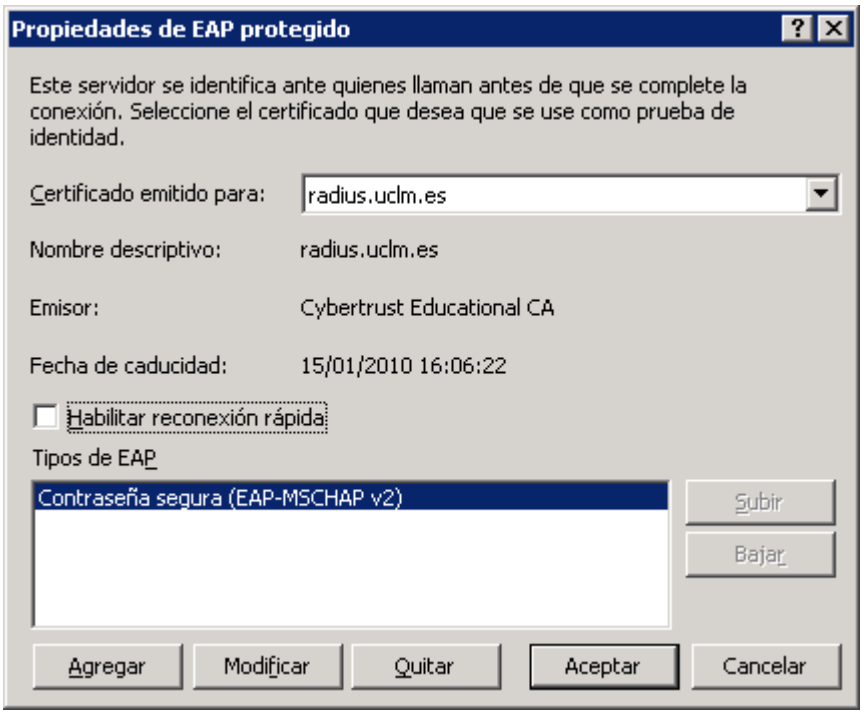
- En la pestaña *Archivo de registro*:
  - *Directorio*: <Directorio para ficheros de log>
  - *Formato*: Base de datos compatible (si se desea importar posteriormente a una base de datos relacional).
  - *Crear un Nuevo archivo de registro*: diariamente.
  - Desmarcar *Eliminar los registros más viejos cuando el disco esté lleno*.

6.5 Directivas de acceso remoto

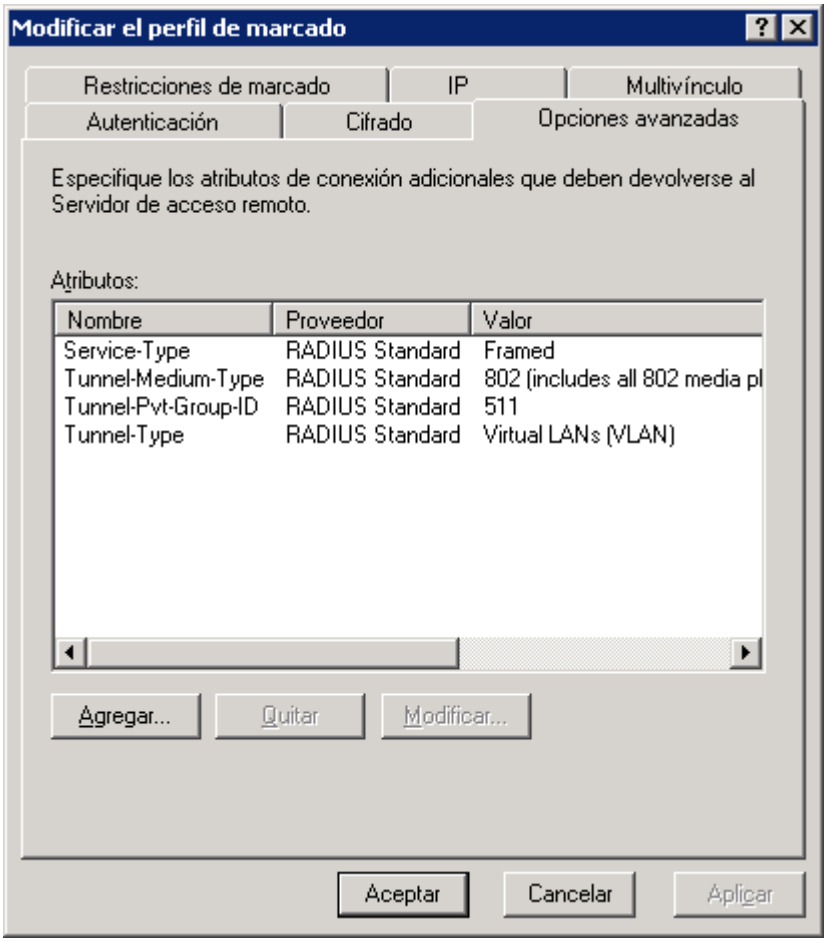
- Seleccionar *Inicio -> Herramientas administrativas -> Servicio de autenticación de Internet -> Directivas de acceso remoto*. Directivas (en este orden):

  - *Eduroam Usuarios <INSTITUCIÓN> en itinerancia*
    - "Nueva directiva de acceso remoto" -> "Utilizar el asistente" -> Nombre: "Eduroam Usuarios <INSTITUCIÓN> en itinerancia" -> Método de acceso: "Inalámbrico" -> Conceder permiso al grupo "<INSTITUCIÓN>\Usuarios.Eduroam" -> Tipo de EAP: PEAP -> Pulsar en configurar -> Seleccionar el certificado "<radius>.<organización>.<tld>". "Habilitar reconexión rápida" debe estar desmarcado y en tipos de EAP debe aparecer "Contraseña segura (EAP-MSCHAP v2)"
    - En las condiciones de la directiva de acceso remoto "Agregar…"->"Client-Friendly-Name coincide con ^radius.*\.rediris\.es$"
    - En las condiciones de la directiva de acceso remoto marcar la condición "NAS-Port-Type" y pulsar "Quitar". Esto garantiza que se cumplirán las condiciones de la directiva incluso cuando la organización visitada no envíe el valor de este atributo (lo habitual).
    - Asegurar que está directiva es procesada antes que el resto de directivas relacionadas con "Eduroam *".

  - *Eduroam Bloqueados*
    - "Nueva directiva de acceso remoto" -> "Utilizar el asistente" -> Nombre: "Eduroam Bloqueados" -> Método de acceso: "Inalámbrico" -> Conceder permiso al grupo "<INSTITUCIÓN>\Eduroam.Bloqueados". Editar y marcar "Denegar permiso de acceso remoto". La finalidad es bloquear el acceso a Eduroam de los usuarios con incidentes pendientes de resolver.
  - *Eduroam PDI*
    - "Nueva directiva de acceso remoto" -> "Utilizar el asistente" -> Nombre: "Eduroam PDI" -> Método de acceso: "Inalámbrico" -> Conceder permiso al grupo "<INSTITUCIÓN>\Eduroam.PDI" -> Tipo de EAP: PEAP -> Pulsar en configurar -> Seleccionar el certificado "<radius>.<organización>.<tld>". "Habilitar reconexión rápida" debe estar desmarcado y en tipos de EAP debe aparecer "Contraseña segura (EAP-MSCHAP v2)"



- Ir a la solapa “Opciones avanzadas” y añadir los siguientes atributos:
  - Tunnel-Medium-Type: 802 (Ethernet)
  - Tunnel-Type: VLANs
  - Tunnel-Pvt-Group-ID: <Identificador numérico de VLAN para el colectivo PDI>



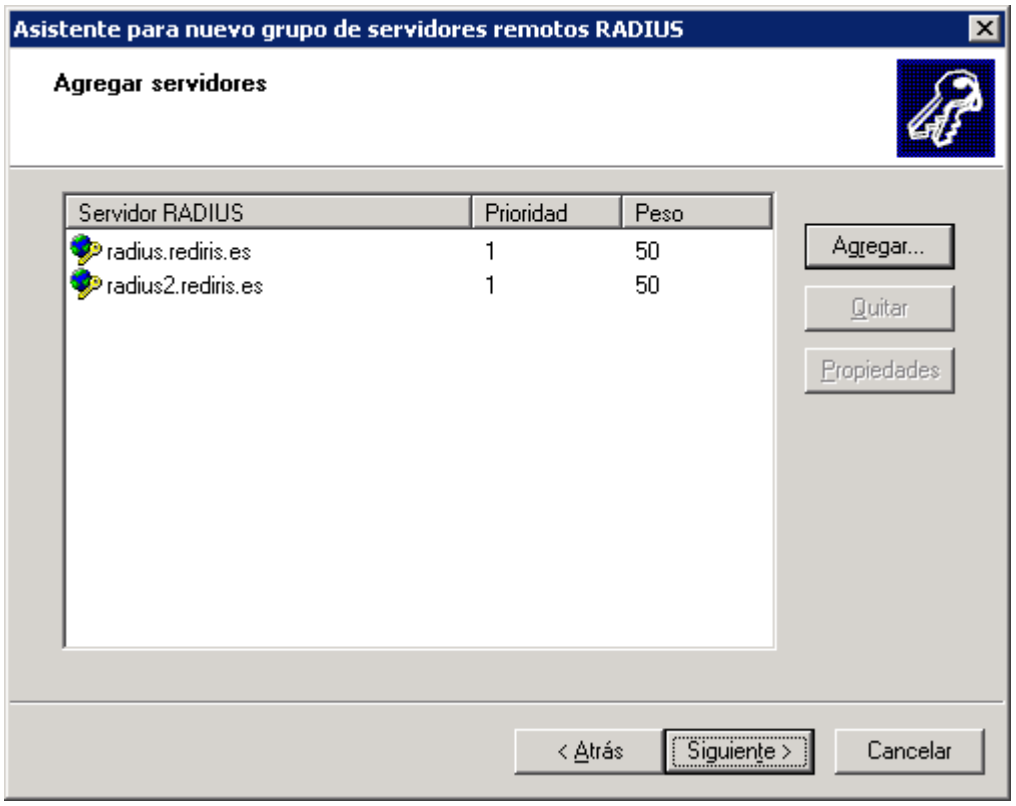
- Para “Eduroam PAS” utilizar:
  - Grupo de Seguridad: <INSTITUCIÓN>\Eduroam.PAS
  - Tunnel-Pvt-Group-ID: <Nº VLAN PAS>
- Para “Eduroam Alumnos” utilizar:
  - Grupo de Seguridad: <INSTITUCIÓN>\Eduroam.Alumnos
  - Tunnel-Pvt-Group-ID: <Nº VLAN Alumnos>
- Para “Eduroam Resto” utilizar:
  - Grupo de Seguridad: <INSTITUCIÓN>\Eduroam
  - Tunnel-Pvt-Group-ID: <Nº VLAN Invitados>

La finalidad de la directiva “Eduroam Usuarios <INSTITUCIÓN> en itinerancia” es conseguir que a las peticiones provenientes del exterior no se les asignen atributos (Tunnel-*). Existen dos motivos:

- La directriz a nivel nacional y europeo es que no se envíen este tipo de atributos fuera de la organización.
- Se ha comprobado empíricamente que impide el acceso a nuestros usuarios en algunas instituciones donde se usan VLANs dinámicas y donde no está prevista la reescritura de atributos.

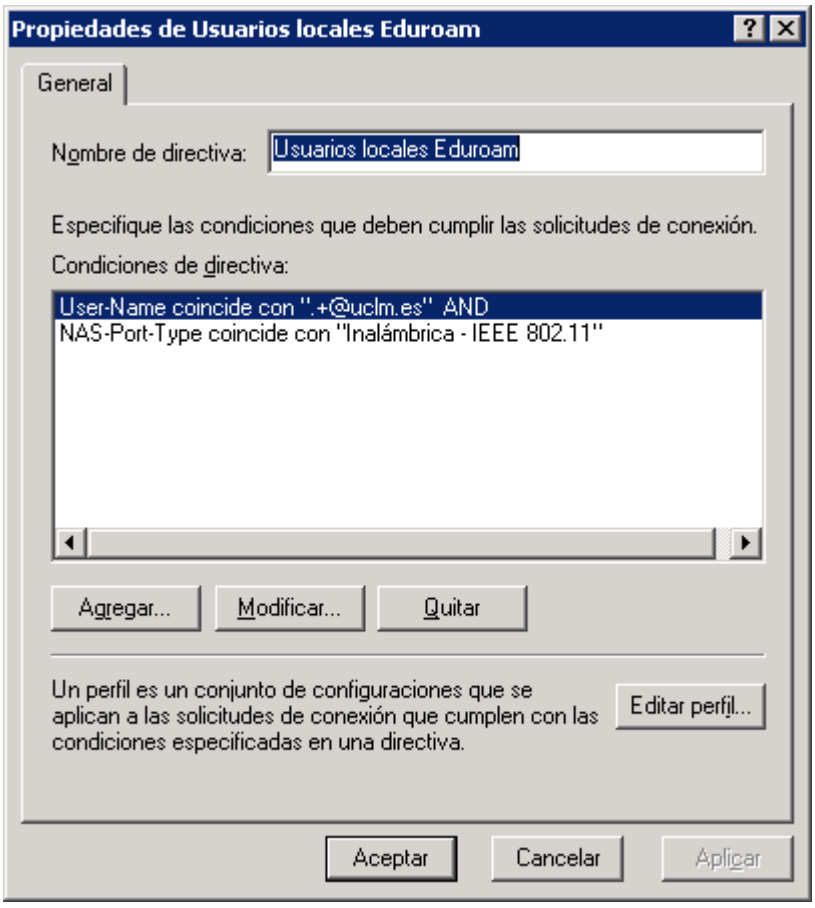
6.6 Procesamiento solicitud de conexión

- Seleccionar *Inicio -> Herramientas administrativas -> Servicio de autenticación de Internet -> Procesamiento solicitud de conexión -> Grupos de servidores remotos RADIUS -> Nuevo grupo de servidores remotos RADIUS -> Personalizada -> RADIUS Nacional Eduroam*.
- Añadir, introduciendo los secretos compartidos acordados con RedIRIS y dejando el resto de opciones con los valores por defecto:

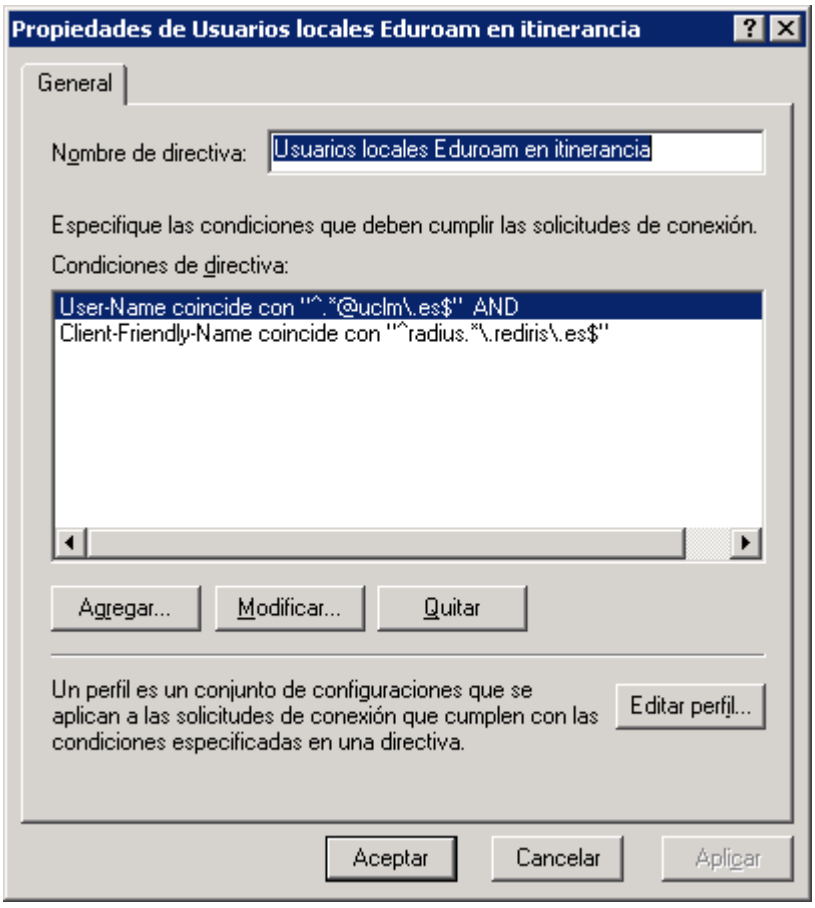


- Seleccionar *Inicio -> Herramientas administrativas -> Servicio de autenticación de Internet -> Procesamiento solicitud de conexión -> "Directivas de petición de conexión" -> "Nueva directiva de solicitud de conexión"*. Configuramos:

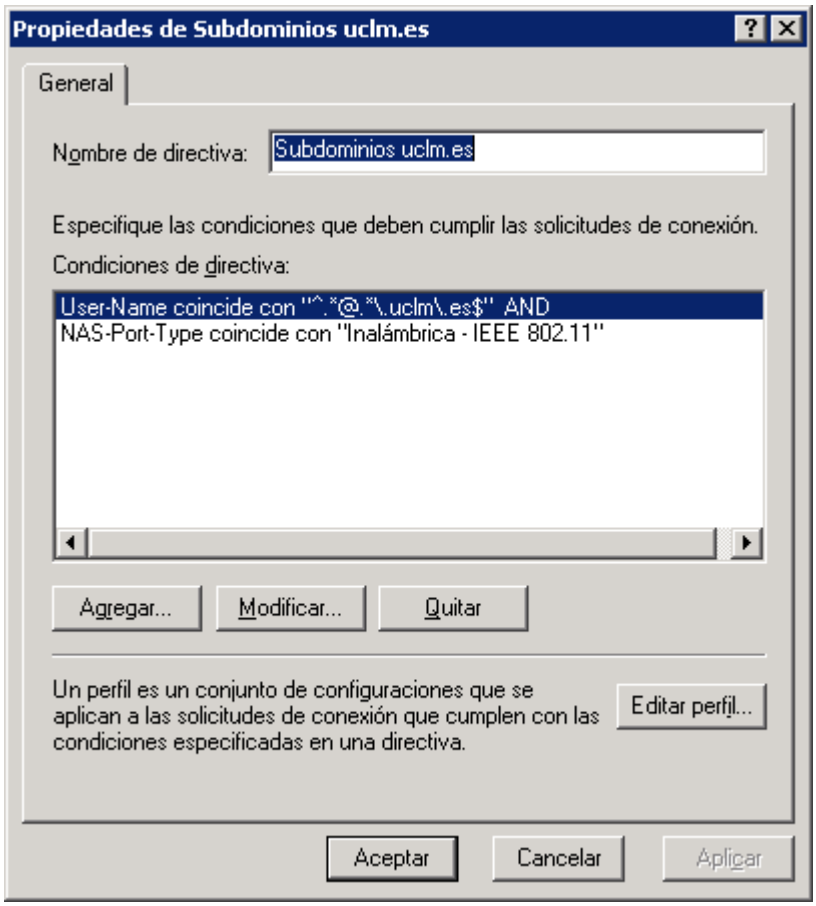
  - "Usuarios locales eduroam". Sólo es necesario editar las condiciones de directiva:
    - User-Name coincide con "^.+@<institución>\.<tld>$" y
    - NAS-Port-Type coincide con "Inalámbrica IEEE 802.11"



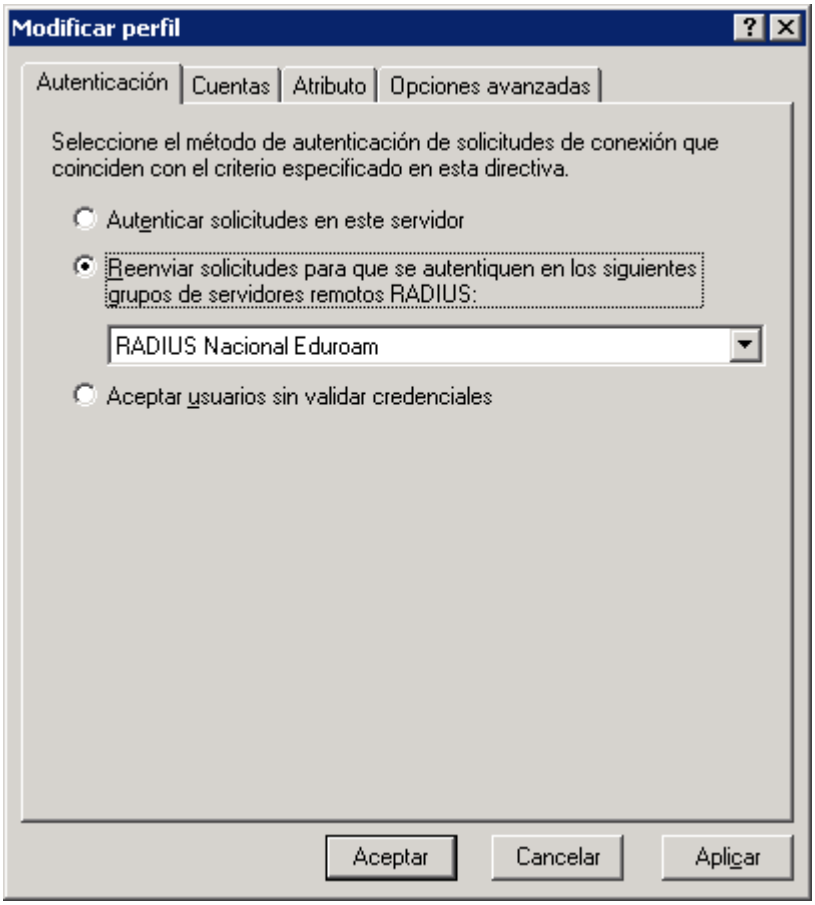
- "Usuarios locales Eduroam en itinerancia". Sólo es necesario editar las condiciones de directiva:
  - User-Name coincide con "^.+@<institución>\.<tld>$" y
  - Client-Friendly-Name coincide con "^radius\.rediris\.es$"



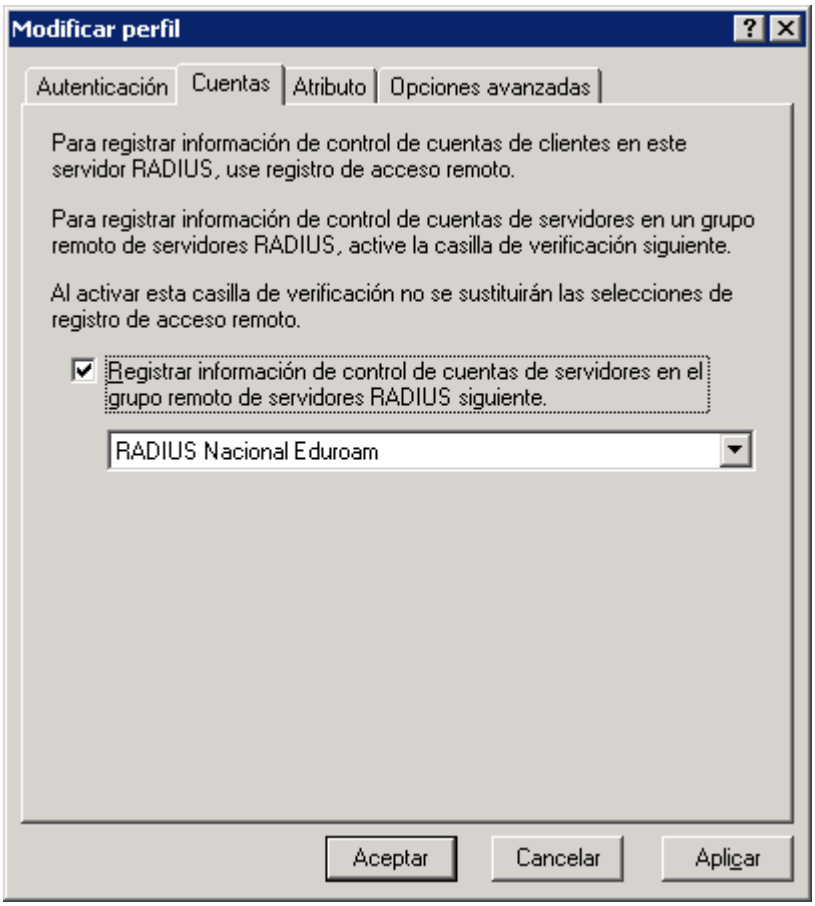
- "Subdominios <organización>". Se trata de procesar localmente las peticiones que se refieran a subdominios de la institución, incluso si son incorrectas. Mediante la expresión regular adecuada, esta directiva se podría fundir con "Usuarios locales eduroam". Sólo es necesario editar las condiciones de directiva:



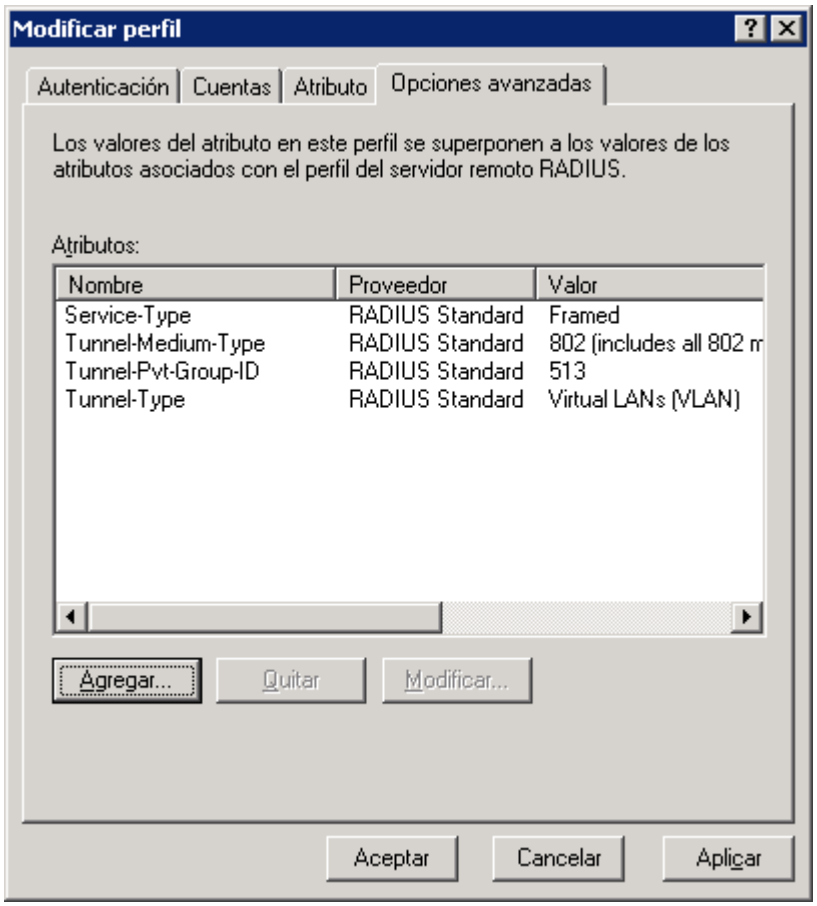
- "Usuarios externos Eduroam".
  - En las condiciones de directiva:
    - User-Name coincide con "^.*@.+$" (porque en algunos casos la identidad externa se suministra como sólo "@dominio") y
    - NAS-Port-Type coincide con "Inalámbrica IEEE 802.11"
  - En el perfil:
    - Autenticación. Reenviar a "RADIUS Nacional Eduroam"



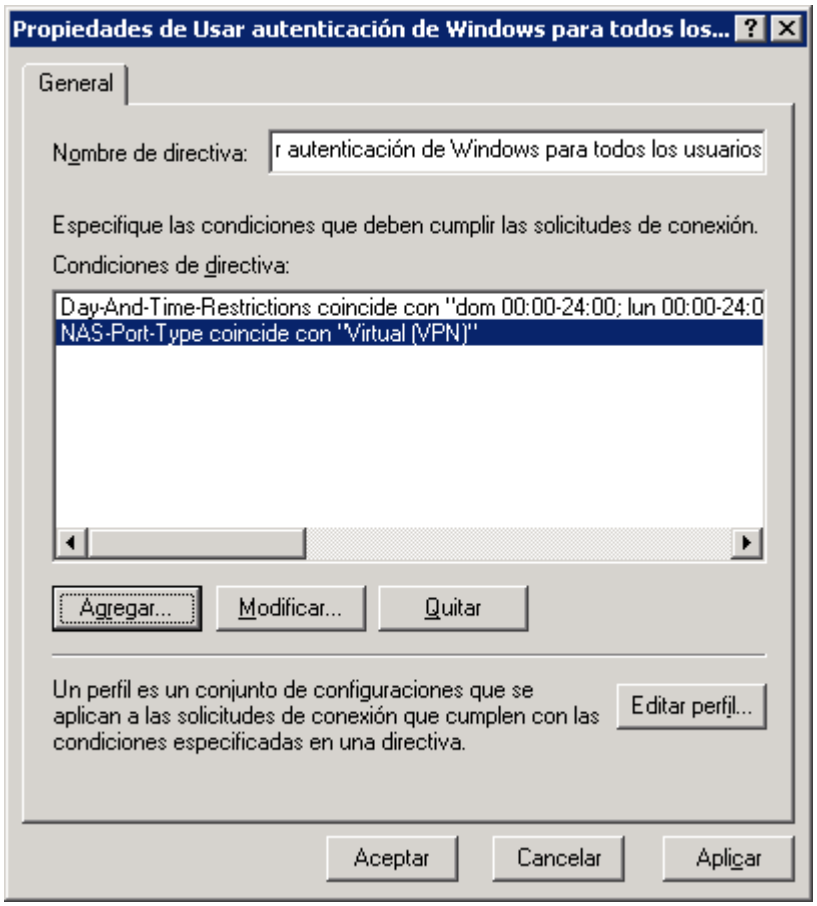
- Cuentas. Registrar información de cuentas en "RADIUS Nacional Eduroam".



- Atributo. No se modifica porque no se alterará ninguno de los atributos suministrado al servidor RADIUS Nacional.
- Opciones avanzadas. Se reescribirán los valores de los atributos asignados por el RADIUS origen para adaptarlos a la política de permisos locales:
  - Service-Type: Framed
  - Tunnel-Medium-Type: 802
  - Tunnel-Pvt-Group-ID: <Nº VLAN Invitados>
  - Tunnel-Type: VLAN



- Quitar la directiva “Usar autenticación de Windows para todos los usuarios”. Si el servidor RADIUS va a ser utilizado para otros tipos de acceso (por ejemplo VPN) entonces modificar la directiva “Usar autenticación de Windows para todos los usuarios”:
  - Agregar la condición “NAS-Port-Type coincide con Virtual (VPN)”.



De esta forma, aunque existan otros uso, se previene que las peticiones WIFI eduroam cuyas credenciales no se ajuste al patrón "usuario@subdominio.tld" pasen por esta última directiva. Se trata de una decisión de diseño para evitar configuraciones Wi-Fi que funcionen en local y no lo hagan en itinerancia.

- Reordenar las reglas para que se procesen en este orden:
  1. "Usuarios locales eduroam"
  2. "Subdominios <organización>"
  3. "Usuarios locales eduroam en itinerancia"
  4. "Usuarios externos eduroam"
  5. "Usar autenticación de Windows para todos los usuarios"

6.7 Configuración del usuario para pruebas del servicio RADIUS

RedIRIS suele utilizar el usuario radius-test@<institución>.<tld> para hacer las pruebas de disponibilidad del servicio.

En MS IAS es posible configurar una cuenta ficticia de la que el servidor no dejará rastro en los logs y que siempre devolverá fallo, que es lo que necesitamos. Pasos:

1. *Inicio -> Ejecutar -> regedit* -> En `HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\IAS\Parameters` añadir la entrada de registro `Ping User-Name` del tipo RG_SZ con valor radius-test@<institución>.<tld>

6.8 Configuración del los cortafuegos perimetrales

Si se han desplegado los servidores IAS en direccionamiento privado y/o protegidos por cortafuegos perimetrales, es necesario realizar cambios en los mismos para permitir el tráfico entrante desde los RADIUS de RedIRIS a los puertos UPD 1812 y UDP 1813.

6.9 Corrección del problema de MS IAS con el atributo Operator-Name

En Noviembre de 2010, JANET informó sobre un problema en MS IAS y NPS relacionado con la gestión del atributo Operator-Name. Este problema provoca que nuestros usuarios en itinerancia no accedan a eduroam en las instituciones visitadas que devuelven el atributo Operator-Name.

La guía Operator-Name RADIUS Attribute Issues with MS IAS and NPS describe tanto el problema como la solución para MS IAS y NPS.