Acceso seguro a redes inalámbricas: movilidad de usuarios en el CSIC

Juan Manuel Bolaño, Dolores de la Guía
Centro Técnico de Informática
Consejo Superior de Investigaciones Científicas
C/ Pinar 19 - 28006 Madrid

Abstract

En este trabajo se presenta la infraestructura de movilidad basada en redes inalámbricas instalada en centros del Consejo Superior de Investigaciones Científicas (CSIC) y que ha sido integrada dentro del proyecto internacional Eduroam. Esto permite a los usuarios de las instituciones adscritas a dicho proyecto realizar conexiones inalámbricas a Internet de forma segura cuando se encuentre en cualquiera de los centros participantes. Además, el usuario no necesita realizar ningún cambio en la configuración de su ordenador personal, tanto si está en su puesto de trabajo habitual como si se encuentra desplazado a otra institución participante en Eduroam.

Pálabras Clave
Redes inalámbricas, movilidad, acceso seguro, Eduroam, servidores Radius, protocolo IEEE 802.1x, SSID.

1 Introducción

En los últimos años hemos venido asistiendo a un notable incremento de la demanda de conexiones a la red mediante el uso de dispositivos inalámbricos en todos los centros del CSIC, al igual que ha ocurrido en el resto de organizaciones. Ya nadie adquiere un ordenador portátil sin una tarjeta de red inalámbrica integrada.

No sólo aumenta el número de usuarios que se conecta a este tipo de redes sino también sus exigencias por acceder a recursos, que hasta ahora sólo se alcanzaban a través de conexiones por cable. El usuario no quiere notar diferencia entre las prestaciones a las que está acostumbrado en un equipo fijo y otro con conexión inalámbrica [1] pero no es consciente de la disminución en la seguridad de transmisión de sus datos al pasar de un medio cableado a otro por ondas electromagnéticas.

Estos usuarios ya no conciben desplazarse (reuniones, congresos, estancias, etc.) sin su ordenador portátil y sin utilizar los servicios de sus centros de origen. Además, suelen ser una carga de trabajo añadida a los responsables de los servicios técnicos del centro que visitan.

Por tanto, a la hora de diseñar una infraestructura de red inalámbrica en los centros del CSIC, se ha tenido presente intentar dar soluciones a todos estos aspectos:

- Satisfacer el aumento de la demanda.
- Minimizar los problemas de seguridad.
- Facilitar a los usuarios la utilización de la red en sus desplazamientos.
- Intentar disminuir en lo posible la carga de trabajo a los administradores de los servicios de red.

2 Eduroam

Eduroam (Educational Roaming) [2] es un proyecto internacional cuyo objetivo es crear un único espacio WI-FI que posibilite el acceso inalámbrico a Internet de forma sencilla cuando se lleve a cabo un desplazamiento a otra institución asociada al proyecto.

En el caso particular de organismos de investigación españoles, la iniciativa está liderada por RedIRIS que se encarga de coordinar a nivel nacional todas la infraestructuras inalámbricas con el fin de conseguir un espacio único de movilidad a nivel nacional.

Este espacio único de movilidad está formado por un amplio grupo de organizaciones que en base a una política de uso y a una serie de requerimientos tecnológicos y funcionales permiten que sus usuarios puedan desplazarse entre ellas, disponiendo en todo momento de los servicios móviles que pueda necesitar.

El objetivo último sería que estos usuarios al llegar a otra organización dispusieran, de la manera más transparente posible, de un entorno de trabajo virtual con conexión a Internet, acceso a servicios y recursos de su organización origen, así como acceso a servicios y servicios de la organización que en ese momento les acoge.

Así, se proporciona cobertura inalámbrica mediante un mecanismo ágil y sencillo de movilidad y con técnicas seguras dentro de la comunidad académica en los países integrados en el proyecto. Actualmente, se encuentran englobados la mayoría de los países europeos y algunos países de la zona de Asia-Pacífico, como se pueden ver en los mapas representados en las figuras 1 y 2.

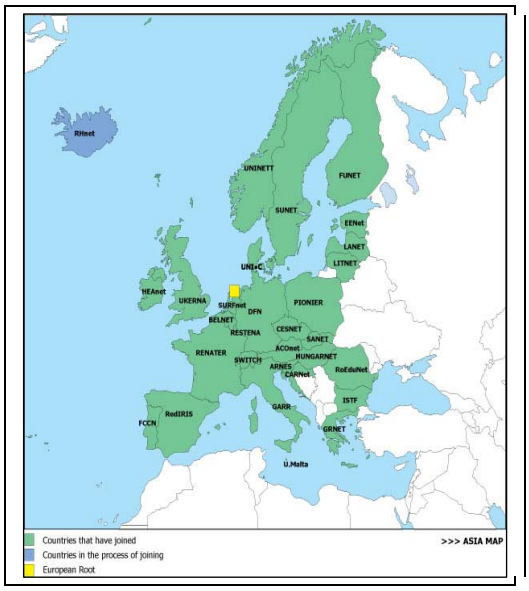

Figura 1. Despliegue de Eduroam en Europa(*)

Figura 2. Despliegue de Eduroam en el área Asia-Pacífico(*)

Eduroam impone las siguientes condiciones para poder sumarse a su proyecto:

- El servicio de movilidad común debe ser prestado únicamente a usuarios que pertenezcan a organizaciones afiliadas a redes de investigación adscritas al proyecto de espacio común de movilidad a nivel internacional.
- A todos los usuarios móviles se les requerirá autenticarse frente a su organización origen, con el fin de obtener servicios de acceso en la organización visitada.
- Todos los usuarios móviles son responsables de sus credenciales y deben respetar la política de uso aceptada por su organización origen.
- Las organizaciones visitadas deben ofertar servicios de acceso, y además, los usuarios móviles podrán reconocerlos y hacer uso de ellos.
- La organización visitada debe garantizar la transmisión segura de las credenciales de los usuarios móviles.
- La organización visitada tiene potestad de bloquear el acceso a cualquier usuario móvil, institución o red europea de investigación, si no cumpla con la política de uso de la organización visitada.
- Las organizaciones visitadas establecerán la autorización para el acceso a los servicios prestado a los usuarios móviles.
- La organización origen será responsable de dar soporte a sus usuarios, incluyendo formación en tecnologías de acceso y aceptación de políticas de uso.

En cada uno de los países partipantes hay una institución que coordina la integración de los organismos nacionales dentro de Eduroam. En el caso de España, RedIRIS es la encargada de gestionar la iniciativa Eduroam ES [3]. Los requisitos técnicos impuestos para participar en Eduroam ES son los siguientes:

1. Las organizaciones participantes deben responsabilizarse de formar a sus usuarios en el respeto a las políticas de uso de las organizaciones visitadas, y ayudar en cualquier aspecto relacionado con sus usuarios.
2. Las organizaciones participantes deben poseer un servidor de autenticación (NAS) que pueda, de un modo seguro, procesar y transmitir las credenciales de usuario solicitadas, utilizando para ello paquetes Access-Accept de RADIUS, en conformidad con la sección 3.16 de la RFC3580.
3. Las organizaciones participantes deberían disponer de mecanismos para informar a los usuarios visitantes de en qué medida y cómo ofertan sus servicios de movilidad.
4. Es obligatorio el uso del SSID (*Service Set Identifier*) "eduroam" excepto en aquellos casos en los que exista un solapamiento de puntos de acceso de distintas organizaciones físicamente muy cercanas. Para aquellos puntos de acceso en los que se de este solapamiento se recomienda el uso de SSIDs de la forma "eduroam-[INST]", donde [INST] son una sigla descriptiva de la institución a la que pertenece cada uno de los puntos de acceso en cuestión.
5. Las organizaciones participantes deberían disponer de mecanismos para informar a sus usuarios visitantes de los niveles de seguridad ofrecidos en la transmisión de credenciales.
6. Las organizaciones participantes deben informar a sus usuarios del servicio de movilidad, señalando que el soporte técnico recae sobre su organización origen. Sólo

cuando la organización origen determina que el problema es responsabilidad de la organización visitada, éste debe ser revisado con la organización visitada.

7. Las organizaciones participantes deben guardar información relativa a sesiones de autenticación y acceso a la red. Asimismo deben ser capaces de capaces de realizar un seguimiento de un usuario por razones de seguridad o gestión de capacidad. En concreto, deberán mantener la correlación de direcciones MAC y direcciones IP dadas a los visitantes mediante DHCP (*dinamic host configuration protocol*), junto con la hora, establecida a partir de una fuente fiable de tiempo, en la que se produjo la asignación. Las organizaciones participantes deben comunicar problemas de seguridad o uso fraudulento tanto a los responsables de la iniciativa eduroam ES, como a los responsables de seguridad de RedIRIS (IRIS-CERT), para solucionarlo de manera coordinada.
8. Las organizaciones participantes deben disponer de mecanismos de monitorización y seguimiento que permitan conocer el estado de los servidores de autenticación, para poder analizar problemas de conexión.
9. De acuerdo con la política establecida para el servicio a nivel europeo, sólo podrá usarse el SSID "eduroam" para mecanismos de control de acceso basados en el estándar IEEE 802.1x. Aquellas organizaciones que usen otros métodos (notablemente, los basados en redirecciones HTTP) cuentan para su adaptación con una moratoria que expiró **el 30 de septiembre de 2007**.

Numerosas instituciones académicas ya forman parte de Eduroam ES. En el mapa de la figura 3 aparecen las ciudades donde están ubicadas dichas instituciones.

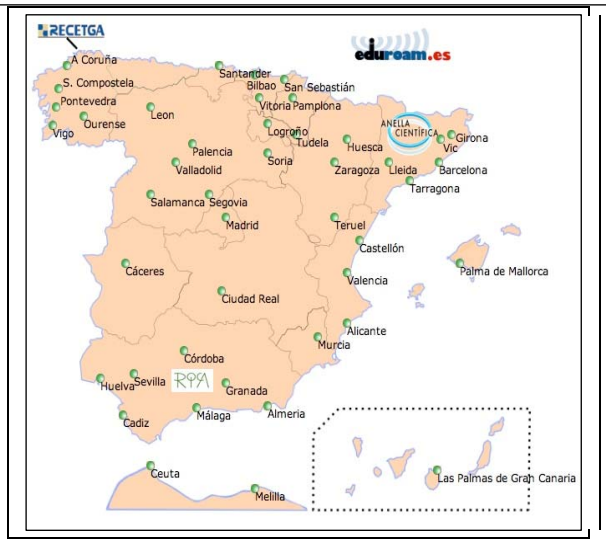

Figura 3: Despliegue de Eduroam ES (**)

3 Red inalámbrica en el CSIC

3.1 Objetivo y alcance

El CSIC abordó a mediados de 2006 la puesta en marcha del un proyecto para la dotación de cobertura WI-FI a la totalidad de edificios que conforman la red del campus de Serrano de

Madrid. El despliegue ha continuado a lo largo del año 2007 a otros centros de Madrid, Cataluña y Murcia. En breve se va a implantar en centros de Valencia y para el año 2008 se pretende desplegar la solución en el resto de los centros ubicados en el territorio nacional.

Los puntos fundamentales a la hora de diseñar la solución WI-FI han sido la seguridad, la movilidad y la facilidad de gestión.

Seguridad. En los últimos años se ha asistido a un gran despliegue de redes inalámbricas y numerosos foros de seguridad se han encargado de poner manifiesto su vulnerabilidad y la facilidad de sufrir ataques no deseados en estas redes. Por ese motivo, los fabricantes han convertido la seguridad es un elemento primordial a tener en cuenta en el diseño de los equipos. Estos nuevos dispositivos, incorporan elementos de seguridad que permiten la restricción a determinados recursos no críticos para evitar que personas no autorizadas puedan entrar en ellos. Otro elemento importante en el tema de la seguridad en redes inalámbricas son los puntos de acceso inalámbricos "piratas" que puedan instalar personas no autorizadas en el entorno sin ningún tipo de medidas de seguridad y que pasan a convertirse en puertas traseras abiertas sin control a la red del CSIC.

Gestión. Hasta hace algún tiempo, las tareas de administración y gestión representaban un gran esfuerzo y carga de trabajo. Las tecnologías empleadas permiten la gestión centralizada de todos los elementos por lo que un cambio de configuración o una ampliación del número de puntos no tiene que verse como un gran esfuerzo ni un gran aumento del trabajo habitual.

Movilidad de los usuarios. En el entorno académico, se están desarrollando algunos proyectos que facilitan a los usuarios el acceso móvil a servicios, tanto desde el punto de vista de la telefonía, como desde el punto de vista de acceso a servicios telemáticos que necesiten de una conexión inalámbrica a una red. Por su relación con RedIRIS y toda la comunidad académica, el Centro Técnico de Informática del CSIC participa en la iniciativa Eduroam.

En resumen, el CSIC está dotando a sus centros de una solución de red inalámbrica basada en dispositivos que garanticen, por un lado, conexiones seguras a los usuarios con independencia de su ubicación y, por otro lado, faciliten a los administradores la configuración, la gestión y el mantenimiento de la infraestructura asociada.

3.2 Configuración de la red WI-FI en el CSIC

La tecnología inalámbrica más adecuada para el acceso a redes de voz y datos simultáneos es la que sigue la norma 802.11 a/b/g/n en WI-FI y ha sido, por tanto la elegida. Esta tecnología debe ser potenciada con técnicas adicionales que aseguren la calidad de servicio, seguridad y gestión centralizada. Por ejemplo, deben ofrecer la posibilidad de configurar múltiples políticas para asegurar la privacidad y autenticidad de acceso.

La solución implantada ha contemplado todos estos aspectos y se ha optado por una solución comercial basada en punto de acceso (*access points*, AP) "ligeros" donde la inteligencia está en un único concentrador WI-FI central con el valor añadido de ser una plataforma segura, escalable (hasta 512 APs por concentrador) y de fácil administración, además, de realizar una gestión inteligente del espectro de radiofrecuencia. La cobertura inalámbrica es del 100% en el interior de los edificios.

Se contempla la creación de múltiples SSID que permiten realizar el control seguro de usuarios basado en identidades, a través del cortafuegos incorporado en la plataforma. Esta posibilidad permite asignar distintas políticas de acceso dependiendo del rol del usuario y conducirle a una determinada red virtual (VLAN).

La plataforma también dispone de herramientas de detección y prevención de intrusiones para evitar ataques a nivel de radiofrecuencia. Esto facilita la localización de AP cercanos no pertenecientes a la red del CSIC e impide que sean operativos aquellos de uso fraudulento (*rogue AP*). Por ejemplo, un AP que haya instalado un usuario sin consentimiento para hacerlo.

En el aspecto de la seguridad, están incluidos diferentes métodos de cifrado como WPA y WPA2.0. Como método de autenticación se utiliza el estándar IEEE 802.1x. En este protocolo entran en escena tres elementos básicos:

- Suplicante: cliente inalámbrico que solicita la conexión a la red
- Autenticador: elemento de nivel 2 que proporciona la conexión de red
- Servidor de autenticación: dispositivo que verifica la autenticidad del suplicante

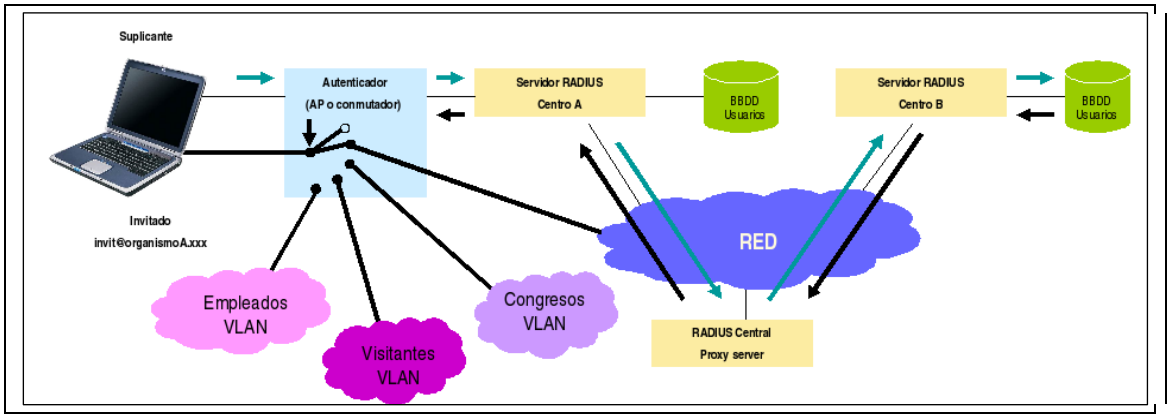

Figura 4: Esquema de funcionamiento del protocolo de autenticación IEEE 802.1x

En la figura 4 se pueden ver los elementos mencionados y el funcionamiento del protocolo IEEE 802.1x. El servidor de autenticación estaría compuesto por un servidor Radius y el directorio corporativo o base de datos de usuarios. La iniciativa Eduroam permite la integración de una jerarquía de servidores Radius que facilita la movilidad de los usuarios. IEEE 802.1x engloba a otros protocolos como EAP (*Extensible Authentication Protocol*) sobre el que están definidos otros tipos: TLS, TTLS, PEAP, GTC, etc. En el CSIC se ha optado por EAP-TTLS por ser un protocolo más estándar y del que existe una implantación gratuita (SecureW2), de acuerdo con la política de Eduroam.

Se han incorporado herramientas de monitorización y gestión que permiten conocer en todo momento el estado de la infraestructura inalámbrica así como realizar un seguimiento del uso de los recursos (número de usuarios conectados en cada SSID o en cada AP, trazabilidad de las conexiones de los usuarios, etc). Estas estadísticas facilitan la comprobación del correcto dimensionamiento de la red inalámbrica.

4 Conclusiones y proyectos futuros

En este trabajo se ha descrito el diseño de la red inalámbrica en el CSIC. Su implantación se inició en el año 2006, con un primera fase que incluía a los centros ubicados en el Campus de Serrano del CSIC en Madrid más el Centro de Ciencias Humanas y Sociales. En total, fueron

incluidos veinte edificios, que necesitaron 315 AP para dar la cobertura necesaria y dos concentradores WI-FI.

A lo largo del año 2007 se ha abordado una segunda fase que incluía a veinte centros situados en Madrid, Barcelona y Murcia, con un total de 665 AP y veinte concentradores WI-FI. A finales de 2007 se va a iniciar una tercera fase que incluye a seis centros en Madrid, Gerona y Valencia y se tiene previsto extender esta red al resto de centros durante el año 2008. En total, se calculan tener instalados unos 2000 AP.

A tenor de los resultados obtenidos hasta la fecha, el proyecto puede considerarse como satisfactorio y se manifiesta un uso creciente de esta infraestructura. Hasta ahora, no se ha tenido constancia de incidentes de seguridad. Por estos motivos, se considera un acierto la elección de la solución.

En un futuro, se estudiará dar cabida a otros servicios sobre esta infraestructura como son telefonía IP WI-FI (ToIP WI-FI) y servicios de localización de personas o de objetos. También se está pensando dar cobertura a exteriores a través de soluciones malladas.

Aunque el diseño presentado está incluido dentro del marco de instituciones académicas, es perfectamente extrapolable a cualquier otro entorno que pretenda ofrecer un servicio de movilidad a sus usuarios con acceso seguro a los recursos telemáticos del organismo.

5 Bibliografía

[1] Potter, B. and others, 802.11 Security, O'Reilly & Associates, Inc., Dec. 2002

[2] http://www.eduroam.org

[3] http://www.eduroam.es

(*) Las figuras 1 y 2 se han obtenido de las páginas web de Eduroam

(**) La figura 3 se ha obtenido de las páginas web de Eduroam ES