Education Roaming
Movilidad segura para la comunidad académica

Módulo 1: Conceptos básicos

¿Qué es eduroam?

eduroam (education roaming) es el servicio mundial de movilidad desarrollado para la comunidad de educación e investigación, permitiendo que los estudiantes, investigadores y académicos obtengan conectividad Internet a través de su campus y cuando visiten otras instituciones participantes con solo abrir su portátil.

¿Cómo trabaja eduroam?

Proceso de autenticación y autorización en eduroam:

1. El dispositivo móvil de pepe se une a SSID eduroam
2. El cliente sobre el dispositivo móvil de Pepe envía una solicitud de conexión a la red eduroam de INICTEL como pepe@uni.edu
3. El servidor local RADIUS de INICTEL (que está conectado a la infraestructura inalámbrica de INICTEL) reconoce que el dominio de pepe (@uni.edu) no es local, por lo que reenvía la solicitud al servidor RADIUS nacional.
4. El servidor RADIUS nacional envía la solicitud al destino apropiado, dominio uni.edu
5. El servidor RADIUS de UNI, envía un certificado de desafío (*certificate challenge*) de regreso a pepe. Este es el paso que permitirá a pepe estar seguro que el SSID eduroam de INICTEL es un miembro de confianza de la red de eduroam.
6. Si el certificado fue cargado previamente en el dispositivo de pepe (un importante paso en el proceso de eduroam), el dispositivo aceptará el certificado y establece un túnel encriptado SSL/TLS entre el dispositivo de Pepe y el servidor RADIUS *home* (origen) de la institución de Pepe.
   Si el dispositivo móvil de Pepe no reconoce el certificado, a Pepe se le pedirá que acepte o rechace el certificado. En todos los casos, el certificado mostrará el nombre común (por ejemplo: eduroam-radius.uni.edu). Pepe no debería aceptar un Certificado con un nombre desconocido (por ejemplo: verdad.com).

7. Ahora que se ha establecido el túnel encriptado entre el dispositivo de Pepe y el servidor RADIUS de UNI, las credenciales de Pepe son pasadas a través del túnel encriptado SSL/TLS entre el dispositivo de Pepe y el servidor RADIUS de UNI para la verificación. Este paso de autenticación permite al servidor RADIUS ser conectado al Servicio de Directorio de la institución.
8. Sobre la autenticación exitosa, el servidor RADIUS de UNI envía un *Access-accept* y algún material clave a la infraestructura de INICTEL (fuera del túnel SSL) y algún material clave privado a pepe (dentro del túnel).
9. La infraestructura inalámbrica eduroam de INICTEL negocia con el dispositivo de pepe el intercambio de la clave de encriptación para permitir el acceso a la red y habilitar la encriptación entre el dispositivo de pepe y los puntos de acceso inalámbrico de INICTEL.
10. Pepe ahora puede conectarse a SSID eduroam en INICTEL y disfrutar de la conectividad autenticada y encriptada entre su dispositivo y la red inalámbrica de INICTEL.

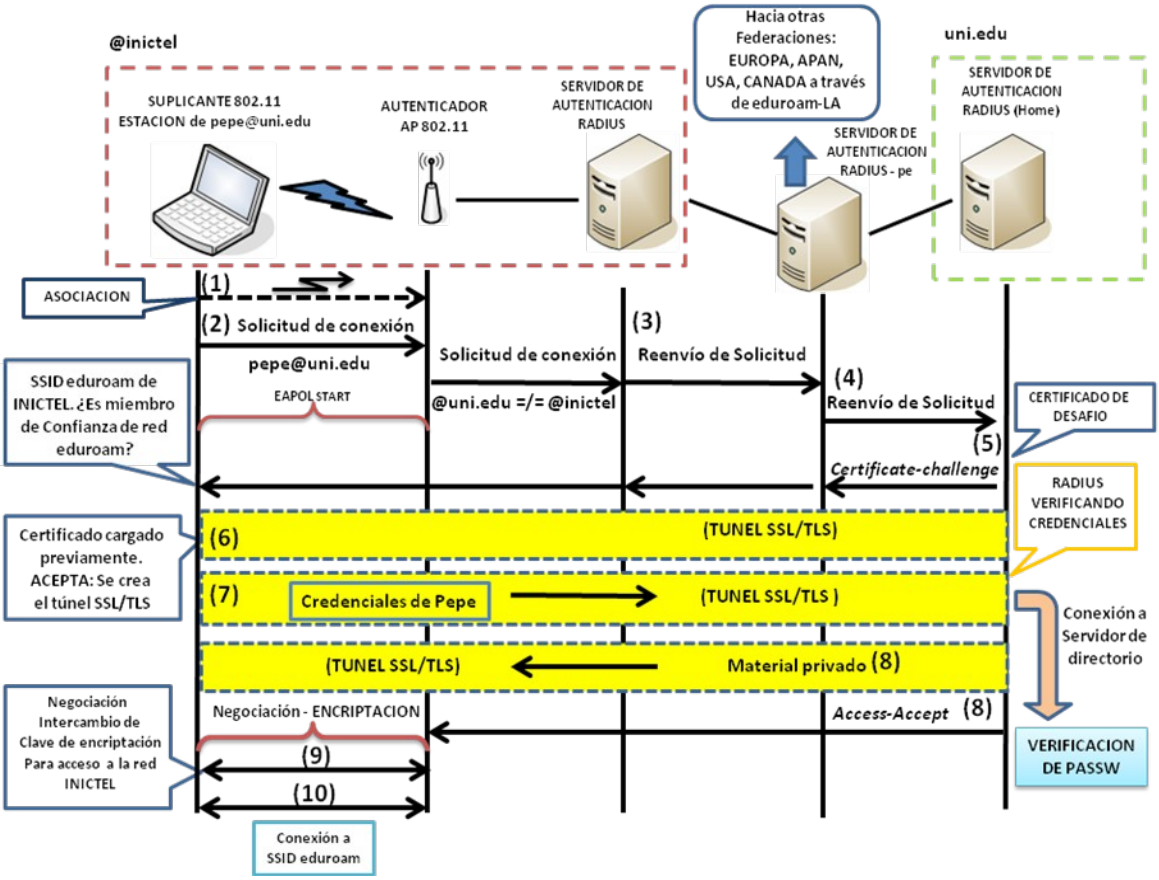

Fig 1. Proceso de autenticación y autorización en eduroam

Infraestructura de eduroam

Definiciones y conceptos generales *(Fuente: **Deliverable DJ5.1.5,3: Inter-NREN Roaming Infrastructure and Service Support Cookbook – Third Edition)***

Suplicante

Es un software (a veces es parte del sistema operativo o como un programa separado) que usa el protocolo IEEE 802.1X para enviar la información de solicitud de autenticación usando EAP. Los suplicantes son instalados y operan en dispositivos de cómputo de usuarios finales (Notebooks, PDA, teléfonos celulares con Wi-Fi habilitado, entre otros).

Access Point (autenticador)

Son dispositivos de acceso LAN inalámbrico conforme al estándar IEEE 802.11 y necesitan tener la capacidad IEEE 802.1X. Deben tener la capacidad de reenviar las solicitudes de acceso desde un suplicante al servidor RADIUS del Proveedor de Servicio (red visitada), para dar acceso a red luego de una correcta autenticación, permitiendo la asignación de usuarios a una VLAN específica basada en la información recibida desde el servidor RADIUS. Además los access point intercambian material clave (vectores de inicialización, claves públicas y sesiones, etc.) con sistemas de clientes para impedir sesiones hijacking.

Switches

Necesitan ser capaces de reenviar las solicitudes de acceso que viene de un suplicante al servidor RADIUS del Proveedor de Servicio, para permitir el acceso a red tras una apropiada autenticación y posiblemente asignar usuarios a VLANs específicas basadas en la información recibida del servidor RADIUS.

Estándar IEEE 802.1X

Fuente 1: Traducción de "Mobility Task Force. Deliverable D: Inventory of 802.1X-based solutions for inter-NRENs roaming. Version 1.2"
Authors: Erik Dobbelsteijn erik.dobbelsteijn@surfnet.nl
Contributions: Klaas Wierenga (SURFnet bv) klaas.wierenga@surfnet.nl, Paul Dekkers (SURFnet bv) paul.dekkers@surfnet.nl, Henny Bekker (SURFnet bv) henny.bekker@surfnet.nl, James Sankar (UKERNA) j.sankar@ukerna.ac.uk, Tim Chown (University of Southampton) tjc@ecs.soton.ac.uk, Sami Keski-Kasari Tampere (University of Technology, Finland) samikk@cs.tut.fi
Fuente 2: http://www.eduroam.edu.au/tech/install/radius

Una red habilitada con el estándar IEEE 802.1x, permite el acceso a red solo a usuarios autorizados, esto se logra cuando se tiene creado previamente la cuanta del usuario. EL sistema operativo debe soportar IEEE 802.1x.
La ventaja para el usuario es que puede desplazarse libremente de una red a otra. Las redes pueden ser fijas o inalámbricas. En el caso de redes inalámbricas esto es importante, ya que no depende el estar físicamente conectado a un *switch* para conseguir conectividad como sucede en redes fijas.

El principio de funcionamiento de IEEE 802.1x se centra en que los *switchs* y a*ccess point* que realizan la autenticación IEEE 802.1x sólo permitirán el tráfico 802.1x cuando los usuarios se conecten a estos dispositivos. Una vez que los usuarios han sido autenticados y autorizados se permitirá cursar su tráfico a través de ellos.

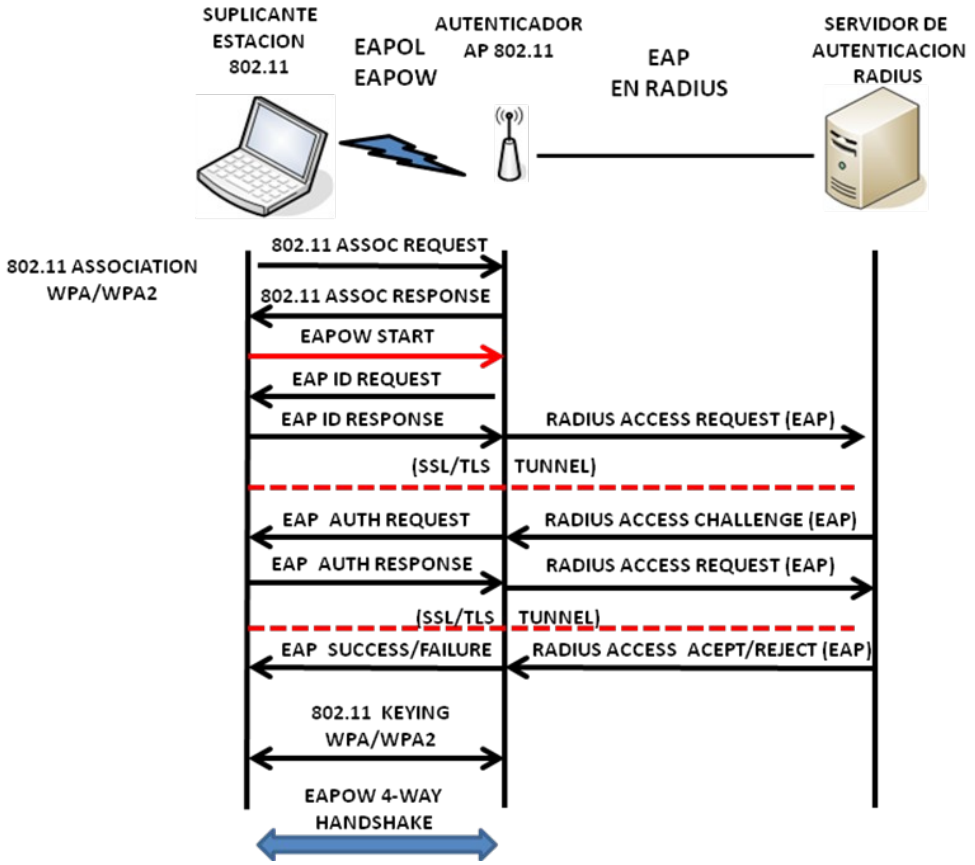

Fig 2: Secuencia de operación de IEEE802.1x - Autenticación EAP

Para el caso de redes alambradas Ethernet se habilitará el puerto del *switch* para el usuario autenticado, y en redes inalámbricas será el *acccess point* quien negociará una clave única con la interfaz inalámbrica del usuario autenticado. La clave negociada durante la autenticación 802.1x es dinámica, además de ser única para cada usuario y también cambiante.
La clave única se usa para encriptar el tráfico entre el usuario y el *Access point*.

La autorización en IEEE 802.1x se realiza a través del Protocolo de Autenticación Extensible (*EAP - Extensible Authentication Protocol*), que permite que las solicitudes de clientes sea reenviado al servidor de autenticación, bajo el uso de diversos métodos de autenticación. Las operaciones de IEEE 802.1x se muestran en la Fig 2.

Arquitectura

Las tramas 802.1X añaden funcionalidad a los componentes existentes en una red. Por lo tanto, no son necesarios componentes adicionales.
En una red fija, el terminal (PC o portátil, por ejemplo) tiene que tener una tarjeta de red (NIC), y el sistema operativo debe tener una funcionalidad que se le denomina suplicante 802.1X en la tarjeta, este es el cliente.
El puerto al que se conectará la terminal se encuentra en un switch que tiene activado 802.1X. Al switch se le denomina el autenticador.

Sobre la base de comandos 802.1X, el switch puede abrir y cerrar una conexión en el puerto. El tercer componente de la arquitectura es el servidor de autenticación. En general, un switch preguntará a un servidor RADIUS para verificar si el usuario está permitido a usar el puerto, y a que VLAN debe ir el tráfico.
Cuando 802.1X se aplica a una red inalámbrica, un dispositivo de control de acceso inalámbrico sustituye al switch como el autenticador. No es relevante qué protocolo de transporte inalámbrico (802.11b ó protocolos como el 802.11g) se utiliza. La Fig 3 muestra la infraestructura de autenticación.

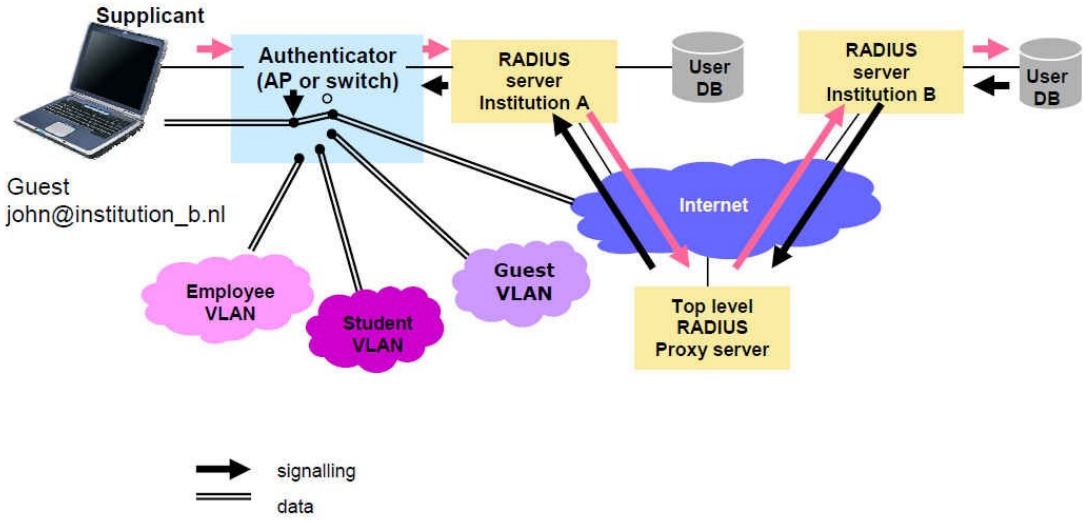

Fig. 3 Infraestructura de autenticación para autenticación entre dominios usando 802.1x (Fuente 1: "Mobility Task Force. Deliverable D: Inventory of 802.1X-based solutions for inter-NRENs roaming. Version 1.2")

Cuando un usuario se conecta a la red suministra sus credenciales al autenticador (el dispositivo de control de acceso) que verifica esto usando el RADIUS *backend*. Las credenciales deberían siempre incluir un nombre de usuario y un dominio que se traduce en una credencial que se parece a una dirección e-mail (user@dominio.topleveldomain).

Si un usuario visitante utiliza la red, el servidor RADIUS local se dará cuenta de que el dominio del usuario no es el dominio del cual se sirve. Ahí es donde el mecanismo de RADIUS proxy entra y asegura de que las credenciales EAP encapsuladas sean transportadas hacia el *home* RADIUS server.

De hecho, el servidor RADIUS sólo tiene que remitir la petición a un servidor RADIUS de alto nivel (higher-level RADIUS proxy server). Este servidor proxy conoce a todos los servidores RADIUS en la constelación de *roaming* y reenvía la solicitud al servidor que se sabe puede mantener este dominio.

El *home* RADIUS server, se instala en la red de origen (home network) del visitante, ya sea en el mismo país o en el extranjero, donde el usuario se autentica contra una base de datos de usuario local.
El servidor RADIUS local sólo tiene que saber a qué proxy deben ser enviadas las peticiones de usuario desconocido. Cuando una nueva red ingresa su acuerdo de *roaming*, solamente el proxy tiene que ser actualizado.

Respecto a la pila de protocolos del formato IEEE 802.1X (Fig 4), la información de autenticación se realiza sobre el protocolo de autenticación extensible (EAP, RFC 2284), un protocolo que permite el uso de cualquier método de autenticación, como nombre de usuario/contraseña, certificados, OTP (*One Time Password*, por ejemplo a través de SMS) o credenciales SIM-card de operadores móviles. Estos mecanismos se aplican en los tipos de EAP: MD5, TLS, TTLS, MS-CHAPv2, PEAP, Mob@c, y EAP-SIM.

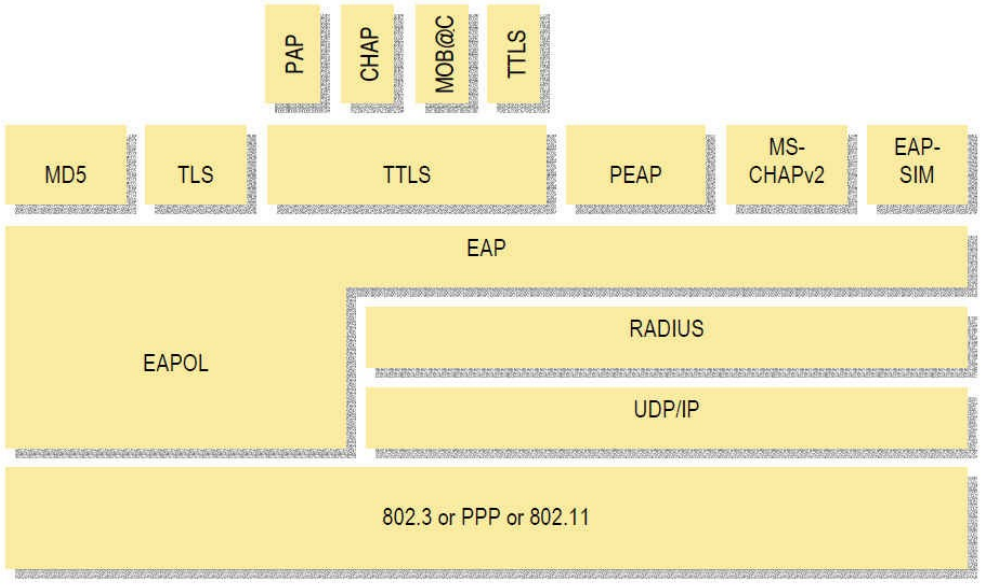

Fig. 4 EAP puede soportar varias formas de mecanismos de autenticación. (Fuente 1: **"Mobility Task Force. Deliverable D: Inventory of 802.1X-based solutions for inter-NRENs roaming. Version 1.2")**

Tanto el solicitante y el home RADIUS server deberían utilizar el mismo tipo de EAP. El dispositivo de control de acceso, switch o servidores proxy RADIUS no tienen que ser conscientes del tipo de EAP.

En la actualidad, TLS (Transport Layer Security), TTLS (Túnel Transport Layer Security) y PEAP (EAP protegido) son los candidatos más serios para su aplicación inmediata. Pruebas adicionales se realizaron con la autenticación basada en el envío de contraseñas a través de SMS.

TLS, TTLS y PEAP configuraran una conexión TLS entre el cliente y el dispositivo de control de acceso basado en un certificado de servidor RADIUS. Este mecanismo de autenticación mutua puede impedir ataques *Man in the Middle*. Entonces TLS usa un certificado de cliente para autenticar al usuario, mientras que TTLS es generalmente utilizado para el transporte de nombre de usuario/ contraseña. Dado que tanto TTLS y PEAP son protocolos de túnel, cualquier otro protocolo puede ser utilizado sobre ellos. MOBAC es un ejemplo de esto, implementando *One Time Password* a través de SMS.

Si el usuario está verificado apropiadamente contra el proceso final de autenticación de origen (*home authentication backend*), que puede ser LDAP, por ejemplo, él será autenticado y el *home* RADIUS server pasa un acuse de recibo al dispositivo de control de acceso. Cuando un usuario se encuentra en su red de origen (home network), el servidor RADIUS puede decir al autenticador en cual tráfico de VLAN de usuario debe residir. Entonces, el dispositivo de control de acceso pasa el tráfico de usuario en esta VLAN hasta la de-autenticación. La conmutación VLAN se basa en el estándar 802.1Q. Un visitante ingresará en una VLAN-huésped determinada por el servidor RADIUS de la red visitada.

En esta etapa del proceso, la conectividad Ethernet se proporciona, después del cual los mecanismos habituales para la obtención de conectividad IP pueden desempeñar su papel, como ofrecer al cliente una dirección IP a través de DHCP. De hecho, cualquier cosa es posible en la capa 3, después del proceso de autenticación: no sólo el protocolo IP, cualquier otro protocolo de capa 3 puede ser transportado (IPv6, IPSec, IPX, PPPoE etc.) y cualquier mecanismo de la capa 3 (VPN, Multicast, etc NAT) encuentra una capa dos transparente, capa de transporte.

Cuando el usuario retira el cable o sale del área de cobertura de un dispositivo de control de acceso inalámbrico, el dispositivo de control de acceso detecta la interrupción de la conexión y el puerto será cerrado. Cada vez más Suplicantes también tienen incorporado la posibilidad de desconectarse de una red, y que les permite volver a conectarse con credenciales diferentes para acceder a otras VLAN.

Escalabilidad

Como se mencionó antes, el servidor RADIUS local sólo tiene que saber a qué proxy deben ser enviadas las solicitudes de usuario desconocido.

Cuando una nueva red entra en este acuerdo de *roaming*, sólo el proxy tiene que ser actualizado.

Para ampliar o extender esta infraestructura de *roaming* a una escala Europea, un proxy RADIUS sobre un nivel internacional es el único componente que debe ser agregado, como se aprecia en la Fig. 5 Arquitectura de roaming internacional.

Cuando una nueva institución ingresa a la constelación, sólo su dominio tiene que ser ingresado al servidor Proxy RADIUS, no en los servidores de otras instituciones. Lo mismo ocurre cuando se agrega un grupo de instituciones en un país que ingresa en la constelación: el nivel superior de servidor Proxy RADIUS (Top Level) debe ser actualizado con el nuevo dominio de alto nivel (high-level), por ejemplo “. nl”, tras lo cual el mecanismo de reenvío trabaja por cada institución en la constelación.

Siempre es posible realizar relaciones bilaterales entre los servidores que intercambian mucho tráfico, o tráfico que sólo es localmente relevante.

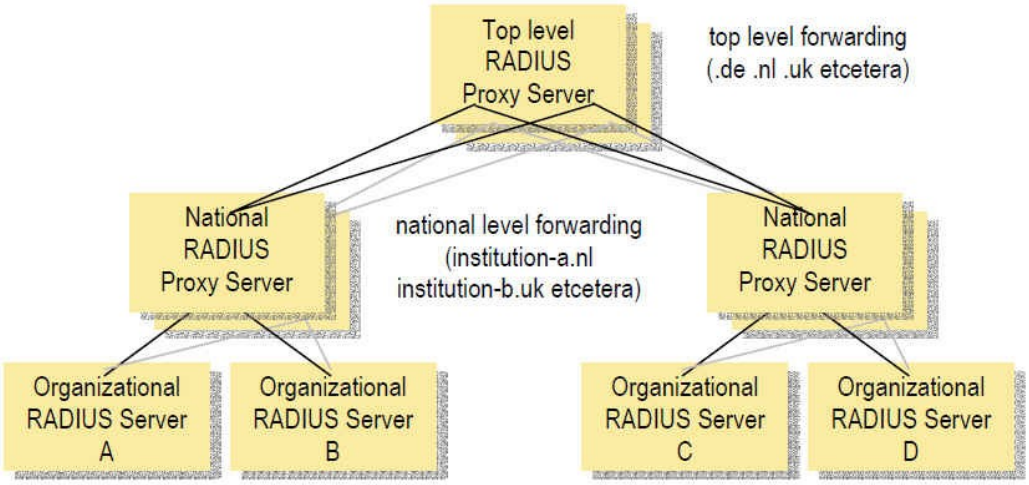

Fig. 5 Arquitectura de roaming internacional. (Fuente 1: "**Mobility Task Force. Deliverable D: Inventory of 802.1X-based solutions for inter-NRENs roaming. Version 1.2**")

El uso de RADIUS también hace que sea fácil de conectar la infraestructura *roaming* existente a un operador de red móvil existente (WiFi, GPRS o UMTS). La infraestructura de RADIUS como se describe aquí puede introducir bucles en el flujo de mensajes, que puede conducir a la falla de servidores RADIUS. Para evitar esto, cada servidor RADIUS puede ser obligado a no reenviar mensajes destinados al dominio que maneja. Además, el proxy puede filtrar estos eventos, y observar la cantidad de saltos en los mensajes.

Los dispositivos de control de acceso pueden ser instalados en pares, aunque esto no suele hacerse debido a los altos costos. Además, cada dispositivo de control de acceso puede ser configurado para preguntar a dos (o más) servidores RADIUS. Cuando un servidor RADIUS falla, el otro puede hacerse cargo. El mismo mecanismo se puede utilizar entre servidores RADIUS en la infraestructura proxy. La Fig.6 muestra la autenticación en entorno proxy Radius.

Puesto que en promedio, el software de los servidores RADIUS no consume muchos recursos de hardware, una computadora de características promedio podría servir decenas de solicitudes de autenticación, o incluso cientos de solicitudes de reenvío por segundo.

La autenticación es sólo necesaria en el comienzo de una sesión de usuario y cuando un usuario se mueve entre los dispositivos de control de acceso, por lo tanto un servidor RADIUS en un nivel proxy nacional puede servir potencialmente miles de sesiones de usuarios al mismo tiempo.

La escalabilidad en términos de rendimiento de procesamiento es implícitamente lograda por el hecho de que cada dispositivo de control de acceso se encarga del cifrado de datos en la capa 2 a la velocidad de cable.

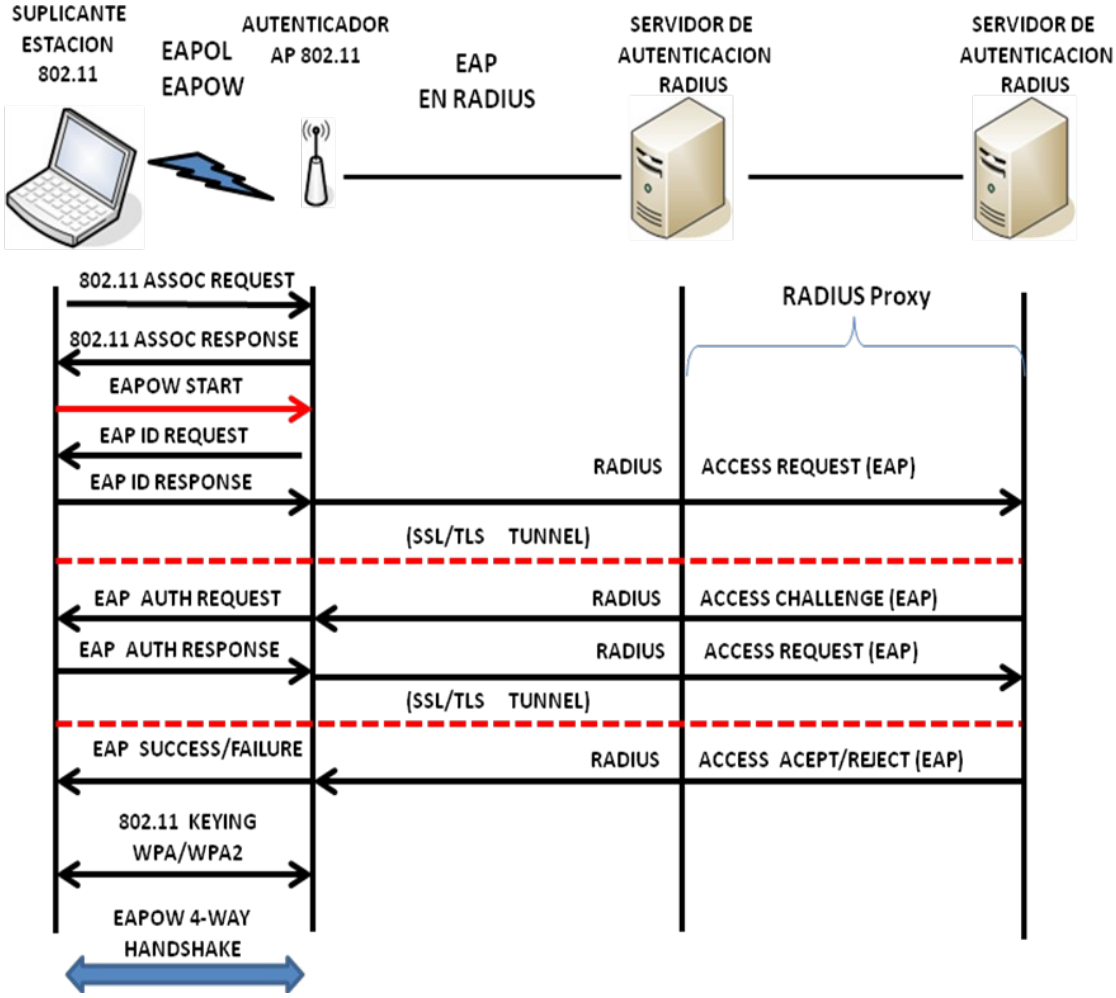

Fig. 6 Autenticación con IEEE 802.1x entorno Proxy Radius

Lecturas sugeridas

(Se encuentran en los recursos del módulo 1)

- Deliverable DJ5.1.4: Inter-NREN Roaming Architecture: Description and Development Items
- Deliverable DJ5.1.5,1: Inter-NREN Roaming Infrastructure and Service Support Cookbook - First Edition
- Deliverable DS5.1.1: eduroam Service Definition and Implementation Plan