Sistema para el control de acceso a red basado en servicios

System for service-based network access control

Jon Matías

Resumen

Cada vez las redes universitarias y académicas son más complejas y difíciles de gestionar debido a la gran cantidad de usuarios y servicios ofrecidos por las mismas, todo ello unido a su doble condición como red de producción y red para la experimentación. En este contexto, es común la aparición de escenarios puramente conmutados basados en tecnología Ethernet, en los que la gestión de los usuarios se hace en base a perfiles asociados a VLAN. Este tipo de soluciones para el control de acceso a los servicios no son tan granulares como sería deseable, por lo que se presenta una alternativa que trata de dar una respuesta más flexible mediante una modificación realizada sobre el estándar IEEE 802.1X. Las aportaciones fundamentales sobre el mismo son la definición de servicio, el control de acceso a red basado en puerto de servicio (en contraposición a puerto físico o lógico) y la extensión EAPoL-in-EAPoL que permite múltiples procesos de autenticación simultáneos desde un mismo nodo. Como resultado el usuario tendrá que autenticarse frente a cada servicio antes de poder acceder al recurso, logrando únicamente acceso a la red para alcanzar aquellos destinos previamente autorizados.

Palabras clave: seguridad, AAA, IEEE 802.1X, servicios Ethernet.

Summary

University and academic networks are becoming increasingly complex and difficult to manage due to the high number of users and services they offer, coupled with their dual role as production and experimentation networks. In this context, it is common to see purely commutated scenarios based on Ethernet technology, in which user management is based on VLAN associated profiles. These types of solutions for controlling service access are not as granular as would be desirable, for which reason an alternative is offered that endeavours to respond more flexibly through a modification carried out on the IEEE 802.1X standard. The fundamental contributions it makes are service definition, service port based network access control (as opposed to physical or logical ports) and the EAPoL-in-EAPoL extension that allows for multiple simultaneous authentication processes from a single node. As a result, users will have to login to each service before they can access the resource and will only given access to the network to reach those areas for which authorisation has been granted.

Keywords: security, AAA, IEEE 802.1X, Ethernet services.

Cada vez es más común la aparición de escenarios conmutados basados en tecnología Ethernet

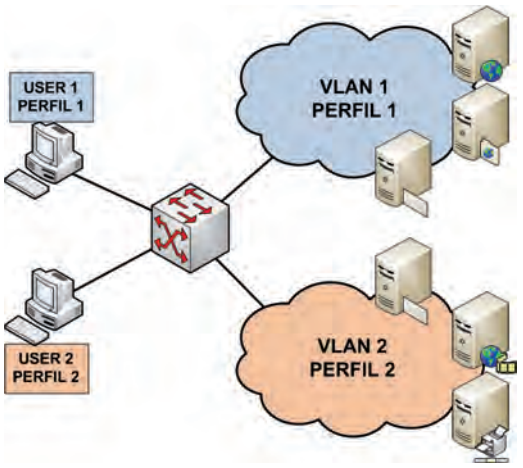
1. Introducción

Las redes universitarias (y académicas) pueden ser consideradas como entornos de una considerable complejidad debido a que aúnan una doble vertiente tanto como red en producción como red de experimentación e investigación. Además, en muchos casos se une el gran número de usuarios a gestionar (más de 50.000 en el caso de la UPV/EHU[1]) con múltiples sedes geográficamente dispersas (31 facultades distribuidas en tres campus), lo que supone una red de un tamaño importante. Por si no fuera poco, a esto se une la gran cantidad de servicios que sobre dicha red se ofrecen, tanto desde los propios gestores de la red como desde los propios usuarios de la misma, como profesores, investigadores, departamentos, grupos y alumnos (normalmente con acceso restringido a estos últimos servicios desde fuera de la propia red).

El gran número de usuarios a gestionar múltiples sedes geográficas supone una red de un tamaño importante

Cada vez es más común la migración de dichas redes a entornos totalmente conmutados haciendo uso de tecnología Ethernet[2][3] (como es el caso de la red de la UPV/EHU), restringiendo en gran medida el empleo de routers. En este tipo de escenarios **(figura 1)** es frecuente el uso de las VLANs [4] para la diferenciación de los diversos perfiles de usuario y el control del acceso a los servicios a los que tiene acceso cada usuario por el hecho de pertenecer a un determinado perfil.

FIGURA 1. GESTIÓN DE USUARIOS BASADA EN PERFILES



Todos los alumnos de un mismo perfil tendrán acceso al mismo conjunto de recursos y servicios de la red

Sin embargo, debido a las características del entorno ese tipo de control puede resultar poco granular, perdiendo a nivel de red la capacidad de realizar un control basado en la identidad del usuario. De esta forma, un alumno tendrá potencialmente el acceso al mismo conjunto de recursos y servicios de la red que el resto de alumnos por pertenecer a ese perfil.

Debido a las limitaciones del sistema presentado, se pretende obtener una solución mucho más flexible y potente. Por lo tanto, primeramente se analizarán los objetivos que se pretenden alcanzar con dicha propuesta, para posteriormente introducir los fundamentos y aportaciones de la misma. Además, también se presentará una plataforma de pruebas que ha sido construida para validar el diseño realizado y validar todas las hipótesis realizadas. Finalmente, se realizarán una serie de conclusiones sobre el trabajo realizado y se mostrarán las líneas futuras en las que actualmente se está investigando.

2. Objetivos

El principal objetivo es conseguir controlar el acceso que cada usuario pueda tener a los sevicios disponibles en base a su identidad

El principal objetivo que se persigue en esta propuesta es el de conseguir un sistema capaz de controlar a nivel de red y de forma individualizada el acceso, que cada usuario pueda tener a los servicios y recursos disponibles en base a su identidad.

De esta forma, ese mismo alumno que por su condición de alumno accedía a una serie de servicios de la red, podrá además pertenecer a un grupo de investigación y tener acceso a un subconjunto mayor de recursos exclusivamente alcanzables por los miembros de dicho grupo. De entre todos ellos, la salida a Internet puede ser un recurso más a ser controlado.

La gestión de dicho sistema puede llegar a ser descentralizada, de forma que en el caso anterior, el grupo de investigación sería capaz de gestionar y controlar el acceso a sus propios recursos. Por lo tanto, será el propio grupo el encargado de dar de alta o de baja a los miembros que pertenezcan a dicho grupo.

El sistema propuesto tiene que cubrir además, una serie de objetivos parciales que permitan alcanzar de una forma adecuada el objetivo principal.

Por una parte, es necesario abordar la definición de lo que se entiende por servicio. Esto será de vital

importancia, ya que la propuesta variará ostensiblemente en función de la misma. Por lo tanto, un servicio será todo recurso de red que se ponga a disposición de un conjunto de usuarios y que sea susceptible de ser controlado. Esto quiere decir que un servicio será identificado de forma genérica, pudiendo ser definido a cualquier nivel (físico, enlace, red,... o incluso aplicación). Sin embargo, dicha identificación tendrá que ser unívoca, convirtiendo a dicho servicio en algo único que pueda ser diferenciado del resto.

Por otro lado, la seguridad es un elemento fundamental de la solución, siendo uno de los objetivos prioritarios de la misma. En este sentido, se destacan dos aspectos de la seguridad: AAA (Authentication, Authorization y Accounting) y control de acceso. En cuanto a la AAA[5], cada usuario deberá ser autenticado y autorizado antes de poder acceder a cada servicio. En el otro ámbito, se realizará un control de acceso a nivel de red en función de la identificación del servicio y de la identidad del usuario.

Finalmente, la solución tendrá como objetivo la configuración adecuada y segura de los diversos nodos y elementos involucrados en la provisión del servicio. La fase de configuración será necesaria y estará ligada al proceso de autenticación anterior. Por lo tanto, la configuración también dependerá del servicio en cuestión y de la identidad del usuario.

La seguridad es un elemento fundamental de la solución, siendo uno de los objetivos prioritarios de la misma

3. Sistema de Control de Acceso Basado en Servicios

En esta sección se va a profundizar sobre cada uno de los elementos que componen la propuesta realizada para el control de acceso basado en servicios. Dichos elementos se corresponden con los objetivos planteados en el apartado anterior a los cuales se tratará de dar una respuesta viable.

3.1. Definición de servicio

Hasta ahora se ha presentado un escenario en el cual los usuarios son agrupados bajo perfiles para su gestión. En este caso, cada usuario sólo podía pertenecer a un perfil, el cual iba a hacerse corresponder con una determinada VLAN. De esta forma, se llevaba a cabo una asociación entre cada perfil y un conjunto de servicios que estaban disponibles a través de la VLAN correspondiente.

FIGURA 2. DEFINICIÓN DE SERVICIO BASADO EN PERFIL XML

```
<service id="EHUtb">
  <flowid>
    <!- Service related info -->
      <dip>158.227.0.0/16</dip>
  </flowid>
  <clients>
    <!- Client related info -->
    <client id="jonatEHUtb">
      <security>
        <smac>00:01:02:03:04:05</smac>
      </security>
      <qos>
        <bandwidth>10Mbps</bandwidth>
      </qos>
    </client>
  </clients>
</service>
```

A partir de ahora, tal y como se ha adelantado, un servicio será un recurso de red cuyo acceso será susceptible de ser controlado. El servicio podrá ser definido a cualquier nivel (enlace, red,...), siendo incluso admisible una definición a múltiples niveles. De esta forma, se logra una definición suficientemente genérica como para dar cabida a posibles escenarios futuros.

Un servicio será un recurso de red cuyo acceso será susceptible de ser controlado

Todo servicio tiene que poder ser identificado de forma unívoca para que se pueda ser reconocido a la hora de establecer el control de acceso. En este caso, se ha propuesto una definición de los mismos basada en perfiles XML **(figura 2).** En estos perfiles se pueden distinguir dos tipos de parámetros: los de servicio y los de usuario. Los parámetros de servicio identifican unívocamente a los servicios, mientras que los de usuario contienen información específica de cada usuario.

Es importante tener en cuenta que la identificación de los servicios afecta directamente al control de acceso que deba ser aplicado en cada caso.

3.2. Seguridad

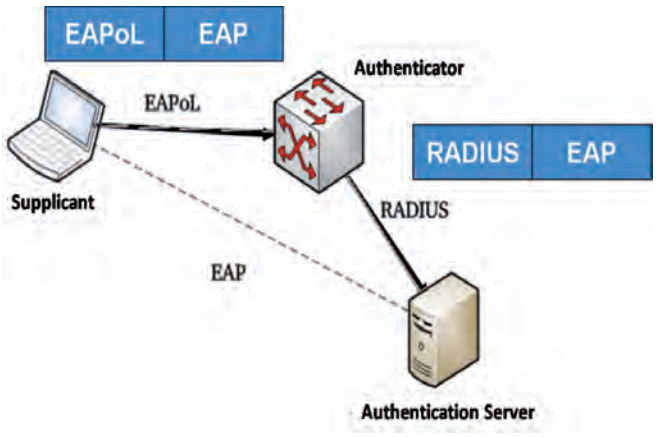
A nivel de la seguridad del sistema se puede distinguir entre la solución de autenticación y el control de acceso a aplicar. A continuación se profundizará en cada uno de ellos.

3.2.1. *Autenticación y Autorización*

El objetivo principal que se persigue es el de lograr un sistema en el cual cada usuario tenga que ser autenticado y autorizado antes de poder acceder a un recurso cualquiera. Para ello se opta por un modelo de seguridad basado en el estándar IEEE 802.1X[6]. Esta decisión se debe al tipo de entorno en el que se desarrolla la solución, una red universitaria basada en Ethernet totalmente conmutada. Por lo tanto, se trata de buscar una solución nativa (IEEE 802.1X es la propuesta a nivel de estándar para las redes 802) y eficiente[7]. Además, se trata de una alternativa ampliamente utilizada tanto en entornos WiFi como Ethernet.

Se persigue lograr un sistema en el que cada usuario tenga que ser autenticado y autorizado antes de poder acceder a un recurso cualquiera

FIGURA 3. PROTOCOLOS ESTÁNDAR IEEE 802.1X



El suplicante es el usuario que accede a la red y el autenticador el nodo que controla el acceso

El estándar IEEE 802.1X **(figura 3)** define tres entidades: suplicante, autenticador y servidor de autenticación. El suplicante es el usuario que quiere acceder a la red, mientras que el autenticador es el nodo que controla el acceso a la misma. Por su parte, el servidor de autenticación será el encargado de constatar la identidad del usuario y si procede, autorizar el acceso del mismo a la red.

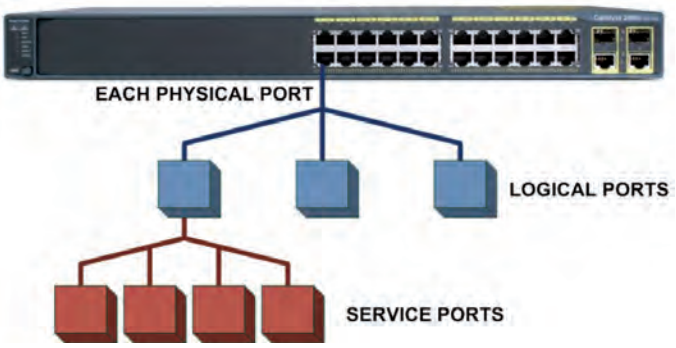
Sin embargo, el estándar no es capaz de dar respuesta al reto planteado, siendo necesarias varias modificaciones. El problema reside en su capacidad de todo o nada a la hora de permitir el acceso a la red.

Por lo tanto, la propuesta se basa en una modificación del estándar 802.1X que posibilita la concurrencia de múltiples procesos de autenticación y el control basado en puerto de servicio (frente al concepto de puerto lógico), siendo fundamental la identificación que se haga del servicio.

La primera de las modificaciones hace referencia al concepto de puerto **(figura 4)** definido dentro del estándar. Inicialmente el puerto se correspondía con cada puerto físico existente en un dispositivo. Dicho

concepto evolucionó hacia lo que hoy día se conoce como puerto lógico, que no es más que la virtualización de cada puerto físico, lo que permite mantener el control sobre múltiples usuarios que se encuentran compartiendo el mismo medio físico. La diferenciación de cada puerto lógico se puede realizar de una forma muy sencilla en base a la dirección MAC origen de los paquetes. Hasta ahora, nada nuevo con respecto al estándar.

FIGURA 4. DEFINICIÓN DE PUERTO DE SERVICIO



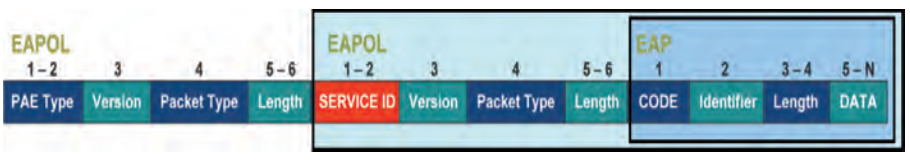
Cada puerto de servicio tendrá asociado un perfil XML

Debido a la necesidad de controlar de forma individualizada el acceso a múltiples servicios por parte de un mismo cliente, se introduce el concepto de puerto de servicio. Un puerto de servicio es la virtualización del puerto lógico que permite realizar un control de acceso basado en la identificación particular de cada servicio. Por lo tanto, cada puerto de servicio tendrá asociado un perfil XML como el definido en el apartado 3.1.
Además del puerto de servicio, se introduce una segunda modificación sobre el estándar IEEE 802.1X y es relativa al protocolo EAPoL. Como ya se ha comentado, este protocolo se encarga de la comunicación entre el suplicante y el autenticador. Sin embargo, EAPoL restringe la autenticación a un solo proceso de forma concurrente. Lo que con este se logra es la autorización del acceso a la red a través del puerto lógico.

Como una nueva aportación, se presenta el protocolo EAPoL-in-EAPoL **(figura 5),** el cual permite a un mismo usuario autenticar múltiples recursos de forma simultánea. Esto implica modificaciones software tanto en el usuario como en el nodo de acceso a la red. Este nuevo protocolo es compatible con EAPoL, ya que se fundamenta en la definición de un nuevo tipo de paquete capaz de encapsular a dicho protocolo de una manera identificada.

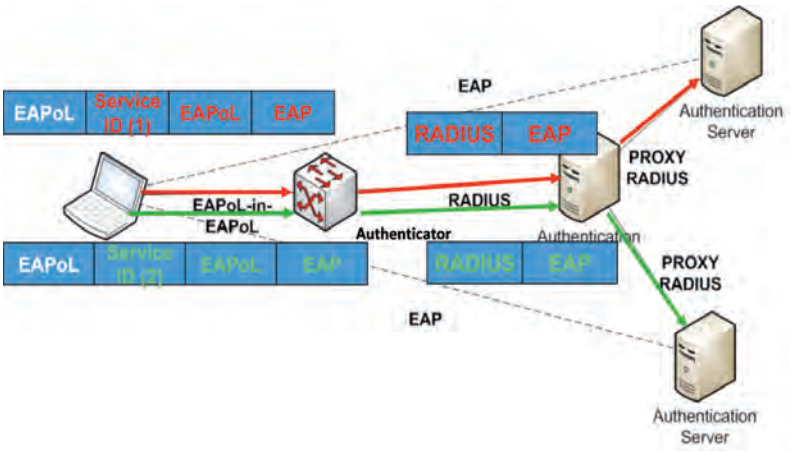
El protocolo EAPol-in-EAPol permite a un mismo usuario autenticar múltiples recursos de forma simultánea

Figura 5. Trama EAPoL-in-EAPoL



En la **figura 6** se puede ver a este protocolo en acción, donde se logran realizar dos procesos de autenticación a dos servicios diferentes de forma simultánea.

FIGURA 6. MÚLTIPLES AUTENTICACIONES SIMULTÁNEAS

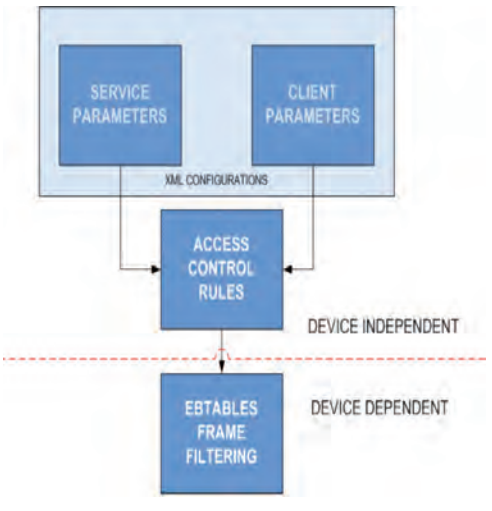


Se pretende obtener un sistema capaz de controlar el acceso de forma dinámica y granular

3.2.2. *Control de Acceso*

El control de acceso definido dentro del IEEE 802.1X está íntimamente relacionado con la definición de puerto que en este se realiza (puerto lógico). Esto quiere decir que debido a la nueva definición de puerto que se ha introducido (puerto de servicio), el control de acceso tendrá que modificarse para adaptarse a la definición e identificación del servicio en cuestión.

FIGURA 7. CONTROL DE ACCESO BASADO EN EBTABLES



Se ha implementado un control basado en una herramienta de filtrado de tramas de nivel dos: ebtables

En esta ocasión se pretende obtener un sistema capaz de controlar el acceso de forma dinámica y granular. Esto quiere decir, que dicho control va a definirse en función de los parámetros del servicio extraídos del perfil XML y de la identidad del usuario. Con todo ello se generarán las reglas de acceso que serán implementadas por el nodo de acceso en función del mismo. Como caso particular, se ha implementado un control basado en una herramienta de filtrado de tramas de nivel dos conocida como ebtables. De esta forma, la autenticación exitosa del servicio desencadena la creación de dichas reglas asociadas al servicio.

3.3. Configuración

Por último, asociado al proceso de autenticación se establece un proceso de configuración[8]. Dicho proceso se desencadena por parte del servidor de autenticación y se encarga de configurar adecuadamente todos los nodos de red necesarios para la correcta provisión del servicio. Es importante tener en cuenta que parte de los argumentos de entrada necesarios para llevar a cabo la configuración dependen del proceso de autenticación. Además, dicha relación entre ambos procesos se establece en un contexto seguro, lo cual otorga gran fiabilidad y seguridad al sistema final.

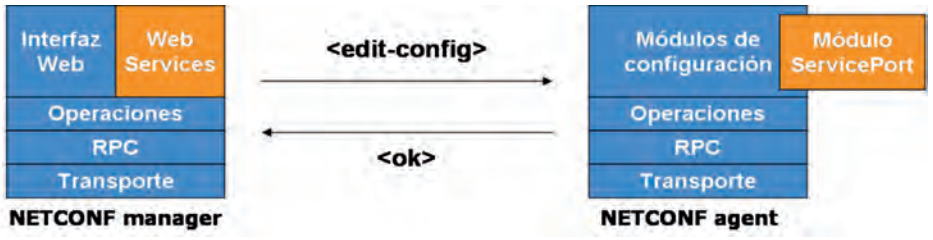
La configuración depende de varios parámetros como son: el resultado del proceso de autenticación previo, la identidad del usuario y su localización, la naturaleza del servicio y las particularidades de la red.

Se ha optado por utilizar NETCONF, que es un sistema de configuración y monitorización de red definido por el IETF (RFC 4741). NETCONF posee capacidades avanzadas de configuración y permite la definición de configuraciones complejas. Las configuraciones se representan en formato XML y se agrupan en base a módulos. Además, se definen varias operaciones (<edit-config>, <get-config>, <copy-config>, <lock>...) que se realizan sobre una capa de transporte segura (SSH,...)

NETCONF posee capacidades avanzadas de configuración y permite la definición de configuración complejas

En este caso son necesarias dos aportaciones. Por una parte, es necesario unir el proceso de autenticación al posterior proceso de configuración, por lo que se crea una interfaz Web Services para permitir iniciar la configuración a través de NEFCONF desde el servidor de autenticación. Por otro lado, es necesario definir un nuevo módulo denominado ServicePort, encargado de soportar las nuevas capacidades de configuración para la identificación de servicios y control de acceso.

FIGURA 8. NETCONF

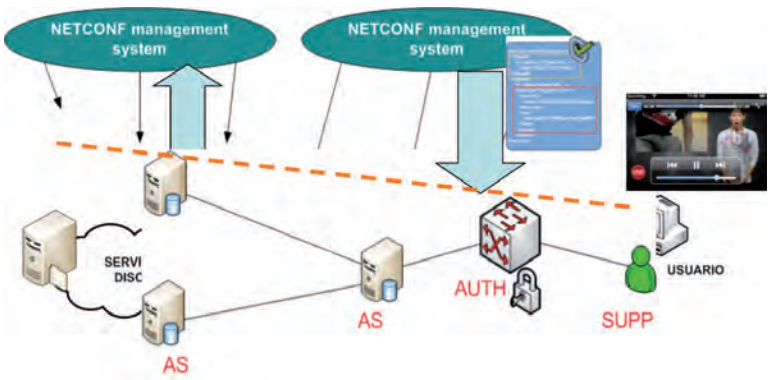


Es necesario unir el proceso de autenticación al proceso de configuración

4. Plataforma de Pruebas

Se dispone de una plataforma (Fig. 9) capaz de controlar el acceso de usuarios por servicio, en la cual se realiza una gestión de los recursos distribuida y el acceso se configura en base a perfiles XML dinámicamente generados en función de la identidad del usuario y en los que se identifica el servicio que se habilita. Dichas reglas de acceso se aplican sobre los elementos frontera una vez terminado exitosamente el proceso de autenticación.

FIGURA 9. PLATAFORMA DE PRUEBAS



Se ha conseguido un sistema capaz de controlar el acceso de cada usuario a los servicios de la red en base a su identidad

El proceso se puede resumir de la siguiente manera. Primeramente para acceder al servicio es necesario completar un proceso de seguridad. Una vez que el cliente completa exitosamente el proceso de seguridad, el servidor de autenticación invoca un proceso de configuración basado en NETCONF. En este punto, se envían los perfiles XML que permiten identificar los servicios, a partir de los cuales se generan las correspondientes reglas de control de acceso. Una vez aplicadas estas reglas en el nodo de acceso, ya se empieza a ofertar el servicio.

5. Conclusiones

Como conclusión se puede resumir que se ha obtenido un sistema capaz de controlar a nivel de red y de forma individualizada el acceso de cada usuario a los servicios en base a su identidad. Además, el sistema final permite un acceso nómada logrando obtener los mismos servicios con independencia de la localización.

La gestión del sistema puede ser descentralizada

Tal y como se ha comentado previamente, la gestión del sistema puede ser descentralizada, siempre y cuando exista una relación de confianza con terceras entidades. De esta forma, se podría llegar a una situación en la que el acceso sea gestionado por el propio proveedor del recurso. Aún así, y para evitar posibles agujeros de seguridad, se debe de controlar que el recurso que se activa y al cual se permite el acceso, pertenezca al propio gestor.

La propuesta realizada está basada en modificaciones del estándar IEEE 802.1X. Las principales aportaciones son las siguientes: permitir múltiples procesos de autenticación simultáneos gracias a EAPoL-in-EAPoL, realizar un control basado en puerto de servicio, y definir la identificación del servicio acorde a lo expuesto. Además, se dispone de una plataforma capaz de controlar acceso de usuarios por servicio, en la cual el proceso AAA está basado en EAPoL-in-EAPoL, se realiza una gestión distribuida, la configuración se hace en base a perfiles XML dinámicamente generados en función de la identidad del usuario, y se crean reglas de acceso aplicadas con ebtables.

Como resultado se obtiene un incremento de la seguridad de la red, ya que únicamente progresan hacia cada servicio o recurso conexiones previamente autorizadas. Otro factor que contribuye al incremento de dicha seguridad es el control que de forma simultánea se realiza tanto a nivel de origen como de destino de los paquetes.

6. Líneas futuras

Actualmente se está trabajando en una completa definición de servicios capaz de cubrir todo tipo de escenarios, mediante la identificación del flujo de servicio a diversos niveles. También se está tratando de integrar la solución con la definición de servicios realizada por el MEF, en donde se definen escenarios ciertamente complejos, como servicios E-Line, E-LAN o E-Tree.

Por otro lado, se quiere lograr la integración de una solución con soporte de calidad de servicio, en la que de la misma forma en que se configuran otra serie de parámetros, se puedan incluir parámetros de QoS en la fase de identificación del servicio. En este caso la QoS podrá depender tanto del servicio como de la identidad del usuario. Posteriormente, la política de calidad se aplicará en la fase de configuración.

Adicionalmente, el proceso de autenticación por el cual se logra el acceso al servicio puede emplearse como desencadenante de que dicho servicio se genere bajo demanda, mediante la creación de un recurso virtualizado. En este caso, al proceso de autenticación y configuración, se une el proceso de creación. También sería interesante la integración del sistema con la autenticación y autorización de acceso a servicios de e-Ciencia. En este tipo de entornos es muy común hacer uso de la red como recurso más para la experimentación. Finalmente se está pensando en la creación de un framework que permita la gestión sencilla tanto de los recursos como de los usuarios.

Se está trabajando en una definición completa de servicios para cubrir todo tipo de escenarios

Referencias

[1] Universidad del País Vasco (UPV/EHU), *http://www.ehu.es*

[2] D. Minolti, P. Johnson, E. Minolti, *Ethernet-Based Metro Area Networks.* Planning and Designing the Provider Network, McGraw-Hill. 2002

[3] A. Kasim, Delivering Carrier *Ethernet: Extending Ethernet Beyond the LAN*, McGraw-Hill. 2008

[4] *IEEE Std. 802.1Q*, Virtual Bridged Local Area Networks, 2005

[5] Minhyung Kim et al., *"High performance AAA architecture for massive IPv4 networks"* Future Generation Computer Systems Volume 23, Feb 2007, pp. 275-279

[6] *IEEE Std. 802.1X-2004*, Port-Based Network Access Control, 2004

[7] Juniper White Paper, *"Using PPPoE and IPoE in Ethernet Broadband Networks"*, Jan 2008

[8] Alexander Clemm et al.,*"Generic provisioning of heterogeneous services – a close encounter with service profiles"* Computer Networks Volume 43, 2003, pp.43-57

Jon Matías
(jon.matias@ehu.es)
Universidad del País Vasco