Modelo de Red Orientado a Servicios Basado en Ethernet

Jon Matias, Eduardo Jacob, Purificación Saiz, Marivi Higuero, Armando Astarloa
Universidad del País Vasco (UPV/EHU)
Alda. Urquijo s/n, 48013 Bilbao
Telf: 94 601 7370, Fax: 94 601 4259
E-mail: {jon.matias, eduardo.jacob, puri.saiz, marivi.higuero, armando.astarloa}@ehu.es

Resumen

Ethernet es una tecnología que ha conseguido evolucionar desde su origen en las LAN hasta convertirse en una alternativa para ofrecer conectividad con calidad de proveedor. Esto ha sido posible gracias un gran esfuerzo realizado desde los principales organismos de estandarización (ITU-T, IEEE, MEF). Sin embargo, aún hay algunos aspectos que no están totalmente resueltos en cuanto a la aplicación de políticas de calidad y procedimientos OAM. Aquí se presenta un modelo de red orientado a servicios basado completamente en tecnología Ethernet, el cual define un entorno multiproveedor y multiservicio. También se presentan algunos de los servicios más relevantes en los que se están trabajando y una solución para introducir un mecanismo de autenticación, autorización y control de acceso a los mismos.

1. Introducción

Ethernet es una tecnología de área local que ha conseguido implantarse tanto en redes domésticas como empresariales gracias a su sencillez, flexibilidad, interoperabilidad, ancho de banda y bajo costo.

Como tecnología de acceso Ethernet, Ethernet First Mile (IEEE 802.3ah), permite superar el cuello de botella que presentan actualmente el resto de tecnologías de primera milla (PSTN/ISDN, xDSL, cable coaxial, T1/E1, T3/E3 o OC3/STM-1). Otras ventajas son la sencillez, escalabilidad, único protocolo extremo-extremo, capacidad para el tráfico de datos, voz y video… y sobre todo a mucho menor coste. Se definen tres topologías de red: EFM Copper, EFM Fiber y EFM PON.

Como tecnología de transporte Ethernet ha tenido un gran desarrollo en los últimos años gracias al trabajo de los principales organismos de estandarización: el ITU-T SG15 (Ethernet Private Line G.8011.1, Virtual Private Line Service G.8011.2, UNI/NNI G.8012, G.8021), el MEF (MEF 6 y 10, UNI MEF 11) y el IEEE (redes conmutadas de proveedor 802.1ad, redes conmutadas troncales de proveedor 802.1ah, 802.17). Se recogen las claves de este funcionamiento destacando la jerarquía, reenvío basado en IVL, OAM, ingeniería de tráfico, resiliencia y seguridad. Por otra parte se presentan los dos servicios basados en Ethernet propuestos desde el MEF: E-Line (punto-punto) y E-LAN (multipunto-multipunto).

Los dos principales problemas que presenta Ethernet como tecnología de acceso y transporte son el soporte eficiente de SLA (QoS) y la gestión del tráfico en tiempo real (OAM). En este caso tanto el ITU-T SG13 (Y.17ethoam) como el IEEE (802.1ag) están trabajando en paralelo.

Por último se presenta un modelo de red orientado a servicios que se basa únicamente en Ethernet. Se plantea un entorno multiproveedor, en el que la conectividad de nivel de enlace la ofrezcan diferentes proveedores de acceso, y multiservicio, en el que cada servicio se puede contratar con un proveedor diferente con independencia de quién ofrezca el acceso.
Los servicios ofertados pueden ser de nivel dos o superior, siendo siempre accesibles a través de Ethernet debido a la naturaleza de las redes de acceso y transporte. La ubicuidad y el plug&play son características únicas que posicionan a Ethernet como la mejor alternativa para ofrecer aplicaciones centradas en servicio. Entre estos servicios se pueden destacar los de voz, video, datos, Internet, VPNs… De esta forma habrá proveedores de servicio que no ofrezcan conectividad y viceversa, pudiendo cada cliente contratar cada servicio con un proveedor distinto.

En el artículo se presentan los resultados de nuestro trabajo realizado tanto en el proyecto PlaNetS (Eureka Medea+) como en el proyecto EthSec (MCyT TIC2003-09585-C02-01).
Dentro del proyecto PlaNetS se ha trabajado en la autenticación de servicios y aspectos del control de acceso e identificación de flujos. En este caso cada usuario final se conectará a su proveedor de acceso el cual controlará el acceso a los distintos servicios ofertados por terceras partes.
El objetivo del proyecto EthSec es la creación de un nuevo servicio de cifrado de Ethernet extremo a extremo, dicho servicio podría pasar a formar parte del grupo de servicios ofertados en el modelo presentado con anterioridad.

2. Ethernet como única tecnología

No es nada nuevo que cada vez los usuarios finales residenciales demandan un mayor ancho de banda ya que cada vez sus necesidades son mayores. Originariamente la navegación y el correo se

limitaban al intercambio de texto e imágenes de cierta calidad, actualmente los usuarios demandan contenidos visuales atrayentes y de gran calidad. La llegada de contenidos multimedia hacen las páginas web y los correos cada vez más pesados. Además las aplicaciones para la comunicación basadas en audio o video están cada vez más extendidas. Otro gran factor a tener en cuenta son las comunicaciones P2P, que demandan un gran ancho de banda.
Desde el punto de vista de las empresas la necesidad de conectividad está cada vez más extendida. El modelo empresarial actual hace cada vez más valiosa la información, siendo igualmente importante poder acceder a la misma en todo momento de forma compartida por todos los empleados autorizados. Esto hace que la capacidad de transportar cada vez un mayor volumen de datos y a mayor velocidad sea algo demandado por este tipo de usuario.
Uno de los aspectos a tener más en cuenta es el factor económico que limitará el éxito de la solución técnica aportada.
Desde el punto de vista de los proveedores de acceso existe la necesidad de conseguir un mayor ancho de banda y un mayor control de la QoS de los datos que viajan a través de su red. La tendencia actual es a que los proveedores hagan uso de la misma red para ofrecer servicios tan dispares como son el transporte de datos, voz y video.
Actualmente en las soluciones de proveedor emplean múltiples tecnologías, haciendo necesaria la traducción entre las diferentes pilas de protocolos. Esta conversión tiene tres problemas de rendimiento, conflictos en la traducción por las particularidades de cada protocolo, y dificultades en la labor de gestión asociada al sistema final resultante.

Por otra parte cabe reseñar el hecho de que la mayor parte del tráfico empieza y termina en Ethernet como tecnología de nivel dos. Esto es debido a que Ethernet es un protocolo sencillo, con gran flexibilidad, que alcanza altas velocidades de transmisión y que permite desarrollos baratos. Aunque se hable de Ethernet como una única tecnología en realidad se trata de un conjunto de estándares y definiciones, todas ellas fácilmente interoperables al compartir el formato de trama y el protocolo de acceso al medio (CSMA-CD).
Un aspecto importante a la hora de elegir una tecnología (de cara a futuro) es su capacidad para aumentar el ancho de banda que es capaz de transmitir y la sencillez con la que se pueda migrar una red en producción a nuevas versiones. Esto es lo que realmente hace a Ethernet una buena opción como tecnología, su continua evolución y fácil compatibilidad con las versiones anteriores.

La pregunta en este punto es, ¿sirve Ethernet como única tecnología extremo a extremo? o más concretamente la cuestión es si desde el punto de vista de un proveedor de acceso se va a poder hacer uso de Ethernet como tecnología de acceso y de transporte. La respuesta a esta pregunta es inmediata, NO. Ethernet inicialmente fue creada para dar respuesta a una problemática concreta, dar solución al acceso a un medio compartido en entornos de área local. Antes se han obviado una serie de desventajas que presenta desde el punto de vista del proveedor de acceso como son la falta de soporte para ofrecer una cierta calidad de servicio y sus limitaciones en labores de gestión y mantenimiento (OAM). Esto se analizará en el apartado 2.3 dedicado a las limitaciones de Ethernet.
¿Y entonces? Por suerte es posible mediante una serie de modificaciones acceder a las ventajas tan atrayentes que Ethernet es capaz de aportar. Actualmente se está trabajando para dotar de una cierta calidad de servicio a Ethernet con el objetivo de que pueda cumplir con los requisitos que impongan las SLAs, equiparándose a otras tecnologías. Por otra parte también se está realizando un gran trabajo en la definición de un conjunto de mecanismos de OAM.

2.1. Ethernet como tecnología de acceso

En este apartado se va a introducir Ethernet como tecnología de acceso desde la red de usuario hasta la red del proveedor. En este ámbito se puede destacar la labor llevada a cabo tanto por el IEEE 802.3ah (EFM) como por el Metro Ethernet Forum (el MEF absorbió en 2004 a la Ethernet in the First Mile Alliance, EFMA). Su objetivo es crear y promocionar juntos un estándar que garantice la total interoperabilidad. El grupo del IEEE se encarga de la definición del estándar que emplea la tecnología Ethernet como red de acceso, mientras que el MEF es un consorcio de compañías que se encarga de preparar el mercado para la futura explotación del estándar.

Los enlaces DSL y cable modem trabajan a una capacidad muy inferior a las LAN 10BaseT o las redes wireless. Incluso las líneas T1 a 1.5 Mbps son cuello de botella para muchas aplicaciones, que aún pudiendo ser más rápidas, no lo son lo suficiente, y además con un coste mucho mayor. En este caso aparecerían protocolos como PPP, ATM y SONET/SDH, haciendo que el equipamiento de red extremo a extremo incluya módems, DSLAMs, routers y switches. A medida que aumenta la complejidad de traducciones de protocolos y equipamiento, incrementa el coste de la red.
La tecnología Ethernet va a cambiar todo esto rápidamente en las redes de acceso, y lo hará sobre la infraestructura física existente actualmente utilizando el cableado de cobre existente o la fibra cuando esté disponible. Esto revolucionará las redes de acceso como en su día lo hizo con las redes empresariales, siendo la tecnología dominante en este ámbito. La visión de EFM es un acceso universal de banda ancha haciendo uso de una tecnología simple extremo a extremo, creando servicios y aplicaciones ilimitadas de banda ancha. El resultado es un acceso de banda ancha varias

veces superior, sin complejidad y sin posibles errores en la conversión de protocolos.
Como tecnología de acceso ofrece una serie de ventajas, se trata de un estándar simple y globalmente aceptado que garantiza la interoperabilidad entre dispositivos y que proporciona una gran capacidad de ancho de banda para el transporte para aplicaciones de datos, video y voz. Además, se trata de la infraestructura más efectiva para los servicios de datos, permitiendo un muy bajo coste debido a la economía de escala.

En el esquema de la red de acceso se destacan dos elementos: el Nodo de Acceso y el CPE (Customer Premises Equipment). El primero es el equipamiento de red del operador que se encuentra normalmente en la Central Office (CO), siendo este el nodo que recibe, concentra y dirige los datos desde y hacia las redes troncales de alta velocidad. Al otro lado del enlace se encuentra el abonado, el cual se conecta a la red pública empleando el CPE a través de varias posibles tecnologías (RDSI, DSL, cable, T1/E1, T3/E3 o OC3/STM-1). Con la introducción de EFM en este mercado, el usuario final será capaz de conectarse a la red pública de una forma sencilla por medio de un interfaz Ethernet.
EFM es solución válida para distintas arquitecturas, entornos y medios físicos, como son el par trenzado de cobre, fibra óptica y cable coaxial. Además también contempla diferentes topologías de red: redes punto a punto de cable de cobre (EFMC), redes punto a punto de fibra óptica (EFMF) y redes punto a multipunto de fibra óptica (EFMP). La tecnología EFMH permite la interconexión de las tres anteriores.
El EFM Copper (EFMC) se plantea como solución para las infraestructuras existentes de cobre (Cat3), permitiendo velocidades de 10 Mbps en ambas direcciones (750m). El EFM Fiber (EFMF) plantea una especificación punto a punto sobre fibra como capa física a velocidades desde 100Mbps hasta 1Gbps (10Km). El resultado final se espera que sea la sustitución de las actuales (y caras) líneas T1 y T3. El EFM PON (EFMP) presenta topología punto a multipunto sobre fibra con velocidades de 1Gbps (20Km). Para ello hace uso de la tecnología PON (Passive Optical Network), que es una única fibra que hace uso de splitters ópticos (baratos) para dividir la fibra en diferentes hilos que lleguen a cada abonado.

Uno de los aspectos más importantes es una correcta definición de la gestión para redes Ethernet. El estándar 802.3ah incluye una definición OAM y métodos para redes de cobre y fibra óptica de gestión y monitorización de enlaces y problemas de caídas en el servicio. Aunque ya existía previamente una definición OAM en Ethernet, 802.3ah las extiende y adapta para los escenarios de operación del EFM. Los procedimientos soportados incluyen monitorización, testeo de loopback, detección de fallos y aislamiento.

2.2. Ethernet como tecnología de troncal

Ethernet presenta ciertas limitaciones en capacidad de escalado debido a su propia naturaleza. Por una parte Ethernet presenta un direccionamiento plano, lo que no facilita (sobre todo en redes de tamaño relativamente alto) la labor de conmutado ya que las tablas de conmutación pueden crecer de forma extraordinaria, tablas que tendrán que modificarse en caso de que un nodo final cambie su localización. Por otra parte el uso de mecanismos de auto-descubrimiento broadcast y multicast que emplea no son el mejor sistema para redes de este tipo. Otro de los aspectos más importantes a tener en cuenta es el hecho de que Ethernet es una tecnología que no tiene protección frente a bucles, por lo que se tiene que garantizar que una red que haga uso de esta tecnología no presente bucles en la misma. Todo ello hace que Ethernet tenga limitaciones en cuanto al tamaño máximo que se puede alcanzar en la red final.
Las primeras aproximaciones que tratan de solucionar esta problemática pasan por segmentar la red en múltiples dominios libres de bucles. Esta solución se basa en el empleo de VLANs (Virtual Local Area Network) que identifican partes de la red, lo que también permite segmentar la red en entornos multicast y broadcast diferenciados. Para la interconexión entre equipos que pertenecen a diferentes VLANs es necesario el uso de dispositivos de nivel tres, como es el caso de routers (o dispositivos de nivel dos con funciones de nivel tres).

2.2.1 802.1q / 802.1ad / 802.1ah

El uso y definición de las VLANs viene recogido en el estándar IEEE 802.1q, en él se introduce el tag VLAN a la cabecera Ethernet. Esto es posible mediante la definición de un nuevo EtherType (0x8100) que especifica que lo próximo en la cabecera es un tag VLAN. Tras este campo se introducirá el EtherType original de la trama y se recalculará el campo de control de errores (FCS). El tag VLAN está formado por:

- Priordad de usuario (3 bits): empleado para almacenar el nivel de prioridad de la trama. El uso de este campo se especifica en el estándar IEEE 802.1p.
- CFI (Canonical Format Indicator, 1 bit): flag que indica si la dirección MAC está en formato canónico.
- VID (12 bits): es el identificador de VLAN, y permite hasta 4096 diferentes VLANs.

Con el objetivo de permitir a los proveedores disponer de su propio espacio de VLANs sin afectar el uso que los clientes hagan de dicho campo, se define una extensión de VLAN en el estándar IEEE 802.1ad (Provider Bridges). Este estándar, también conocido como Q-in-Q, permite el desarrollo de lo que se conoce como redes conmutadas de proveedor, en las cuales se definen dos zonas: la red de cliente y la red de proveedor. Esto permite

solventar dos problemas. Por una parte el campo de VID únicamente permite 4096 VLANs distintas, suficientes para la red de cliente pero que no permite al proveedor gestionar adecuadamente su propia red. El otro problema que soluciona es el escalado de la red en dos aspectos, permite a los clientes mantener sus propias VLANs e independiza la red de proveedor de la red de cliente. De no ser así el proveedor tendría que acordar previamente con los clientes el uso que se van a hacer de las VLANs, cuales puede utilizar cada uno y de que forma van a ser gestionadas por el proveedor.

IEEE 802.1ad basa su funcionamiento en apilar de forma consecutiva dos tags VLAN, uno para el proveedor (S-VLAN) y otro para el cliente (C-VLAN). El mecanismo es similar al empleado en 802.1q, las tramas de cliente que llegan al proveedor con tag VLAN (lo que pasará a ser el C-VLAN) son encapsuladas mediante una S-VLAN que vendrá determinada por el servicio al que el cliente haya accedido.

El tag de servicio identifica tanto a una comunidad de interés como a una topología específica dentro de la red de proveedor. Al instanciar un servicio específico en el núcleo Ethernet cada grupo individual de interés (identificado por un S-VID) se asocia a una instancia de spanning tree (MSTP).

Sin embargo, la escalabilidad lograda mediante IEEE 802.1ad no es suficiente y su aplicabilidad es restringida. Esto es debido a que no consigue solucionar los problemas de direccionamiento plano y los aspectos asociados a los dominios broadcast. Además, tal y como se comenta anteriormente el tamaño del VID es inferior al que una red de proveedor requiere.

Dentro de una isla IEEE 802.ad se distinguen dos tipos de elementos principalmente: los que se encuentran en la frontera de la isla y aquellos elementos internos. Las funciones que cada uno de ellos deben de cumplir no son las mismas.

En el caso de los elementos frontera se tendrá que realizar una labor de conversión entre lo que entra por parte del cliente (802.1q) y lo que luego viaja por la red (802.1ad). Se definen diferentes interfaces de cliente a través de los que se proporciona acceso a una instancia de servicio dada, se pueden destacar: interfaz de servicio basada en puerto, interfaz de servicio C-tagged e interfaz de servicio S-tagged.

Los elementos que se encargan de la interconexión interna de la propia red únicamente tendrán en cuenta el identificador S-VLAN a la hora de tomar decisiones.

El empleo de jerarquía es un mecanismo bien conocido para lograr escalabilidad y seguridad en un sistema, labor que Q-in-Q no consigue solventar. Es por este factor por lo que el estándar IEEE 802.1ah (Provider Backbone Bridges) es un elemento fundamental para lograr convertir Ethernet en una tecnología válida para proveedores. Este estándar, también conocido como MAC-in-MAC, aporta a Ethernet las herramientas necesarias para conseguir una infraestructura de proveedor jerárquica verdaderamente escalable, virtualizable y completamente aislada de los dominios broadcast de cliente.

La jerarquía tiene especial utilidad cuando el modelo de cliente se compone de un gran número de relativamente pequeñas comunidades de interés, reduciendo la cantidad de estados de reenvío y aprovisionamiento en el núcleo de la red.

IEEE 802.1ah se fundamenta en el encapsulado de toda la trama Ethernet en una nueva cabecera Ethernet que referencia recursos propios de backbone de la red del proveedor. Esto permite el completo aislamiento del direccionamiento MAC del proveedor y del cliente. Se definen el B-SA y el B-DA para identificar el origen y destino de los datos dentro de la red de proveedor, también se definen el B-VID (identificador de VLAN del backbone), y el I-SID (identificador VLAN de instancia de servicio).

MAC-in-MAC implica un proceso recursivo por el cual las subredes Ethernet de cliente se encapsulan totalmente y se aíslan de la red Ethernet del proveedor. Sin embargo, la capa de servicio, salvo modificación, sigue heredando limitaciones asociadas al autoaprendizaje y el requerimiento asociado de disponer de una topología libre de bucles.

Al igual que en las islas 802.1ad, en MAC-in-MAC se distinguen dos tipos de elementos en la red: aquellos que hacen de puente entre las islas 802.1ad y la red troncal de proveedor, y el interno a la troncal. Del mismo modo varían las funciones que cada uno de ellos desempeñan.

En el caso de los elementos frontera que se encargan de realizar la encapsulación, tendrán que acometer la labor de realizar la correspondencia entre el entorno Q-in-Q y como gestionarlo en su paso por la parte troncal de la red.

Los elementos que se encuentran dentro de la troncal y que no tienen interacción con elementos de la red 802.1ad se basan exclusivamente en los parámetros de la cabecera Ethernet definida para la red troncal (B-SA, B-DA, B-VID y I-SID) para las tareas de conmutado.

En la siguiente Fig. 1 se puede ver la evolución que se ha seguido desde el estándar 802.1 para lograr un Ethernet jerárquico. Para ello primeramente se introdujo el estándar IEEE 802.1q (VLAN), posteriormente el IEEE 802.1ad (Provider Bridges) y finalmente el IEEE 802.1ah (Provider Backbone Bridges).

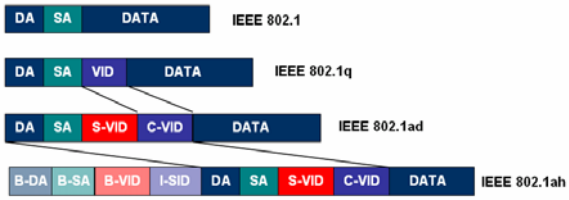

Figura 1.- Evolución de IEEE 802.1

2.2.2. Nuevos modos de reenvío (forwarding)

El aislamiento jerárquico de la red de cliente de las operaciones de proveedor le permite emplear diferentes modos de reenvío y obtener determinismo y predictibilidad en las operaciones mediante la uso de ingeniería de red. La ingeniería de red es un requerimiento básico para los proveedores por el cual son capaces de gestionar los servicios de cliente de forma determinista el tráfico, los fallos y el rendimiento. Mientras que las redes Ethernet estaban anteriormente limitadas a topologías sin bucles y a las imposiciones del protocolo spanning tree (STP), un procedimiento alternativo mediante serie de opciones del plano de control permite dotarlas de una infraestructura con capacidad de ingeniería de red. Esto es gracias a disponer de su propio espacio MAC y VLAN, sin necesidad de compartirlo con el cliente.
El fundamento de todo conmutador se basa en el empleo de las tablas de reenvío de forma que en base a un parámetro que identifique el destino se le asocie a cada trama de entrada un puerto de salida. Por definición, la forma de identificar un destino en Ethernet es mediante la dirección MAC del destino, parámetro que viaja en el campo DA dentro de cada trama. De este modo un conmutador tendrá que rellenar la tabla de conmutación mediante asociaciones MAC destino-puerto salida.

El modo de reenvío basado en IVL (Independent VLAN Learning) se basa en la capacidad que tienen los switches de poder reenviar cada paquete en función de analizar no sólo la dirección MAC destino sino también el tag VLAN. Los conmutadores con soporte de IVL introducen una variación en las tablas de reenvío que las hacen mucho más potentes. En este caso el parámetro que identifica un destino ya no es la dirección MAC destino, sino que a ésta se le añade el identificador de VLAN, basando la decisión de reenvío en 60 bits (frente a los 48 habituales). Así, la tabla de reenvío asociará un puerto de salida a cada par MAC destino-VID. Gracias a IVL se va a permitir la definición de múltiples caminos entre un mismo origen y destino, no sólo por razones de seguridad (para tener rutas alternativas) sino también por motivos de balanceo de tráfico.
Esta capacidad IVL es algo que debe soportar el switch y es independiente del procedimiento por el que se produzcan las asociaciones en la tabla de conmutación. Es importante esta distinción, ya que el IVL es un mecanismo que se puede emplear tanto por procedimientos automáticos para la creación de tabla de conmutación (MSTP) como por procedimientos deterministicos.
MSTP (Multiple Spanning Tree Protocol) es una variante del protocolo de árbol de expansión (STP) que permite la creación de diferentes entornos STP, uno por cada identificador VLAN. Esto permite poseer múltiples árboles de expansión, logrando tener varios caminos entre un mismo origen y destino.

El empleo de otro modo de reenvío más determinista es posible con el mismo hardware de una forma muy sencilla, deshabilitando mediante el plano de control algunas funciones de conmutado. El funcionamiento normal se basa en el aprendizaje de direcciones MAC y el procedimiento de inundación (flooding) para rellenar las tablas de reenvío, pero los switches también permiten la configuración explicita de la tabla de reenvío para el plano de control o gestión.
Es importante tener en cuenta que mediante este procedimiento se configuran pares MAC-VID que crean conexiones unidireccionales. El establecimiento bi-direccional de conectividad puede establecerse mediante una función espejo, pero también es posible definir caminos distintos en un sentido y otro.

2.2.3. Metro Ethernet Forum (MEF)

El Metro Ethernet Forum (MEF) es un comité técnico encargado de analizar las ventajas económicas y de operativa en el despliegue de la tecnología Ethernet en el área metropolitana, y de buscar posibles soluciones a las limitaciones técnicas identificadas. También debe asegurarse de la interoperabilidad entre los diferentes equipamientos. Con este objetivo el comité técnico del MEF tiene centrado su trabajo en cinco áreas: Gestión, Arquitectura, Protocolos/Transporte, Servicios y Testeo.
Un concepto básico promovido por el MEF son las Metro Ethernet Networks (MEN), que son redes que interconexionan LANs de empresas geográficamente dispersas. Esto es debido a que Ethernet tiene la capacidad de incrementar la capacidad de la red desde un punto de vista coste-efectivo, y de ofrecer un amplio rango de servicios de forma escalable, simple y flexible.
Pero las MEN no tienen futuro sin un buen modelo de negocio, para lo que se desarrollaron las SLA (Service Level Agreement) que son la descripción comercial de las SLS (Service Level Specification). La SLS técnico/operativa en la concreción de un conjunto de requisitos de QoS. Para poder ofertar esta QoS sobre redes Ethernet se deben de combinar de varias técnicas, pudiendo proporcionar diferentes anchos de banda y garantizando en cierta medida una protección frente a la pérdida de paquetes.
En definitiva lo que se pretende el MEF es ofrecer redes metropolitanas basadas en la tecnología Ethernet pero con calidad de operador, es decir, garantizando un determinado servicio.

A continuación se va a mostrar la arquitectura definida por el MEF. Los abonados se conectan a la MEN a través del punto de referencia denominado Interfaz de Red de Usuario (User-Network Interface, UNI). Generalmente, los elementos de la red (Network Elements, NE) internos se interconectan a través de los interfaces Internos Red-Red (Internal Network-to-Network, NNI). Dos MEN autónomas se pueden conectar a través de un punto de referencia externo (External NNI, E-NNI). Una

MEN puede interconectarse con otras redes de transporte y de servicio a través de puntos de referencia NNIs de Interconexión de Redes (Network Interworking NNI, NI-NNI), o Interconexión de Servicios (Service Interworking NNI, SI-NNI).

Una de las claves de los atributos de servicio Ethernet es la conexión virtual Ethernet (EVC). Un EVC es una asociación entre dos o más UNIs, en donde una UNI es un interfaz Ethernet estándar que es el punto de delimitación entre el equipamiento de abonado y la MEN del proveedor de servicios. De una manera sencilla, el EVC tiene dos funciones principalmente: conectar dos o más sedes de abonado (UNIs) posibilitando la transferencia de tramas del servicio Ethernet entre ellos, y evitar la transferencia de datos entre sedes de abonados que no son parte de la misma EVC, logrando una privacidad y seguridad similar a Frame Relay o a los circuitos permanentes virtuales (PVC) de ATM.
El MEF define dos tipos básicos de servicios que se analizan a continuación, pudiéndose definir otros servicios en el futuro.
El servicio E-Line proporciona una conexión virtual Ethernet (EVC) punto a punto entre dos UNIs. En su concepción más simple, un servicio E-Line proporciona un ancho de banda simétrico sin ningún rendimiento garantizado, por ejemplo, un servicio best effort entre dos UNIs a 10 Mbps. En formatos más sofisticados, un servicio E-Line puede garantizar un CIR (Committed Information Rate) y un CBS (Committed Burst Size) asociado, un EIR (Excess Information Rate) y un EBS (Excess Burst Size) asociado, y un retardo, jitter y tasa de perdidas garantizado entre dos UNIs de diferente velocidad.
El servicio E-LAN proporciona una conectividad multipunto, pudiendo conectar dos o más UNIs. Los datos del abonado enviados desde una UNI pueden recibirse en una o más de las demás UNIs. Cada sede (UNI) está conectada a un EVC multipunto. Mientras nuevas sedes (UNIs) se van añadiendo, estas son conectadas al mismo EVC multipunto lo que simplifica el alta y la activación de nuevos servicios. Desde el punto de vista de un abonado, el servicio E-LAN hace que la MEN parezca una LAN. En su forma más simple no garantiza ningún rendimiento, mientras que en formatos más sofisticados puede garantizar CIR y CBS, EIR y EBS, y retardo, jitter y tasa de perdidas garantizado.

2.3. Limitaciones de Ethernet

Comparando Ethernet con tecnologías como ATM y FR, posee diversas limitaciones como son el que no ofrece garantía de QoS extremo a extremo, no posee mecanismos de protección, no ofrece capacidad de mantenimiento, y no permite escalabilidad en la utilización de los recursos de la red.

Ethernet se diseño sin tener en cuenta la calidad de servicio (QoS) ni la clasificación de posibles servicios (CoS), por lo que el salto de esta tecnología de redes LAN a su empleo como tecnología de proveedor no es sencillo. Toda relación entre un usuario y su proveedor de acceso se recoge en una SLA en la cual se especifican los parámetros de calidad que se garantizan. Este es uno de los mayores retos que se le presentan a Ethernet en su paso a las redes de proveedor.
Tanto la QoS como la CoS necesitan de la capacidad de discriminar el tráfico. QoS necesita diferenciar un determinado flujo de datos entre un origen y un destino para poder aplicar diferentes políticas. CoS es algo más genérico que un determinado flujo, se identifica el contenido de los datos que viajan y se hace corresponder globalmente con el tipo de datos de otras conexiones. CoS sirve para aplicar políticas de gestión a tráfico que requiere determinadas características, como bajo jitter, bajo retardo, gran ancho de banda o servicio best effort.
La solución en ambos casos pasa por el empleo de VLANs. Este tag permite el uso del VID para identificar diferentes flujos entre un mismo origen y destino, y el empleo de los tres bits de prioridad para la clasificación de tráfico (IEEE 802.1p). Otro aspecto a tener en cuenta es el de las políticas para la reserva de los recursos implicados en el camino y la traducción de las mismas entre los diferentes elementos de la red (802.1q, 802.1ad, 802.1ah).
Aparece en este ámbito un concepto que se denomina QoE (Quality of Experience) que hace referencia a la calidad experimentada desde los usuarios finales, que es al final lo que tendría que controlarse para que los clientes tengan un buen grado de satisfacción. Un apunte importante es el hecho de que una buena QoS entre los diferentes elementos que componen la red no garantiza una buena QoE final.

El otro gran problema que presenta Ethernet a la hora de convertirse en tecnología de proveedor es su limitada capacidad de gestión (OAM). Ethernet no permite detectar si un enlace está caído y reponerse ante ese error, algo básico si el proveedor sólo gestiona el nivel dos. En este sentido se está realizando un gran esfuerzo desde los organismos de estandarización. Existen aportaciones tanto desde el ITU-T SG13 a través del Y.17ethoam, como desde el IEEE a través del 802.3ah (EFM) y el 802.1ag (Connectivity Fault Management), y también desde el Metro Ethernet Forum.

3. Modelo de red orientado a servicios

En este apartado se va mostrar el modelo de red utilizado y las particularidades del mismo. Se trata de un modelo de red orientado a servicios basado únicamente en Ethernet tanto en el acceso como en el transporte, siendo ésta la única tecnología empleada extremo a extremo.
En cuanto a la arquitectura del modelo (Fig. 2) se pueden diferenciar cuatro partes: la red de usuario, la red de acceso, la red de transporte y la red de servicio.

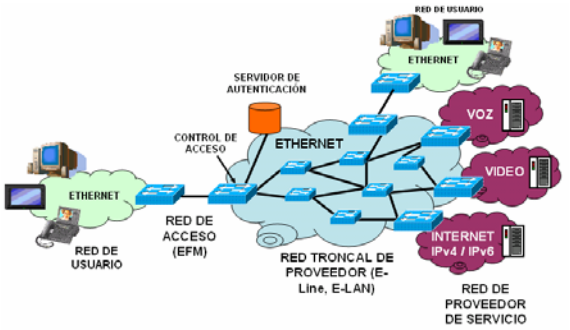

Figura 2.- Modelo de red Orientado a Servicios

El modelo trata de dar respuesta a un entorno multiproveedor y multiservicio, de esta forma un mismo usuario tendría la capacidad de seleccionar con que proveedor quiere contratar el acceso e independientemente de esa decisión seleccionar un proveedor de servicios u otro. Lo que se pretende lograr es un modelo en el que la necesidad de contratar un servicio no implique que se tenga que contratar un determinado proveedor de acceso, y que por lo tanto, la contratación de un proveedor de acceso no limite los servicios que un usuario pueda contratar.

Un aspecto importante a destacar es el hecho de que se define como un modelo orientado a servicios, por lo que el servicio se entiende como fin último de la comunicación. El tener acceso a los servicios es el motivo por el que el usuario decide contratar un proveedor de acceso, sirviendo su red de conexión entre el usuario y el servicio deseado.

Existen multitud de servicios que se analizarán con más detenimiento en un apartado 5, pero a modo de muestra un servicio puede ser la voz, el video (TV o video bajo demanda), el acceso a Internet, un servicio de conectividad extremo a extremo… Según este modelo, independientemente del proveedor de acceso que se contrate, se podrá contratar el servicio de acceso a Internet con el proveedor (ISP) que el cliente desee.

En este sentido se produce un cierto cambio de mentalidad. Servicios tan dispares como la voz, el video e Internet históricamente se entienden como algo diferenciado e incluso su acceso se proporciona por distintos canales. Actualmente esta visión está cambiando y este modelo quiere ir todavía más allá, definiendo un servicio como algo aún más genérico.

El mayor cambio que introduce el modelo presentado es quizás el hecho de que Internet ya no es un modo para acceder a un gran número de recursos, sino que el acceso es algo que permite llegar a Internet al igual que a otra serie de recursos. Las consecuencias de esto no sólo son de procedimiento, sino que esto va a permitir que el acceso a los recursos se realice con una calidad acordada y garantizada. El hecho de acceder a un recurso a través de Internet invalida la capacidad de ofrecerlo garantizando una serie de parámetros puesto que Internet es una red que no ofrece calidad.

El que se especifique el empleo de Ethernet como única tecnología empleada extremo a extremo no limita que por encima puedan viajar protocolos de nivel tres, cuatro o superior. Esta restricción implica que únicamente se tienen en cuenta parámetros de nivel dos para el establecimiento de la comunicación entre el origen (el usuario) y el destino final (el servicio). Por lo que es importante reseñar el hecho de que se trata de una red completamente funcional a nivel dos. Esto permite que la misma red pueda transportar sin problemas diversos protocolos de nivel tres, incluso es posible la definición de servicios que se ofrezcan directamente sobre Ethernet, sin necesidad de ningún otro protocolo por encima.

La capacidad de transportar diversos protocolos de nivel tres hace al modelo transparente a la versión del protocolo IP que cada proveedor de servicios utilice (IPv4 o IPv6) permitiendo incluso la coexistencia de ambos sobre la misma infraestructura del proveedor de acceso. De esta forma la capacidad de soportar diversos proveedores de Internet (ISP) está garantizada de forma sencilla e inherentemente al modelo utilizado, permitiendo diversos esquemas de direccionamiento.

Otro motivo importante que hace interesante el empleo de Ethernet como única tecnología extremo a extremo es la posibilidad que plantea para lograr la interconexión de dispositivos hardware de bajo costo. Este aspecto hace posible la inclusión de redes de sensores y dispositivos con baja capacidad de procesamiento en el modelo.

A continuación se van a sentar las bases técnicas sobre las que se fundamenta el modelo de red presentado. Para ello se va a analizar primeramente la red de usuario, en donde se plantea un escenario de redes LAN Ethernet con capacidad para el tratamiento de VLANs (IEEE 802.1q). En la red del proveedor de servicios se prevé un escenario similar al de la red de usuario, en la que se definirá también un uso propietario de las VLANs (IEEE 802.1q).

La red de acceso al tratarse de una solución puramente Ethernet hará uso de las distintas alternativas aportadas en Ethernet First Mile (IEEE 802.3ah) para el transporte de datos en la primera milla entre la red de usuario y la red de transporte del proveedor de acceso.

En cuanto a la red de transporte existen múltiples alternativas para solucionar la conmutación para establecer conectividad entre la red de acceso y la red del proveedor de servicios. El esquema podría pasar por la definición de múltiples islas de redes conmutadas de proveedor (IEEE 802.1ad). En estas islas se encontrará un elemento frontera encargado de conmutar las VLAN de cliente (C-VLAN) encapsulándolas sobre VLAN de servicio (S-VLAN), las cuales determinarán el servicio al que el cliente haya accedido. Estas islas se interconectarán mediante el empleo de redes conmutadas troncales de proveedor (IEEE 802.1ah) que encapsularán las tramas en un entorno aislado y totalmente controlado por el proveedor.

Uno de los aspectos que hacen a Ethernet una tecnología con futuro para su utilización en el modelo planteado es su capacidad para el tratamiento de tráfico multicast. Esta cualidad queda perfectamente retratada dentro de la definición de servicios que desde el Metro Ethernet Forum se han promovido. El MEF en la actualidad especifica principalmente dos servicios: E-Line y E-LAN.
El servicio E-Line es el que permite la conectividad punto-a-punto y que posibilita el acceso desde los clientes a la red del proveedor de servicio para poder acceder a los servicios que este oferta. De esta forma se instanciaría un servicio E-Line por cada asociación entre usuario-servicio.
Las E-Line son la sustitución natural de las líneas dedicadas que se ofrecen actualmente mediante otras tecnologías para la conexión entre usuarios. Por lo tanto se instanciarían tantos servicios E-Line como pares de usuarios. Esto permitirá, por ejemplo, la interconexión entre distintas sedes de una empresa geográficamente dispersas.
Como se puede comprobar, el problema de las E-Line viene cuando el número de pares crece, ya que cada E-Line es una instancia que se debe reservar y gestionar. Para solucionar esta posible limitación en cuanto al escalado y facilitar la gestión se define el servicio E-LAN, permitiendo mejorar el uso de los recursos en tráfico multipunto-multipunto. E-LAN interconecta mediante una única instancia múltiples puntos de entrada a la red de proveedor.
No siempre es posible la sustitución de varias instancias E-Line por una única instancia E-LAN, pero el caso de interconexión entre múltiples sedes remotas de una empresa recoge perfectamente las ventajas de esta nueva definición. Otro de los servicios que puede encontrar grandes ventajas en las E-LAN es el servicio de video en modo difusión, mientras que el video bajo demanda requiere flujos independientes para cada cliente y no podría aprovechar dichas ventajas.

Uno de los aspectos más importantes a tener en cuenta por el hecho de tratarse de una red formada exclusivamente por conmutadores de nivel dos, es precisamente cuales van a ser los procedimientos de reenvío empleados.
La sencillez característica de Ethernet hace imposible diferenciar a nivel dos el tráfico que desde un origen se manda a un destino. Mediante el identificador de VLAN (VID) se permite identificar un determinado flujo dentro de una comunicación entre un mismo origen y destino. Con el fin de explotar esta capacidad se define el procedimiento IVL, permitiendo independizar procedimientos de reenvío en base a VLANs.
Otro aspecto a tener en cuenta será cuales van a ser los procedimientos por los que se van a rellenar las tablas de conmutación. Tradicionalmente se delega dicha labor en protocolos como STP que asegura la eliminación de bucles dentro de la red. Con la aparición de las VLANs, STP evolucionó permitiendo separar instancias de dicho protocolo por cada VID dando origen a MSTP. MSTP depende del empleo de tablas de reenvío que introduzcan el VID como parámetro por lo que depende del uso de IVL.
Todo esto es de gran ayuda como base para lograr que el modelo presentado tenga viabilidad. Sin embargo, existe una vertiente como procedimiento de rellenado de las tablas de reenvío que aporta todavía más flexibilidad al sistema. Se trata de un mecanismo que permite mediante labores de gestión y control rellenar de forma determinista las tablas. En este caso también se permite el uso en conmutadores con soporte IVL, lo que aumenta todavía más la granularidad del sistema.
Finalmente, y mediante el uso combinado de MSTP y el modo determinista (que IVL permite), se está en posesión de las herramientas necesarias para abordar la misión de dar respuesta al modelo orientado a servicios basado exclusivamente en tecnología Ethernet.

4. Autenticación del acceso a la red

Uno de los aspectos más importantes en todo sistema de comunicaciones es la seguridad, siendo éste un concepto muy amplio. En este apartado se van a tratar temas relacionados con la autenticación de los usuarios que acceden al sistema, más concretamente se van a mostrar algunos de los resultados que este grupo de investigación ha obtenido de su trabajo en el proyecto PlaNetS (Eureka Medea+).

Primeramente, se van a introducir una serie de conceptos relacionados con la autenticación que conviene tener en cuenta. Al hablar de autenticación en el acceso en sentido amplio se entiende la capacidad de la red de controlar el acceso a la misma únicamente por usuarios autorizados, pero esto incluye diversos aspectos.
Por una parte hay que distinguir entre dos conceptos relacionados pero cada uno con entidad propia, autorización y autenticación. La autenticación es el proceso por el cual un proveedor comprueba que un usuario es quien dice ser mediante el uso de un identificador y unas credenciales que sólo podría poseer ese usuario. Sin embargo, la autorización es el proceso por el cual una entidad permite o no a otra el acceso. Una vez autenticado, el proveedor autorizará (o no) al usuario a acceder a la red del proveedor en función del acuerdo alcanzado entre ambos, para ello tendrá que comprobar el tipo de contrato que el cliente tiene suscrito con él (crédito disponible en sistemas prepago, tarifa plana…). Además será importante tener en cuenta el SLA para aplicar las políticas de QoS adecuadas a cada uno.
Para llevar a cabo esto hay dos factores íntimamente relacionados e igualmente importantes que hay que tener en cuenta, que son la identificación de flujos y el control de acceso. La capacidad de identificar diferentes flujos permite al proveedor aplicar distintas políticas de seguridad y de QoS a los

diferentes servicios a los que el usuario acceda en el marco multiservicio en el que se define. El control de acceso es la capacidad de dejar pasar o limitar el acceso del tráfico que proviene desde el cliente. En un marco en el que se permita la identificación de flujos, el control de acceso podría llegar a aplicarse independientemente por cada uno de los flujos.

Volviendo a retomar el modelo presentado en el apartado anterior, se trata de un entorno multiproveedor y multiservicio en el que el acceso a la red lo proporciona una entidad y los servicios los proporcionan otra serie de entidades que en principio no tienen relación con este. Teniendo esto en mente se produce una cierta disociación de funciones, el encargado de llevar a cabo el control de acceso y de aplicar las políticas de seguridad no es el mismo que el que tiene la capacidad de determinar si un usuario está autorizado o no a acceder a un servicio. El proveedor de acceso debería de aplicar las políticas de control de acceso, mientras que el proveedor de servicio es el que conoce las credenciales que aportan los clientes para acceder a los servicios.
Aplicar el control de acceso a los diferentes servicios en el propio proveedor de servicios es una opción que permitiría a los usuarios no autorizados acceder a recursos de la red (recursos como capacidad de transmisión, reserva en el equipamiento de conmutación…). Esto haría a la red enormemente vulnerable frente a ataques promovidos desde usuarios con intenciones maliciosas, ataques principalmente de denegación de servicio. Además, no se podrían aplican de antemano políticas de QoS sin saber que tipo de usuario es el que accede y a que servicio lo hace, ya que la reserva de recursos se tiene que hacer desde la entrada a la red y no una vez que ya se tiene acceso hasta el servicio.
Por otra parte, delegar en el proveedor de acceso la capacidad de autorización implicaría que todos los proveedores de servicios tendrían que hacer accesibles todas las credenciales de sus clientes a todos los proveedores de acceso, hecho que no sólo reduciría enormemente la capacidad de escalado y flexibilidad del sistema sino que disminuiría la seguridad del mismo e incluso atentaría contra la privacidad.

Lo que se pretende conseguir finalmente es un modelo de autenticación que permita autenticar de forma independiente cada uno de los servicios a los que un cliente accede, y que previamente ha contratado, sin que ello suponga la utilización de los recursos del proveedor de acceso antes de que se autorice su acceso.
Además, antes de presentar una solución al problema es importante tener presente que toda la red basa su funcionamiento en Ethernet como tecnología tanto de acceso como de transporte.

Dejando de lado el factor de que se trata de un modelo orientado a servicios, una red construida sobre tecnología Ethernet que ofrece conectividad a los usuarios resuelve mediante el estándar IEEE 802.1X la problemática referente a la autenticación (autenticación, autorización y control de acceso). Por lo tanto, es razonable el pensar en IEEE 802.1X como solución al modelo que incluye como finalidad de la conectividad a los servicios. Por desgracia dicho estándar fue creado para resolver el primero de los escenarios y presenta ciertas limitaciones para su aplicación directa en el modelo planteado.
La principal diferencia entre ambos escenarios es el número de autenticaciones necesarias, factor que condiciona enormemente el diseño de la solución. En el caso para el que fue diseñado el IEEE 802.1X se contempla una única necesidad de autenticación, la de la conectividad a la red. En ese caso, un usuario tendrá que identificarse y presentar unas credenciales para lograr el acceso a la totalidad de los recursos de la red a los que ese determinado perfil de usuario le permita. Dos son las posibles opciones resultantes del proceso de autenticación, se posee pleno acceso a la red o se limita completamente el mismo.
En el caso del modelo orientado a servicios se pretende llevar a cabo una autenticación por cada servicio a los que un mismo usuario quiera acceder. La restricción que esto impone es el hecho de poder diferenciar cada uno de los procesos de autenticación que se inicien. La mala noticia es que IEEE 802.1X no permite realizar dicha diferenciación puesto que en sus especificaciones no se requería dicha característica, la red era el único recurso a autenticar.

IEEE 802.1X es un estándar enormemente modular y con un muy buen diseño, el cual tiene como única pega el no permitir múltiples autenticaciones a un mismo usuario. El estándar define tres partes a las cuales denomina: suplicante, autenticador y servidor de autenticación. El suplicante es el cliente que quiere acceder a la red, el autenticador es el encargado de controlar el acceso a la red y el servidor de autenticación es el que conoce las credenciales del cliente y le indica al autenticador si le debe dejar acceder a la red o no.
El protocolo que encapsula los datos del proceso de autenticación entre el suplicante y el autenticador es EAP (Extensible Authentication Protocol). EAP es un protocolo muy flexible puesto que permite el intercambio de la autenticación pero no limita el tipo de autenticación empleada en el proceso. Para llevar este protocolo sobre Ethernet se hace uso de EAPOL (EAP over LAN).
En el caso de la comunicación entre el autenticador y el servidor de autenticación se emplea un protocolo diferente como RADIUS o DIAMETER, por lo que el autenticador hace de traductor entre el suplicante y el servidor de autenticación. Además, el resultado del intercambio realizado termina con un

envío de autorización o denegación del acceso, desde el servidor de autenticación al autenticador. En función de esa información el autenticador procede a aplicar el control de acceso correspondiente.
Una función interesante de los servidores de autenticación es la capacidad que tienen de realizar consultas a otros servidores de autenticación si no conocen las credenciales de un determinado cliente (proxy), permitiendo el diseño de sistemas con una gran escalabilidad.

Ante el reto que se plantea y con las características tan ventajosas que aporta IEEE 802.1X, sería una lástima no poder hacer uso de las mismas. Es por ello que una vez conocidas las limitaciones que presenta se opte por intentar adaptar el estándar a los requerimientos impuestos. Como ya se ha descrito, el problema surge de la incapacidad tanto de EAP como de EAPOL de discriminar diferentes procesos de autenticación que tienen como origen un mismo suplicante. Las diversas soluciones propuestas sobre las que se están trabajando tienen como denominador común la inclusión de un parámetro que permita distinguirlas, cuál es este parámetro y cómo se utiliza sería lo que las diferencia. De esta forma el autenticador podrá tratarlas independientemente y aplicar distintas políticas de control de acceso en cada caso.
Para poder aplicar políticas de control de acceso individuales a cada una de las comunicaciones entre un mismo cliente y los diferentes servicios a los que accede, es necesario retomar uno de los conceptos que se han introducido con anterioridad, la identificación de flujos. Esta capacidad permitirá al encargado de realizar el control de acceso, en este caso el autenticador, discriminar entre los diferentes servicios para dejar pasar a aquellos que están autorizados.
Una consecuencia de trabajar con un modelo basado exclusivamente en Ethernet hace que la diferenciación de flujos se tenga que realizar a ese nivel, desechando posibles discriminaciones a nivel superior. Según el modelo planteado, una opción para distinguir el acceso desde un mismo cliente a los diversos servicios contratados puede ser el uso de la dirección MAC destino (la del proveedor de servicio), sin embargo es una solución un tanto rígida. Otra alternativa mucho más flexible, y acorde a lo que el concepto de flujo significa, es el empleo de VLANs o más concretamente, de los identificadores de VLANs (VID). Las VLANs permiten separar, identificar e incluso introducir aspectos de CoS (IEEE 802.1p).

En resumen, un usuario tratará de acceder al sistema para hacer uso de un servicio en el que previamente se ha dado de alta. En ese momento el sistema iniciará a través del autenticador el proceso de autenticación por el que identificará al usuario mediante una credencial que previamente (en el proceso de alta) le ha otorgado el proveedor de servicio. Una vez autenticado y autorizado por el proveedor de servicios (mediante proxy), el proveedor de acceso iniciará un proceso para la reserva de recursos entre el usuario y el servicio en base a una determinada QoS acordada. Antes de hacer la reserva comprobará la disponibilidad de los mismos. Una vez hecho esto, el autenticador aplicará una política de control de acceso a un determinado flujo de datos. Ese flujo será el que haga uso de los recursos reservados.

Un aspecto a determinar dentro del esquema propuesto es el punto en el que se realiza el control de acceso. En el estándar IEEE 802.1X el autenticador se sitúa en el mismo segmento de LAN que el usuario, esto es debido a que para el intercambio de datos entre ambos (con EAPOL) se hace uso de direcciones MAC de grupo. Esta característica puede limitar el alcance de este tipo de tráfico, no siendo retransmitido por los posibles elementos intermedios que puedan aparecer. En principio el autenticador se situará en el nodo de acceso a la red del proveedor.

Una característica interesante que se hereda del diseño modular y escalable de IEEE 802.1X es la capacidad inherente de soportar el nomadismo. Esta capacidad hace referencia al hecho por el cual la capacidad de un cliente de acceder a un servicio que ha contratado no depende de su localización, sino única y exclusivamente de sus credenciales. De esta forma un usuario podría cambiar de casa e incluso de proveedor de acceso, y eso no limitaría su capacidad de acceder a ese servicio previamente contratado.

Otro aspecto importante, y que ya se ha comentado antes brevemente, es la mejora en cuanto a la seguridad global del sistema. Tal y como se especifica, los recursos de la red del proveedor sólo se reservan y se utilizan por flujos de tráfico que previamente han sido autenticados y autorizados, y que van exclusivamente desde un cliente a su proveedor de servicios.

5. Servicios

Este apartado se dedica exclusivamente a los servicios debido a que es el fin último de toda comunicación, y en este caso también lo es de la finalidad del modelo. El modelo está orientado a ofrecer los servicios de múltiples proveedores de servicios a través de múltiples proveedores de acceso, y todo ello a través de Ethernet. En este caso el concepto de servicio es algo muy amplio que identifica un fin por el cual un usuario desea acceder a la red, y que posee ciertas características propias en cuanto a requerimientos que tráfico. A continuación se van a mostrar alguno de los ejemplos más representativos de lo que puede ser un servicio.

El servicio de voz es uno de los más conocidos por su larga tradición entre las operadoras. En este modelo el cliente accederá (después de haberse autenticado) a la red del proveedor de acceso, y éste transportará todo el flujo de la comunicación hasta el proveedor de servicio. Será a través de la red del proveedor de servicio donde se establecerá el enlace entre el llamante y el destinatario. El servicio de voz requiere el envío y recepción de datos en tiempo real con ciertas restricciones en cuanto a algunos parámetros de calidad (retraso, jitter…). Por lo general no requiere un gran ancho de banda.

El servicio de video es un servicio que está bastante de moda y que engloba a varios. Esta distinción interna es debida a que se puede diferenciar entre servicios como TV y video bajo demanda (VoD). Según el tipo de servicio las características del tráfico que viaja y los requerimientos que impone son distintos. Una gran diferencia es el hecho de que el servicio de TV puede ofrecerse perfectamente sobre una topología multipunto (como es el caso de las E-LAN), mientras que el video bajo demanda exige tráfico punto-punto entre cada usuario y servicio (usando E-Line). Todas ellas demandan un gran ancho de banda (especialmente el VoD) sobre todo comparándolo con el servicio de voz. Al igual que la voz, el video es tráfico en tiempo real y que requiere un bajo jitter, pero al cual no le afecta sustancialmente el tener un alto retraso, siempre y cuando este sea fijo.

Otro de los grandes conocidos es el servicio de datos o de Internet. Este tipo de servicio permite la interconexión a un gran número de recursos, de los cuales se puede esperar una cierta interactividad pero que no garantiza calidad en absoluto. Se suele denominar de best effort haciendo referencia a que la red te ofrece el mejor servicio que pueda, pero que no garantiza nada. Aspectos como el jitter son contemplados.
El modelo multiproveedor permite la existencia de múltiples ISP en una misma red, algo que no genera ningún tipo de problema ya que la red se basa exclusivamente en el nivel dos para el conmutado. Para que el usuario pueda acceder a Internet necesita que alguien le asigne una dirección IP, pudiendo ser IPv4 o IPv6 de forma totalmente independiente puesto que la red del proveedor de acceso permitirá la coexistencia de distintos esquemas de direccionamiento. La asignación de la dirección IP vendrá por parte del ISP y se realizará como paso final del proceso de autenticación.

Uno de los grandes servicios que se está promoviendo desde el MEF es la creación de VPNs para la interconexión de múltiples sedes remotas de una empresa, explotando para ello el uso de las ventajas que ofrece Ethernet para la gestión multipunto. La creación de multipunto-multipunto se consigue mediante la instancia de un único servicio denominado E-LAN, mientras que en el caso de enlaces punto-punto para conseguir una VPN entre dos sedes se hará uso una instancia E-Line.

Se define un nuevo servicio denominado E2E (extremo a extremo) que permite la conexión de dos o más usuarios finales. La diferencia con el servicio anterior nace del hecho de que una VPN permite la interconexión de dos redes privadas, mientras que en este caso la comunicación se limita a un flujo de datos que viaja de un equipo final a otro. Además, en E2E se presupone un fundamento más dinámico en cuanto al establecimiento de las asociaciones, algo que confronta directamente con una cualidad más estático de los enlaces VPN.
Para lograr establecer una conectividad extremo a extremo entre dos usuarios con un modelo multiproveedor en el que todo usuario puede acceder a la red desde cualquier punto de la misma (sólo necesita presentar unas credenciales) no es algo que se consiga de forma inmediata. En este caso se define un nuevo servicio encargado de hacer corresponder la identidad de un usuario con su localización dentro de la red del proveedor.
Para hacer uso del E2E el usuario tendrá que autenticarse en el sistema, registrar su localización y solicitarle con quién quiere establecer la comunicación. Una vez hecho esto, el servicio comprobará si el destinatario acepta la comunicación y procederá a indicar al primero en donde puede encontrar su entidad par.

El siguiente servicio que se va a presentar es el resultado del trabajo realizado por este grupo de investigación en el ámbito del proyecto EthSec (MCyT TIC2003-09585-C02-01). El objetivo de dicho proyecto es la creación de un nuevo servicio de cifrado de Ethernet extremo a extremo, pudiendo éste pasar a formar parte del grupo de servicios ofertados por el modelo presentado con anterioridad. Otra posible aplicación de los resultados de EthSec es la de lograr securizar a nivel Ethernet el trafico que viaja por los servicios de VPNs que se han comentado con anterioridad.
Dentro del proyecto EthSec se probaron diversos prototipos que lograban cifrar los paquetes Ethernet en los que el formato de trama utilizado era compatible con el definido por el estándar IEEE 802.1ae (MacSec). La diferencia entre MacSec y EthSec radica en que MacSec pretende securizar el uso de un entorno de medio compartido mientras que EthSec es una especificación para securizar una comunicación extremo a extremo. Puesto que ambos securizan el mismo nivel (Ethernet) es lógico que compartan el formato de trama. Las mayores implicaciones a la hora de implementar uno y otro se derivan de los procedimientos que siguen cada uno para lograr las claves de cifrado necesarias y como éstas se emplean posteriormente.
A lo largo del proyecto se han creado varios prototipos que se pueden diferenciar entre los que están basados en sistema operativo y los que se desarrollaron directamente sobre plataformas

hardware (FPGA Virtex-4). Dentro de los que presentan sistema operativo se pueden distinguir dos plataformas: una plataforma PC con sistema operativo Linux, y otra plataforma con PowerPC y módulos de aceleración hardware diseñados también con sistema operativo Linux.

Partiendo de la plataforma PC con Linux se lograron dos modos de funcionamiento. Primeramente se diseñaron bridges cifrantes capaces de establecer comunicaciones con otros bridges cifrantes para crear túneles Ethernet seguros entre ellos. Estos bridges permitían gestionar múltiples conexiones seguras independientes identificadas por el par origen-destino. Para ello se hacia uso del módulo de ebtables y de librerías de cifrado. Este modo de funcionamiento podría servir para dar respuesta a las VPNs seguras a nivel Ethernet.

Una vez probados los bridges, se modifico el diseño para adaptarlo a un modo de funcionamiento extremo a extremo entre dos pares. En este caso también se hizo uso del módulo de ebtables y de las mismas librerías de cifrado. El formato de trama en ambos casos era idéntico.

El paso a la plataforma con el PowerPC no fue ningún problema puesto que esta también estaba controlada por un sistema operativo Linux, por lo que la transición fue inmediata. En este caso se trato de buscar un mayor rendimiento mediante el paso de las funciones criptográficas a rutinas diseñadas sobre el hardware de la plataforma.

El último paso fue el de diseñar un sistema de cifrado de Ethernet totalmente hardware sobre FPGAs (en concreto Virtex-4). El reto en este punto fue el de prescindir de un sistema operativo para diseñar completamente a nivel hardware la solución.

6. Conclusiones

Como conclusión del trabajo es importante destacar el modelo orientado a servicios que aquí se presenta, y que permite dibujar un escenario multiproveedor y multiservicio, en donde el servicio se define como el fin de la comunicación iniciada por el usuario. En este escenario el usuario podrá hacer uso de múltiples proveedores de acceso para lograr la conectividad a los múltiples servicios ofertados de forma que una elección no limite la otra.

En este modelo el proveedor juega un papel importantísimo al tener que garantizar un determinado nivel de calidad, hecho que permitirá ofrecer servicios de forma adecuada a los clientes. El mantenimiento de las SLA por parte del proveedor se fundamentará en su capacidad para dimensionar adecuadamente la red, establecer reservas de recursos, identificar los distintos flujos de datos y aplicar políticas de control de acceso.

Otro aspecto importante a destacar es el empleo de Ethernet como única tecnología de red, permitiendo recoger aquí el estado del arte actual de su utilización en redes de acceso y de transporte. También se han recogido ciertas limitaciones que se derivan de su uso y algunas de las soluciones que se están proponiendo actualmente para paliarlas.

Una vez definido el modelo se ha presentado la solución en la que actualmente se está trabajando en el PlaNetS para llevar a cabo las labores de autenticación, autorización y control de acceso que tan necesarias son desde el punto de vista de un proveedor. También se han presentado ciertas restricciones que se imponen como el hecho de que se lance un proceso de autenticación por cada servicio al que se quiera acceder.

Finalmente se han presentado algunos de los servicios más importantes a los que el sistema daría un acceso con calidad garantizada. Entre ellos se encuentran servicios tan comunes como voz, video, VPNs o Internet. Destacar el servicio de seguridad extremo a extremo en el que se ha trabajado en el marco del proyecto EthSec.

Agradecimientos

Este trabajo está siendo realizado por el grupo de Investigación e Ingeniería Telemática (I2T) de la Universidad del País Vasco (UPV/EHU), dentro del ámbito del proyecto PlaNetS (Eureka Medea+) y EthSec (MCyT TIC2003-09585-C02-01).

Referencias

[1] IEEE Std. 802.3ah-2004, “Ethernet in the First Mile,” 2004

[2] IEEE Std. 802.1ad, “Local and Metropolitan Area Networks, Virtual Bridged Local Area Networks: Provider Bridges,” 2006

[3] IEEE 802.1ah, “IEEE Draft Standard for Local and Metropolitan Area Networks, Virtual Bridged Local Area Networks, Amendment 6: Provider Backbone Bridges.”

[4] ITU-T Rec. G.8011.1/Y.1307.1, “Ethernet Private Line Services,” Apr. 2004

[5] Metro Ethernet Forum, “Ethernet Service Attributes – Phase 1,” MEF 10, Nov. 2004

[6] ITU-T Draft Rec. Y.17ethoam (Y.1731), “OAM Functions and Mechanisms for Ethernet Based Networks.”

[7] IEEE Draft Std. 802.1ag, “Local and Metropolitan Area Networks, Virtual Bridged Local Area Networks, Amendment 5: Connectivity Fault Management”

[8] Aref Meddeb, “Why Ethernet WAN Transport?” IEEE Communications Magazine, Nov 2005, pp. 136-141

[9] David Allan et al., “Ethernet as Carrier Transport Infrastructure” IEEE Communications Magazine, Feb 2006, pp. 134-140

[10] Lothar Zier et al., “Ethernet-Based Public Communication Services : Challenge and Opportunity ” IEEE Communications Magazine, March 2004, pp. 88-95

[11] Mike McFarland et al., “Ethernet OAM : Key Enabler for Carrier Class Metro Ethernet Services ” IEEE Communications Magazine, Nov 2005, pp. 152-157