Establecimiento dinámico de conexiones sobre PBT

Jon Matias, Eduardo Jacob, Mariví Higuero, Jasone Astorga

Dpto. de Electrónica y Telecomunicaciones. Universidad del País Vasco (UPV/EHU)
ETSI de Bilbao. Alda. Urquijo S/N, 48013 Bilbao
Teléfono: 94 601 7370 Fax: 94 601 4259
E-mail: {jon.matias, eduardo.jacob, marivi.higuero, jasone.astorga}@ehu.es

***Abstract* — Las redes de nueva generación tienen un nuevo exponente con la aparición de la tecnología PBT (IEEE 802.1Qay), convirtiendo en realidad una solución de red de transporte basada en Ethernet con calidad de proveedor. Varias han sido las aportaciones que desde los diferentes organismos de estandarización (como IEEE o ITU-T) se han introducido persiguiendo este objetivo. Sin embargo, pese a que responde de forma adecuada a gran parte de las necesidades que un proveedor de conectividad puede requerir, existe un cierto grado de indeterminación para dar respuesta a entornos que puedan demandar un establecimiento dinámico y efímero de conexiones, como es el caso del acceso a servicios. Es en este escenario en el que se presenta una aportación basada en la extensión del protocolo 802.1X (EAPOL-in-EAPOL) para establecer un contexto en el que se dispone de todo lo necesario para poder llegar a establecer dichas conexiones mediante la toma de decisiones a nivel de gestión.**

I. Introducción

Los proveedores de servicios de conectividad han experimentado una gran evolución desde su aparición, logrando siempre adaptarse y dar respuesta a las necesidades que les iban surgiendo a sus clientes. Dichas necesidades han evolucionado a lo largo de los años, sobre todo en disponibilidad y capacidad, pero podrían agruparse en dos grandes vertientes de negocio para dichos proveedores: la conectividad entre sedes dispersas geográficamente y el acceso a servicios, entendiendo servicio en su sentido más amplio (voz, video, datos), como una prestación operada y proporcionada por un tercero.

Cada vez es más común la necesidad de conectar sedes localizadas en puntos geográficamente dispersos (incluso para las PyME), apareciendo la figura del proveedor de conectividad que pone su red a disposición de la empresa para interconectar sus sedes a cambio de una inversión económica asumible. Las conexiones privadas mediante líneas dedicadas punto a punto entre las sedes (e.g. Frame Relay) fueron solución hasta la aparición de alternativas más económicas como son las redes privadas virtuales (e.g. ATM, SONET/SDH, DWDM). El otro gran negocio es dar a los clientes acceso a servicios proporcionados por terceras entidades, en donde aparece la figura del proveedor de servicios, el cual genera o revende contenidos en formato digital: voz, video o datos. En este caso, el reto para el proveedor de conectividad es garantizar unas determinadas condiciones de calidad en el acceso desde cliente a los servicios, y todo ello de una forma eficaz y a precios competitivos. Históricamente se han empleado redes diferentes en función del servicio, el tipo de acceso y la calidad demandada: telefonía, TV o acceso a redes de datos como Internet. El uso de redes específicas ha limitado la competencia transversal entre servicios, sin embargo, este marco ha cambiado con la aparición del concepto de convergencia de redes.

La convergencia es la piedra angular de las redes de nueva generación (NGN). Este tipo de red es capaz de aunar esfuerzos, inversiones y gestión para afrontar con éxito y a precios competitivos todas las necesidades actuales y futuras de los clientes, que mínimo abarcarán todo lo expuesto. Además, tendrá que servir como unión entre múltiples tecnologías de acceso y responder adecuadamente a escenarios de nomadismo y movilidad. Muchas son las iniciativas que giran en torno a NGN tanto a nivel de estandarización como proyectos de investigación. En el presente artículo se presenta la tecnología PBT (Provider Backbone Transport, conocida como Carrier Grade Ethernet Transport), culminación del trabajo que durante los últimos años se ha realizado desde IEEE y ITU-T para dotar de calidad de proveedor a la tecnología Ethernet.

II. Provider Backbone Transport (PBT)

Las NGN tienen el reto de converger en una misma red de forma simultánea servicios basados tanto en la conmutación de circuitos como de paquetes. La tecnología IP apoyada en IP/MPLS ha sido considerada como opción. Sin embargo, Ethernet ha ganado adeptos como alternativa fiable y con ciertas mejoras. Como presentación el 95% del tráfico empieza o termina en Ethernet, sin olvidar su ubicuidad, sencillez, soporte natural de servicios IP o bajo coste. No obstante, Ethernet necesita mejorar algunas de sus limitaciones como tecnología de proveedor antes de poder dar el salto a las redes MAN y WAN.

Como proveedor Ethernet puede ser interfaz (RJ45, SFP, XFP), servicio o tecnología de transporte. Como servicio (e.g. E-Line, E-LAN o E-Tree) ofrece la entrega fiable de paquetes Ethernet en interfaces UNI, pudiendo emplear Ethernet sobre SONET/SDH o sobre MPLS como capa de transporte. Por lo tanto, Ethernet como tecnología de transporte trata de emplear Ethernet de forma nativa como capa de convergencia para NGN. Cinco son los requisitos impuestos Ethernet como tecnología de proveedor: servicios estandarizados, calidad de servicio, escalabilidad, fiabilidad y modo estandarizado para monitorizar, diagnosticar y gestionar la red. PBT es una tecnología que se apoya en varias de las mejoras introducidas en este sentido al estándar original de Ethernet tanto desde IEEE como ITU-T, y que se van a introducir a continuación.

A. Mejoras de Ethernet como tecnología de proveedor

Ethernet fue diseñado para dar un acceso equitativo a la red y requerir una implementación mínima en repetidores y conmutadores haciendo uso de un direccionamiento plano. Válido en entornos LAN, no es aceptable en entornos de proveedor siendo necesario diferenciar servicios y dividir la red para cada usuario. Esto también es interesante a nivel LAN para diferenciar departamentos, originando IEEE 802.1Q [1], que permitía crear LANs virtuales (VLAN) identificas por el Q-tag de 12 bits y dividir la red de modo lógico. Sin embargo, esta misma necesidad apareció en el proveedor que daba servicio de conectividad a estas organizaciones, surgiendo IEEE 802.1ad [2] (PB o Q-in-Q) que encapsula el Q-tag cliente (C-VID) en uno nuevo de servicio (S-VID), y lo dotaba de jerarquía al independizarlos. STP se usa para evitar bucles en cada S-VLAN gracias a IVL (Independent VLAN Learning, 802.1Q), que dispone de una tabla MAC independiente por cada VLAN y aísla el direccionamiento cliente en a cada instancia de servicio (pero no al proveedor). Sin embargo, el tamaño del VID sólo permite 4094 instancias de servicio. Debido a estas limitaciones se desarrolló IEEE 802.1ah [3] (PBB o MAC-in-MAC) que consigue encapsular las tramas 802.1ad en una nueva cabecera Ethernet de proveedor. Para diferenciar clientes en vez de Q-tag se hace uso de un nuevo campo de servicio de 24 bits (I-SID) mucho más escalable. Ahora el reenvío depende de la nueva cabecera (B-DA, B-SA, B-VID) totalmente aislada del esquema de direccionamiento cliente, que aportan mayor escalabilidad. Aún así, sigue siendo una tecnología sin conexión, con inundación si desconoce la MAC destino, STP para evitar bucles y VID por red en vez de por puerto. Proveedores de Japón lo utilizan en la actualidad.

Pese a utilizarse en 802.1ad y 802.1ah, STP no es por definición un protocolo adecuado a entornos de proveedor, ya que se encarga de lograr una topología con el menor número de saltos libre de bucles, pudiendo converger en una situación que desperdicia una gran capacidad de la red de proveedor al coexistir ciertos enlaces congestionados con otros que no se utilizan. 802.1aq permite la definición del árbol desde cada nodo por el camino más corto, diferenciados mediante el VID.

El estándar IEEE 802.1AB [5] es un protocolo para el descubrimiento de la capa de enlace (LLDP) el cual permite a un dispositivo comunicar información propia a sus vecinos. El objetivo del anuncio de esta información no es otro que transmitirla hasta el sistema de gestión, lo que le permitirá conocer la topología de la red o identificar los conectados.

Los protocolos OAM asisten a los operadores de red en su labor de monitorización de la misma y proporcionan operaciones de gestión y administración, siendo capaces de enviar mensajes automáticamente anunciando el estado de la red. El estándar IEEE 802.1ag [6] puede operar sobre cada instancia de servicio de forma independiente y gestiona fallos en redes Ethernet de proveedor permitiendo la detección (mensajes CCM de continuidad), verificación (mensajes LoopBack LBM-LBR al extremo remoto) y aislamiento (mensajes LinkTrace LTM-LTR salto a salto) de errores.

En definitiva, una solución basada en IEEE 802.1ah posee ciertas ventajas como tecnología de proveedor ya que existe una diferenciación marcada entre la red de cliente y de proveedor con una cabecera MAC independiente en cada ámbito, dotando de una gran seguridad al sistema. Además, las operaciones de gestión se simplifican al evitar posibles conflictos de MAC o identificadores VLAN, y es una solución más robusta al aislarse de envíos broadcast y bucles de la red cliente.

B. IEEE 802.1Qay [4]

Provider Backbone Transport (PBT) es una combinación de extensiones de Ethernet creadas con el objetivo de dotar de capacidad de proveedor a una tecnología nacida para los entornos LAN. PBT se corresponde con el estándar IEEE 802.1Qay y está basado principalmente en 802.1Q, 802.1AB, 802.1ad, 802.1ah y 802.1ag (todos ellos introducidos con anterioridad).

Uno de los requisitos para que Ethernet se pueda utilizar como tecnología de transporte en redes de proveedor es la implementación de funcionalidades OAM. Varios son los estándares desarrollados en este sentido que PBT puede utilizar, como son IEEE 802.1ag (señalización proactiva de fallos en el servicio), IEEE 802.3ah (define el uso de Ethernet en la primera milla), IEEE 802.1AB (permite el descubrimiento de la topología), ITU-T G.8031 (protección de Ethernet), ITU-T Y.1731 [7] (capacidades adicionales a 802.1ag) y la definición para la monitorización de rendimiento de Ethernet del MEF.

Otro concepto que aparece en PBT es la ingeniería de tráfico, únicamente posible en Ethernet gracias a la supresión de mecanismos tan extendidos como el de inundación, broadcast, multicast o el aprendizaje de MAC, ignorando además los estados STP asociados a cada puerto. Al deshabilitar estas funciones, el sistema de gestión PBT se convierte en responsable de rellenar las tablas de reenvío de los dispositivos de nivel 2. Para simplificar el proceso, la propia red se encarga a través de 802.1AB de indicar al sistema gestor el aspecto de la misma, haciendo más sencillo el proceso de añadir o quitar nodos.

Haciendo uso de PBT es posible el establecimiento de un camino activo y otro camino de respaldo sobre una red basada en Ethernet (Fig. 1), reservando el ancho de banda apropiado para soportar las métricas de QoS que permitan garantizar la SLA subscrita por el cliente (sin necesidad de sobredimensionamiento). Por tanto, será un proceso de la capa de gestión de la red el que permita crear esos túneles PBT logrando la emulación de servicios orientados a conexión. Por lo tanto, el sistema de reenvío de paquetes se sustenta sobre caminos a través de la red previamente establecidos de forma explícita, sobre los cuales se enviarán mensajes de comprobación de continuidad (CCM) definidos por 802.1ag. En caso de la detección de un fallo, el sistema conmutará al camino alternativo (también previamente establecido) en menos de 50 ms sin más que cambiar en los extremos el identificador de VLAN empleado, fundamento en el que se basa el reenvío.

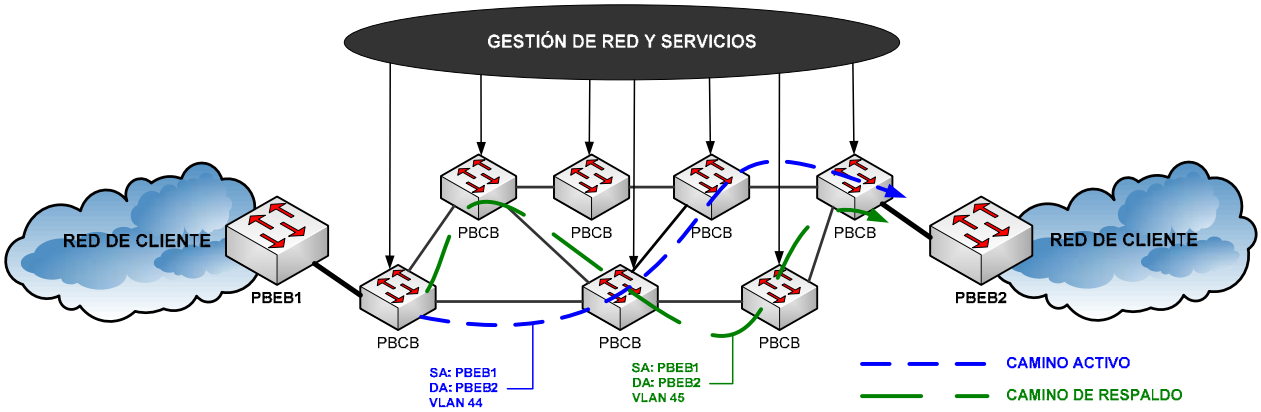

Fig. 1. Configuración de camino activo y de respaldo con PBT.

PBT es un sistema que consigue un comportamiento orientado a conexión en una red de conmutación de paquetes, el cual explota las características del motor de reenvío de los conmutadores basado en las mejoras introducidas por IVL, que permite la toma de decisión de reenvío en función de 60 bits (VID + MAC destino). Esto dota de gran capacidad al sistema de gestión de la red para realizar ingeniería de tráfico, pudiendo especificar desde el plano de gestión el contenido de dichas tablas de decisión. Destacar que los VID en PBT tienen un alcance local (global en las LAN), pudiendo ser reutilizados.

El estándar 802.1Qay utiliza el mismo formato de trama (Fig. 2) que PBB (802.1ah) con una diferencia en el significado de los campos que la componen. En el caso de PBT el B-VID y la MAC destino (B-DA) forman un identificador único con sentido global. El B-VID será el que permita diferenciar caminos entre un mismo origen y destino en la red del proveedor.

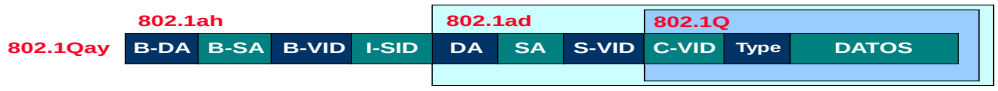

Fig. 2. Formato de trama de PBT (802.1Qay)

En PBT hay que diferenciar tanto en función como capacidades entre conmutadores frontera (Provider Backbone Edge Bridge) y de núcleo (Provider Backbone Core Bridge). Los PBEB se encargarán de realizar en encapsulado MAC-in-MAC de las tramas que llegan de entornos 802.1ad, y asociarlos a una instancia servicio dentro de PBT. Por su parte, los nodos PBCB serán más sencillos, con un funcionamiento similar a los actuales con soporte IVL (deshabilitando ciertas funcionalidades) permitiendo un establecimiento determinista de la tabla de reenvío en la que basan sus decisiones.

III. Creación Dinámica de Caminos PBT Basada en 802.1X

Al inicio se han presentado los dos grandes negocios de proveedores de conectividad. PBT al tener una esencia de asociación más o menos estable a lo largo del tiempo sólo responde a la conectividad entre sedes geográficamente dispersas. En este apartado se va a tratar de cubrir el otro negocio, cada vez con mayor peso al incrementar los servicios ofrecidos debido a la convergencia. Ya no se trata sólo de dar conectividad a Internet, se está hablando de TV, video bajo demanda o conexiones de voz. Este escenario presenta algunas particularidades, como el dinamismo, que lo hacen diferenciarse de los requisitos impuestos a la solución de conectividad. En este caso, los clientes no acceden de forma simultánea ni estable en el tiempo a todos los servicios contratados, incluso la localización del acceso podrá variar (nomadicidad en las redes de proveedor). Esto hace que la creación de los caminos (servicio más reserva) sea variable en el tiempo, permitiendo la reutilización y reasignación de los recursos de la red para dar un servicio más adecuado y competitivo a todos los clientes.

Para poder dar respuesta a esta nueva situación se ha trabajado en el proceso de establecimiento de dichas conexiones asociándolo al proceso de autenticación que es siempre necesario para poder lograr el acceso al servicio en cuestión. Dicho proceso se basa en una modificación introducida sobre el estándar 802.1X que permite el establecimiento de múltiples sesiones simultáneas de procesos de autenticación, algo no soportado por el estándar pero que hace posible tener tanto un control granular por servicio como un desencadenante del proceso de creación (y liberación) de los caminos PBT necesarios para establecer una comunicación con calidad entre el cliente y el servicio prestado. El fundamento de la modificación introducida sobre 802.1X se basa en la creación de un nuevo tipo de mensaje EAPOL que permita encapsular una versión "identificada" del mismo (Fig. 3). Es decir, se trata de hacer encapsulación EAPOL-in-EAPOL logrando reutilizar el campo de tipo del protocolo para diferenciar cada una de las instancias de autenticación lanzadas desde un mismo cliente.

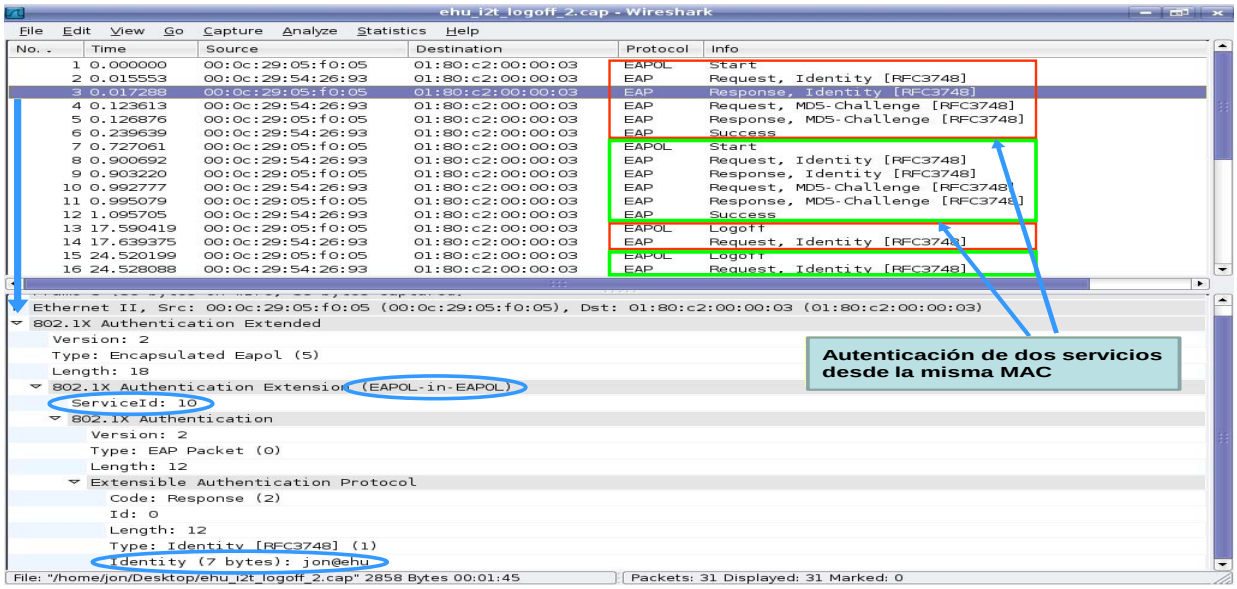

Fig. 3. EAPOL-in-EAPOL basado en 802.1X: múltiples autenticaciones simultáneas (captura wireshark).

El sistema final funcionaría de la siguiente forma (Fig. 4). Por una parte cada vez que un cliente quiera acceder a un nuevo servicio, servicio que podría identificarse a nivel Ethernet como un nuevo destino, se desencadenará una nueva instancia de proceso de autenticación que terminaría en la presentación de las credenciales del usuario en el servidor de autenticación del propio proveedor de servicio. Estas credenciales serán reenviadas mediante proxy desde el proveedor de conectividad, ya que éste no conoce las credenciales de los usuarios para los servicios prestados por dichas terceras partes. Este proceso, que ahora será por servicio, terminará con la aceptación por parte del proveedor de conectividad de una nueva regla en el control de acceso que permitirá el establecimiento de conexiones entre dicho cliente y el prestador de servicios, modificando 802.1X para aceptar paquetes con MAC origen cliente y destino del proveedor de servicios.

Todo ello proporciona un entorno en el cual se establece una asociación segura entre la información del nodo origen y del nodo destino, junto con parámetros adicionales de calidad que pueden ser fácilmente introducidos desde el servicio de autenticación que conoce tanto la identidad del cliente como la QoS asociada al servicio que tiene contratado. Lo que se ha hecho en este caso es relacionar dicho entorno con el proceso de gestión que permita el establecimiento dinámico de dichas conexiones bajo los parámetros de calidad impuestos por el servicio. En este caso es necesario hacer uso de las facilidades brindadas por el conjunto de estándares que componen PBT para poder crear bajo demanda dichas conexiones en función del estado actual de los enlaces entre los conmutadores que compongan finalmente el camino entre el origen y destino. La inteligencia vuelve a estar en manos del sistema de gestión que hará uso de los procedimientos brindados por PBT para el establecimiento y liberación de conexiones.

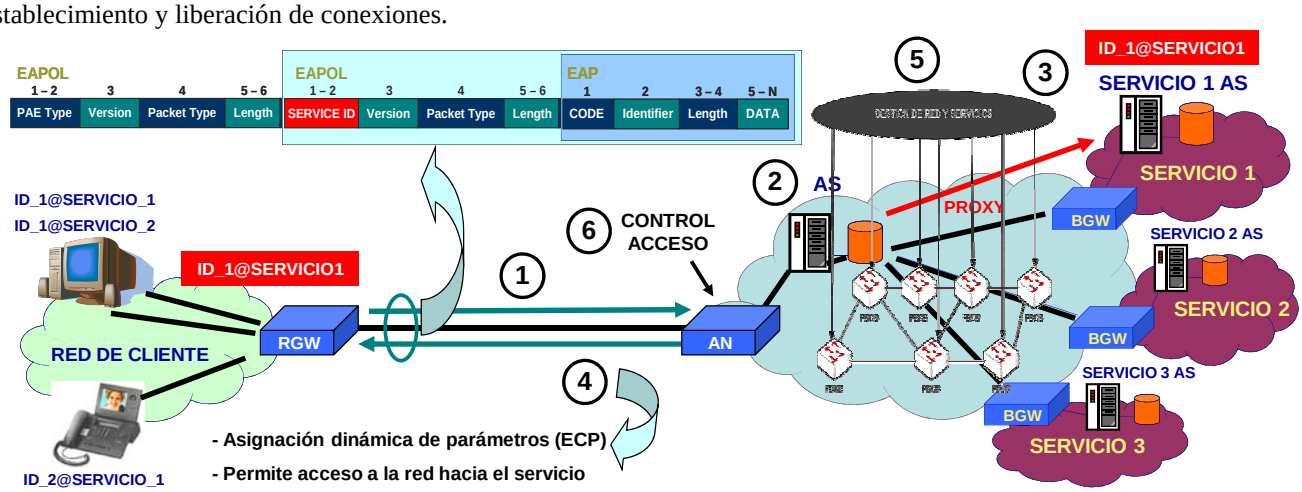

Fig. 4. Creación dinámica de caminos PBT basada en 802.1X.

IV. Conclusión

Muchos son los conceptos que están de moda hoy en día, como las redes de nueva generación, la convergencia, la ingeniería de tráfico o la calidad de servicio, pero detrás de todos ellos existe la figura del proveedor de conectividad que trata de dar respuesta a la necesidad de sus clientes de conectar sus redes y de poder acceder a los servicios que tenga

contratado. Todos estos conceptos tratan de prosperar hacia una solución más eficiente a un precio más competitivo y con una mayor simplicidad. En medio de todo ello aparece la tecnología Ethernet capaz a día de hoy de dar una respuesta adecuada a dichos requerimientos gracias a los últimos avances introducidos.

PBT nace como una respuesta de nueva generación basada en Ethernet capaz de lograr converger en una única red todas las necesidades de conectividad de un proveedor, con escalabilidad, sencillez de gestión, protección frente a fallos, soporte de calidad de servicio asociada a SLAs, y todo ello a precios muy competitivos. Una de las piezas claves para el éxito de la tecnología PBT es la capacidad de dotar de ingeniería de tráfico a Ethernet, esto es, ofrecer la capacidad para organizar el comportamiento de la red a través del sistema de gestión en función de decisiones de proveedor. Para ello se introduce el concepto de caminos Ethernet orientado a conexión, los cuales se logran gracias a la explotación de un sistema de reenvío basado en el identificador VLAN y la MAC destino.

Por último, se ha introducido un nuevo escenario al cual tendrá que hacer frente PBT para lograr realmente la tan ansiada convergencia, y no es otro que el del establecimiento dinámico bajo demanda del cliente de conexiones efímeras de una determinada QoS con el proveedor de servicio al que quiere acceder. Se ha introducido una solución basada en asociar dicho establecimiento al proceso de autenticación: ya que por una parte no se desaprovecharán recursos para el establecimiento de la conexión para que finalmente está no pueda llevarse a cabo por una falta de autorización, en donde incluso la QoS de la conexión puede depender de la identidad del cliente; y por otra parte es el escenario en el que confluyen cliente, proveedor de servicio y sistema gestión del proveedor de conectividad. El fundamento de dicha solución se sustenta sobre la arquitectura mostrada y una modificación del protocolo 802.1X a través de EAPOL-in-EAPOL.

REFERENCIAS

[1] IEEE Std. 802.1Q-REV, *Virtual Bridged Local Area Networks*, 2005
[2] IEEE Std. 802.1ad, *Virtual Bridged Local Area Networks: Provider Bridges*, 2006
[3] IEEE 802.1ah/D4.0, *Draft Standard, Virtual Bridged Local Area Networks: Provider Backbone Bridges*, 2008
[4] IEEE 802.1Qay/D3.0, *Draft Standard, Virtual Bridged Local Area Networks: Provider Backbone Bridge Traffic Engineering*, 2008
[5] IEEE Std. 802.1AB, *Station and Media Access Control Connectivity Discovery*, 2005
[6] IEEE Std. 802.1ag, *Virtual Bridged Local Area Networks – Connectivity Fault Management*, 2007
[7] ITU-T Y.1731, *OAM functions and mechanisms for Ethernet based networks*, 2006
[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] Nortel Networks, *Adding Scale, QoS and Operational Simplicity to Ethernet*, 2006 http://www.nortel.com/solutions/collateral/nn115500.pdf
[11] TPack, *PBT, Carrier Grade Ethernet Transport*, 2006 http://www.tpack.com/fileadmin/user_upload/Public_Attachment/PBT_WP_v2_web.pdf
[12] *PBT Networking*, http://staff.science.uva.nl/~delaat/sne-2006-2007/p34/report.pdf, 2007