Arturo Custodio Salvador
Responsable de Arquitectura y soluciones de red en Alcatel-Lucent España

Evolución del modelo de agregación en redes de banda ancha

La nueva oferta de servicios convergentes *Triple Play*, en los que se combinan aplicaciones de voz, datos y vídeo está obligando a los operadores a llevar a cabo una profunda transformación en sus redes para que sean capaces de absorber la mayor demanda de tráfico y hacerlo además de una manera más eficaz.

El modelo de red, conocido como PPPoE *(PPP over Ethernet)*, con despliegue de redes de acceso ADSL, basa su eficiencia en la naturaleza punto a punto de las comunicaciones entre el usuario y el servidor de acceso a Internet. Pues bien, ahora se plantea por qué no utilizar un modelo IPoE (*IP over Ethernet*), haciendo uso de tecnologías de acceso de más capacidad (ADSL2+, VDSL, fibra óptica) más sencillo y eficiente, en lugar de un modelo IP sobre PPPoE como el hasta ahora desplegado.

Hasta ahora, el concepto de servicio de banda ancha ha estado ligado casi exclusivamente al de acceso Internet a alta velocidad y, por ello, las redes de los operadores de telecomunicaciones se han diseñado para soportar este tipo de aplicación mediante el despliegue de redes ADSL como tecnología de acceso básica para el soporte de alta velocidad, haciendo extensivo el uso de la tecnología Ethernet como medio optimizado en el transporte del protocolo Internet (IP), y estableciendo el protocolo punto a punto (PPP) como mecanismo de control encargado de establecer, autorizar, configurar, monitorizar y terminar la sesiones de acceso a Internet de los usuarios. Este modelo de red, conocido como PPPoE *(PPP over Ethernet)* basa su eficiencia en la naturaleza punto a punto de las comunicaciones entre el usuario y el servidor de acceso a Internet.

"La respuesta a favor de este modelo IPoE es, efectivamente, la escogida por los operadores cuando han de plantear servicios de vídeo, ya que es óptima para proporcionar las comunicaciones multipunto-a-multipunto que el modelo PPPoE no es capaz de soportar"

Sin embargo, la irrupción en el mercado de los servicios convergentes, y en especial de la TV y el vídeo, ha cambiado dos variables importantes en este modelo de red: por un lado, el drástico aumento del ancho de banda debido a los servicios de vídeo en tiempo real, que está originando un movimiento hacia...) y, por otro, la naturaleza punto a multipunto de los servicios de difusión de TV que hace necesario un nuevo mecanismo de control de la comunicación, necesariamente distinto al PPP.

Vemos que, salvo el sustrato Ethernet (ampliamente consensuado como el transporte de datos IP más efectivo), las bases tecnológicas que han de soportar las aplica-

ciones *Triple Play* evolucionan hacia unos estándares de acceso y unos protocolos más modernos y convenientes. Precisamente, siendo Ethernet la capa de transporte básico para IP, ¿por qué no utilizar un modelo que directamente transporte la información IP sobre estas conexiones Ethernet? Esto es, ¿por qué no utilizar un modelo IPoE (*IP over Ethernet*), más sencillo y eficiente, en lugar de un modelo IP sobre PPPoE como el hasta ahora desplegado?

La respuesta a favor de este modelo IPoE es, efectivamente, la escogida por los operadores cuando han de plantear servicios de vídeo, ya que es óptima para proporcionar las comunicaciones multipunto-a-multipunto que el modelo PPPoE no es capaz de soportar.

Sin embargo, cuando se trata de construir un servicio punto a punto, como el servicio de acceso a Internet, se siguen manteniendo en algunos casos redes basadas en PPPoE. La razón, sin duda, se debe a la pura inercia de los operadores en mantener los modelos de red ya construidos, ya que no existe ninguna razón de peso que demuestre que el modelo PPPoE sea el más adecuado, a pesar incluso de la naturaleza punto a punto de este tipo de servicios.

Los defensores de un modelo PPPoE, además de la lógica baza de la reutilización de la red existente, suelen argumentar a su favor la capacidad del protocolo PPP de ejecutar los mecanismos que permiten realizar un control eficiente de la comunicación. Sin embargo, el modelo IPoE siempre puede complementarse (y de hecho así se hace) con un protocolo conocido y fiable como el DHCP -para la asignación dinámica de direcciones IP - que permite la ejecución de todos los mecanismos de establecimiento, autorización, configuración, mantenimiento y control de las comunicaciones, tan eficazmente como el protocolo PPP y, en muchas ocasiones, incluso mejor.

PPP *versus* DHCP

La disputa PPP *versus* DHCP como mecanismo de control para el servicio de acceso a Internet, muchas veces suscitada en foros tecnológicos, nace como consecuencia de estas consideraciones, pero conviene no olvidar que la verdadera raíz de la polémica se encuentra en la elección de un modelo basado en el protocolo PPPoE, con una arquitectura que centraliza el control del tráfico en un único punto de red (en el nodo de acceso a los servicios IP, conocido como BRAS) donde "terminan" todas las conexiones punto-a-punto de los usuarios, frente a un modelo de red con control de tráfico más distribuido, basado en IPoE y con apoyo del protocolo DHCP.

"El principal argumento que valida la opción PPP es, sin duda, la reutilización de las inversiones de red realizadas para el servicio de acceso a Internet"

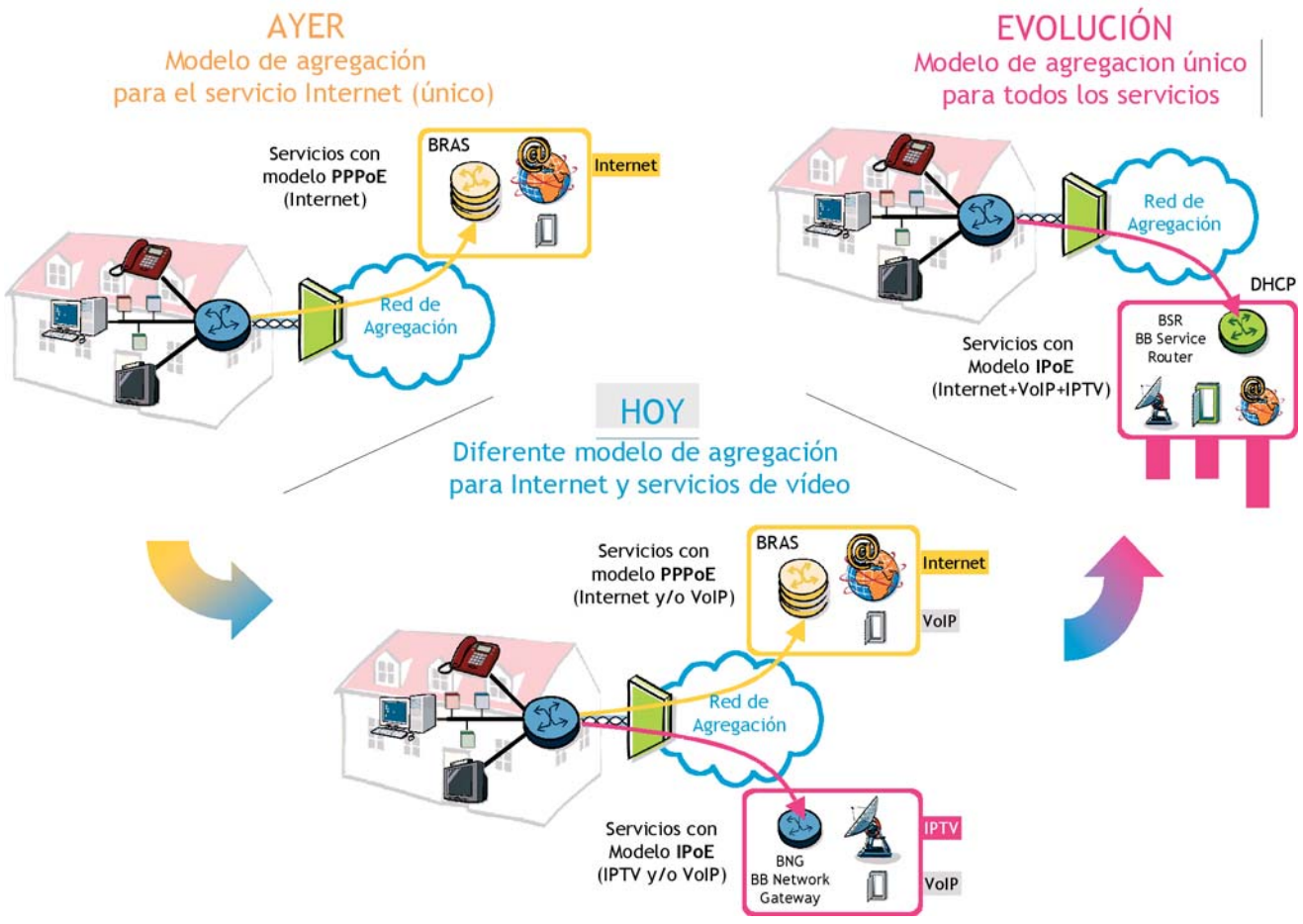
El principal argumento que valida la opción PPP es, sin duda, la reutilización de las inversiones de red realizadas para el servicio de acceso a Internet, mientras que la "opción DHCP" cuenta con la ventaja de permitir un modelo único de red tanto para el acceso a Internet como para el resto de servicios de vídeo y voz, facilitando la creación y control de aplicaciones realmente convergentes.

Al margen de estas notas diferenciadoras, ambos modelos son capaces de implementar los mecanismos de control de tráfico necesarios para el soporte de los servicios. A saber:

Identificación del usuario

En el modelo PPPoE, para identificar al usuario se utilizan, normalmente, los estándares IEEE 802.1Q y/o IEEE 802.1ad (*Q-in-Q*), según los cuales, en cada mensaje enviado por el usuario, el dispositivo de acceso inserta la identificación de la red privada virtual (VLAN) a la que pertenece (una VLAN por usuario), de manera que cada trama Ethernet se "etiqueta" de acuerdo a esta VLAN. La etiqueta puede ser simple (única por usuario) o doble (una por nodo de acceso más otra por usuario dentro de ese nodo). También es posible utilizar la función "*PPPoE intermediate agent*", por la que el nodo de acceso detecta el puerto físico por donde se establece la conexión, lo identifica e informa al nodo remoto de acceso a Internet (BRAS).

En el modelo IPoE con DHCP, también se pueden emplear los estándares IEEE 802.1Q y/o IEEE 802.1ad para el etiquetado VLAN de las tramas Ethernet; sin embargo, con el fin de permitir una mayor flexibilidad a la hora de definir las VLAN, por ejemplo para asignarlas a cada tipo de servicio en lugar de una por cada usuario,



Evolución del modelo de agregación en redes de banda ancha.

se suele utilizar un procedimiento estándar del protocolo DHCP según el cual, el nodo de acceso inserta en el primer mensaje DHCP (el de solicitud de una dirección IP), dentro de un campo conocido como "opción 82", la información del puerto físico que hace dicha petición, quedando el usuario, así, unívocamente identificado.

Autenticación y Autorización

El proceso PPP, incluye, dentro del flujo de mensajes de establecimiento de sesión, una parte dedicada a la autenticación (introducción de la identificación del usuario y la contraseña), que se implementa mediante los protocolos conocidos como PAP (sin cifrado) o CHAP (con cifrado). En este caso, los flujos de autenticación se establecen, a través del nodo remoto de acceso BRAS, entre el dispositivo de usuario y el servidor AAA (*Authentication, Authorization & Accounting*) o RADIUS que es quien permite o deniega la comunicación con el usuario en cuestión.

El modelo IPoE utiliza un proceso basado en el protocolo EAP (*Extensible Authentication Protocol)* que permite la utilización de múltiples mecanismos de autenticación y cifrado (TLS, MD5, OTP, PSK, IKE,...). También en este caso el servidor de autorización podría ser un servidor RADIUS (por ejemplo, el existente en una red inicial basada en PPP); sin embargo, esto no es requisito imprescindible, pudiendo desempeñar las funciones AAA cualquier otro elemento, por ejemplo, el propio servidor de DHCP o un servidor específico de gestión de usuarios o/y servicios.

Monitorización de las sesiones

Para monitorizar el estado de las sesiones, el protocolo PPPoE se encarga de enviar mensajes periódicos, denominados "*PPP keepalives*" interrogando a cada una de las partes de la comunicación. Si alguno de estos mensajes no es respondido un número determinado de veces, se asume que la

comunicación ha finalizado y se cierra la sesión.

De manera análoga, en el modelo IPoE, se envían mensajes especiales de nivel de enlace, denominados *"ARP keepalives"*, que tienen un trato similar: la reiterada falta de respuesta indica el fin de la sesión.

Control del volumen de tráfico

Todo el tráfico intercambiado en las sesiones punto a punto con el protocolo PPPoE se controla a su paso (obligado) por un punto centralizado de la red: el nodo remoto de acceso a Internet (BRAS). Este elemento contabiliza todo el tráfico generado/recibido por el usuario hacia/hasta los servidores de Internet externos, informando a los elementos de gestión de alto nivel correspondientes.

En el modelo IPoE, la naturaleza multipunto a multipunto de la red, permite una arquitectura distribuida en la que no es necesario un único punto central de paso. En este caso, el control del tráfico intercambiado lo han de realizar, de manera distribuida, los diferentes elementos que componen la red de agregación y de borde IP.

Seguridad en las comunicaciones

En el modelo PPP, la naturaleza punto a punto de las sesiones, unido al proceso de autenticación inicial dificulta ya en gran medida la intromisión de terceros. No obstante, lo habitual es que el BRAS establezca mecanismos adicionales de seguridad, por ejemplo, la creación de listas de control de acceso (ACL) que limitan qué usuarios/dispositivos pueden acceder a determinados servicios o elementos.

En el caso de un modelo IPoE, con arquitectura multipunto a multipunto, son los propios elementos que componen la red de agregación basada en Ethernet/MPLS los que garantizan, mediante mecanismos probados y conocidos, la seguridad en las comunicaciones.

Servicios mayoristas

En el modelo PPP, para ofrecer servicios mayoristas, un proveedor de servicio ha de crear caminos específicos y seguros que directamente encaucen el tráfico entre un usuario y el BRAS del operador a quien se le ofrece el servicio. Para ello se emplea un protocolo conocido como L2TP (*Layer 2 Tunneling Protocol)* que es capaz de crear un "túnel" punto-a-punto entre un usuario y un tercero.

De manera análoga, en el modelo IPoE este camino entre usuario y un tercero se implementa mediante túneles de nivel 2 (o nivel de Ethernet). Pero la red Ethernet/MPLS de agregación además permite en este caso crear esos túneles según un modelo multipunto a multipunto, de manera que la oferta mayorista podría incluso extenderse a servicios de esta naturaleza.

Conclusiones

Tras un breve análisis de los aspectos anteriores, se comprueba que para un tipo de servicio punto a punto como el que se ofrece con el servicio de acceso a Internet, ambos modelos (PPPoE e IPoE/DHCP), son capaces de ofrecer, cuando menos, las mismas capacidades con un comportamiento similar. La principal ventaja que ofrece el modelo IPoE para este tipo de servicios es la capacidad de implementar los mecanismos de control de tráfico de una manera distribuida, evitando el "cuello de botella" que supone el elemento BRAS de la arquitectura PPP frente al continuo aumento de tráfico. Esto hecho, unido al carácter del BRAS como elemento único de fallo en la arquitectura, puede llegar a ser crítico para el servicio.

Además, la incapacidad (o ineficiencia) del modelo PPP para soportar la entrega de servicios de multidifusión (punto a multipunto), hacen de la solución IPoE, apoyada sobre el protocolo DHCP, la opción de futuro más plausible como modelo único de red capaz de ofrecer todo tipo de aplicaciones, facilitando así la creación y mantenimiento de servicios realmente convergentes.

Despejada la duda sobre el modelo de futuro a utilizar, el reto para el proveedor de servicios queda centrado en el cómo y el cuándo hacer la transición del modelo PPP heredado del acceso a Internet, hacia un modelo único, IPoE basado en el protocolo DHCP. ◆

"La incapacidad (o ineficiencia) del modelo PPP para soportar la entrega de servicios de multidifusión (punto a multipunto), hacen de la solución IPoE la opción de futuro más plausible como modelo único de red capaz de ofrecer todo tipo de aplicaciones"