Revista Cubana de Ciencias Informáticas
Vol. 7, No. 1, Enero-Marzo, 2013
ISSN: 2227-1899 | RNPS: 2301
Pág. 32-43
http://rcci.uci.cu

Tipo de artículo: Artículo original
Temática: Tecnologías de la información y las telecomunicaciones
Recibido: 15/01/2013 | Aceptado: 5/03/2013

VPLS: alternativa de interconexión a través del *backbone* IP/MPLS de ETECSA

VPLS: alternative of interconnection through ETECSA´s IP/MPLS backbone

Osmel Barreto Prieto

Centro de Investigación y Desarrollo de Electrónica y Mecánica "CID MECATRONICS" Sitio en 15 esquina 86A, Playa, La Habana, Cuba

cid3@reduim.cu

Resumen

La Empresa de Telecomunicaciones de Cuba (ETECSA) maneja en condiciones de exclusividad la infraestructura de telecomunicaciones del país, por lo que el resto de los proveedores necesitan utilizar dicha infraestructura como soporte para la interconexión de los nodos que componen sus redes. Teniendo en cuenta el desarrollo de las tecnologías de las telecomunicaciones, ETECSA ha apostado por la implementación de un *backbone Internet Protocol over MultiProtocol Label Switching:* Protocolo de Internet sobre Conmutación Multiprotocolo basada en Etiquetas) en su red, el cual se espera absorba todos los servicios actualmente soportados por el *backbone Asynchronous Transfer Mode/Frame Relay*. Sin embargo, en estos momentos, la red IP/MPLS solamente oferta servicios *Virtual Private Network:* a nivel de red (nivel tres del modelo OSI), cuestión que, para los otros proveedores, resulta inadmisible. El presente artículo describe una propuesta de implementación de una entidad *Virtual Private LAN Service*: Servicio de LAN Privada Virtual) como alternativa para la migración de los servicios de *Virtual Private Network* de nivel dos que actualmente se soportan sobre el *backbone ATM/Frame Relay*, hacia el *backbone Internet Protocol MultiProtocol Label Switching*, variante que garantiza la independencia por parte de los proveedores que son clientes de ETECSA en la operación y enrutamiento de su red.

Palabras clave: IP/MPLS, independencia en el enrutamiento, migración, VPLS.

Abstract

The Cuban Telecommunications Enterprise (ETECSA) owns exclusively the whole telecommunication infrastructure in the country. Because of that, other services providers need to use its network as a support for the interconnection of the nodes which form part of its own networks. Attending to the development of telecommunication technologies, ETECSA has invested on the implementation of an IP/MPLS (Internet Protocol over MultiProtocol Label Switching) backbone for its network, which is supposed to absorb all the services that are supported by the ATM (Asynchronous Transfer Mode)/Frame Relay backbone. However, at the moment this network supports level three services (according to OSI model), which is unacceptable for the other providers, due to the management requirements of the routing policies of the services they provide. This article describes a proposal of implementation of a VPLS (Virtual Private LAN Service) entity as an alternative for the migration of the level two VPN services that are supported at present over the ATM/Frame Relay backbone, toward the

Revista Cubana de Ciencias Informáticas
Vol. 7, No. 1, Enero-Marzo, 2013
ISSN: 2227-1899 | RNPS: 2301
Pág. 32-43
http://rcci.uci.cu

IP/MPLS backbone. This entity guarantees the operation and routing independence for the service providers that are clients of ETECSA.
Keywords: *IP/MPLS, VPLS, migration, routing independence.*

Introducción

Descripción general de las VPNs

Una VPN es, como lo indica su nombre, una Red Privada Virtual, la cual utiliza una tecnología de túnel para transmitir los datos de usuarios de un lado a otro de la red del ISP (del inglés, *Internet Services Provider*) a la que está conectada (Mitchell, 2011). La palabra "túnel" se usa para simbolizar el hecho que los datos estén cifrados desde el momento que entran a la VPN hasta que salen de ella. Gracias a esto, la información transmitida es incomprensible para cualquiera que no se encuentre en uno de los extremos de la VPN, tal y como si los datos viajaran a través de un túnel. De esta manera, cuando un usuario necesita acceder a la red privada virtual, su solicitud se transmite cifrada al sistema de pasarela, que se conecta con la red remota mediante la infraestructura de red pública como intermediaria.

Una VPN basada en MPLS es aquella que utiliza los LSP (del inglés, *Label Switch Path*) como tecnología de túnel para el cifrado de sus datos. Para entender el funcionamiento de una VPN de este tipo, se hace imprescindible familiarizarse con los términos utilizados en el argot técnico. Entre los más significativos se encuentran: (Rosen and Rekhter, 2006).

- **Router P (*Provider*: Proveedor):** router interno de la red del proveedor de servicios.
- **Router PE (*Provider Edge*: Proveedor de Borde):** router del proveedor de servicios que se encuentra en la frontera de su red. Atiende a uno o varios CEs
- **Router CE (*Customer Edge*: Cliente de Borde):** router del cliente que se encuentra en la frontera de su red. Está conectado directamente con la red proveedor de servicios y que se encarga de la distribución de la información de la red cliente. Pueden existir varios CE para un usuario, pero un CE sólo pertenece a uno de ellos.
- **Sitios:** subredes internas de un cliente que se encuentran separadas físicamente pero unidas lógicamente a través de una VPN.
- **Tablas de información de usuario:** elemento esencial para lograr privacidad entre VPNs. Estas tienen carácter individual para cada usuario y para cada sitio de usuario. Dichos sitios se interconectan a través de LSPs individuales, lo cual permite dicha privacidad. El contenido de cada una depende del tipo de VPN a la cual brinda soporte.

La Figura 1.1 ilustra tres VPNs basadas en MPLS coexistentes sobre una misma estructura. En ella se destacan los elementos que garantizan la privacidad de los datos de las mismas: las tablas de información de usuario.

Revista Cubana de Ciencias Informáticas
Vol. 7, No. 1, Enero-Marzo, 2013
ISSN: 2227-1899 | RNPS: 2301
Pág. 32-43
http://rcci.uci.cu

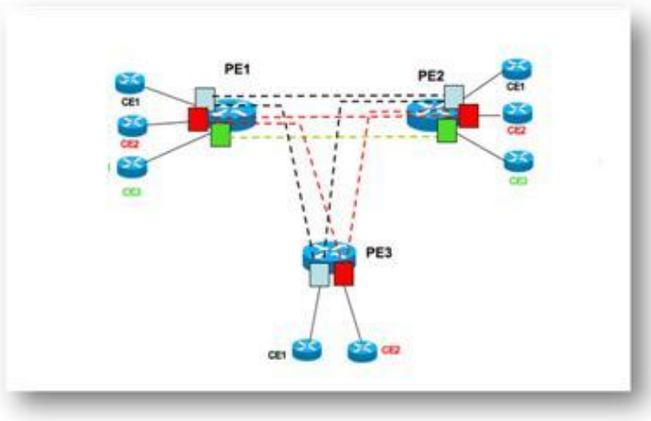

Figura 1. 1. Elementos que permiten privacidad entre VPNs: tablas de información de usuario.

Métodos científicos:

Métodos teóricos:

- Histórico lógico para investigar el desarrollo histórico de la conmutación multiprotocolo basada en etiquetas, con el objetivo de facilitar el análisis del escenario existente en el *backbone* IP/MPLS de ETECSA.
- Análisis y síntesis, para arribar a conclusiones mediante el estudio de la bibliografía, analizar la conmutación multiprotocolo basada en etiquetas, los elementos que la componen, características y facilidades que brinda y adaptarlas a las necesidades de un proveedor de servicios.

Métodos empíricos.

- Entrevistas a los compañeros del Centro de Gestión de ETECSA para caracterizar el estado actual de la conexión de los nodos de las redes de los ISPs clientes de ETECSA y del *backbone* IP/MPLS, con vista a determinar posibles soluciones para la utilización de este último como medio de conexión para los nodos de dichas redes.
- Observación para la acumulación de datos relacionados con las configuraciones de los dispositivos de interconexión.

Materiales y recursos tecnológicos

Para el desarrollo de la presente investigación fue necesario contar con recursos tecnológicos, como computadoras con acceso a Internet para la consulta y búsqueda de información relacionada con el estándar MPLS y la configuración de VPLS. Se necesitó además, contar con la posibilidad de intercambiar información con especialistas en la administración de redes de proveedores de servicios y de ETECSA, los cuales facilitaron el análisis de la situación actual de interconexión de estas redes.

Desarrollo

Las VPN basadas en MPLS pueden clasificarse de distintas formas. Lo más común es basar la clasificación en el nivel del servicio que se está ofreciendo al cliente. Esto da lugar a las siguientes categorías: (Doyle, 2008).

- VPNs capa tres: son también conocidas como Red Privada Virtual Enrutada (*VPRN: Virtual Private Routed Network*). El proveedor de servicios participa en el enrutamiento capa tres del usuario.

- VPNs capa dos: el proveedor interconecta los sitios de usuario a través de la simulación de una tecnología capa dos (usualmente ATM, *Frame Relay* o *Ethernet*) elegida por él. El usuario implementa el protocolo capa tres que desee emplear, sin la participación del proveedor de servicios a ese nivel.

Dentro de las VPNs capa dos existen dos tipos:

- VPN capa dos multipunto: Servicio de Red de Área Local Privada Virtual (*VPLS*, del inglés, *Virtual Private LAN Service*). A través de este servicio, desde el punto de vista del usuario, el proveedor actúa como un switch Ethernet. El atractivo del mismo para los usuarios radica en que pueden hacer que su WAN funcione como una red de campus o red LAN, mediante el uso de una sola tecnología (*Ethernet*), que es barata y conocida.
- VPN capa dos punto a punto: Línea Arrendada Virtual (*VLL*, del inglés, *Virtual Leased Line*). Provee conectividad capa dos punto a punto entre dos sitios. Cualquier tecnología de nivel dos (*Ethernet*, TDM, ATM, etc.) puede ser encapsulada dentro de dichas líneas virtuales.

A continuación se describen brevemente las ventajas que trae consigo la implementación de una VPN capa dos basada en MPLS con respecto a la implementación de una VPN del mismo tipo, pero de nivel tres: (Networks, 2008).

- Separación de las responsabilidades administrativas: el proveedor de servicios es sólo responsable de la conectividad capa dos, y el usuario, de la conectividad capa tres, la cual incluye el enrutamiento. Con esta separación, además, las fallas generadas por el usuario quedan aisladas de la red proveedora.
- Seguridad y privacidad en el enrutamiento: como la información de enrutamiento no es importada de los PEs, como sucede en las VPN capa tres, éstos no pueden procesar ni obtener información del enrutamiento dentro de la VPN del usuario.
- Soporte multiprotocolo natural: la red proveedora no participa en el intercambio de información de enrutamiento de los usuarios, por lo cual puede soportar múltiples protocolos como IP, IPX, SNA, entre otros.

Dentro de las variantes de VPNs analizadas, las de nivel dos son las que proveen una separación completa entre la red del proveedor de servicios y la del usuario, debido a que no hay intercambio de rutas entre los dispositivos CE y PE. Por tanto, una VPN de este tipo permitirá alcanzar la independencia de enrutamiento que requiere un proveedor de servicios que utilice al *backbone* IP/MPLS de ETECSA como medio de interconexión de los nodos de su red.

MPLS L2 VPN punto-multipunto: VPLS

VPLS, también conocido como servicio de LAN transparente (TLS, del inglés, *Transparent LAN Service*), es una VPN punto a multipunto de capa dos que permite conectar múltiples sitios de usuario a través de la simulación de una red de área local (LAN, del inglés, *Local Area Network*) *Ethernet*. Todos los sitios del cliente pertenecientes a una entidad VPLS parecen estar en la misma LAN, sin importar sus localizaciones, tal y como si estuvieran interconectadas a través de un gran conmutador *Ethernet*.

VPLS se basa en el re-envío de tramas *Ethernet*. La red del proveedor de servicios, por tanto, puede re-enviar la información basándose solamente en sus direcciones MAC o teniendo en cuenta además las etiquetas de LAN virtual (*Virtual LAN Tag*, según su denominación en inglés). Es por ello que los *routers* PE deben soportar todas las prestaciones "clásicas" *Ethernet*, como aprendizaje de direcciones MACs, inundación (del inglés, *flooding*) de tramas, etc. Desde un punto de vista funcional, esto implica que los PEs deben implementar un puente o *bridge* (según su

denominación en inglés) por cada instancia VPLS. Este es conocido como puente virtual (VB, del inglés, *virtual bridge*). La funcionalidad VB se lleva a cabo en el PE mediante la asignación de una VFT para cada entidad VPLS.

Los elementos necesarios para constituir una entidad VPLS, como es de esperar, son los mismos que componen una MPLS L2 VPN de manera general: una red central MPLS, *routers* CEs y PEs, circuitos de conexión (AC), puentes virtuales (VB, del inglés, *Virtual Bridge*), túneles y *pseudowires*. Los puentes virtuales no son más que las tablas virtuales de re-envío (VFT) anteriormente mencionadas. Por otra parte, la definición de *pseudowire* es utilizada para denominar a una entidad bidireccional de conexión entre *routers* PEs compuesta por dos circuitos virtuales (VC) o LSPs unidireccionales y de sentidos opuestos. El resto de la nomenclatura mantiene su mismo significado.
El AC que posibilita dicha conexión puede ser tanto un enlace *Ethernet* físico o lógico, un PVC ATM transportando tramas *Ethernet* o incluso un PW *Ethernet*. Con esto se simplifica la frontera LAN/WAN y se logra un aprovisionamiento rápido y flexible del servicio. La Figura 1.2 muestra la estructura descrita anteriormente:

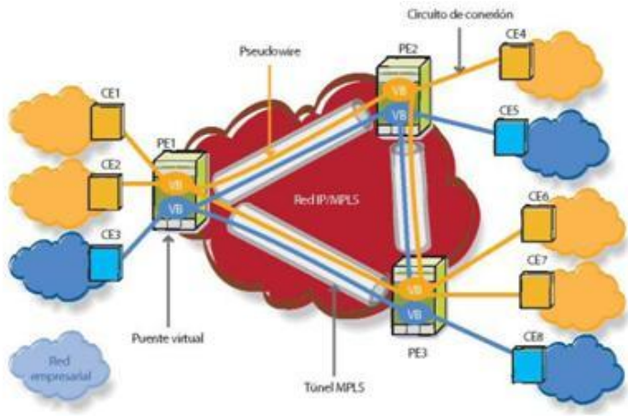

Figura 1. 2. Estructura de una entidad VPLS.

El núcleo de la red IP/MPLS interconecta los PEs que intervienen en la entidad VPLS en cuestión pero no participa realmente en su funcionalidad. El tráfico en este segmento se conmuta simplemente basándose en etiquetas MPLS.

Para el intercambio de información entre dos *routers* PEs se establecen dos circuitos virtuales (LSPs), uno en cada dirección. Estos túneles internos son los mencionados PWs. La arquitectura *pseudowire* está normalizada por Grupo de Trabajo para PWE3 (del inglés, *Pseudowire Emulation Edge to Edge*), perteneciente a la IETF, en el RFC 3985. (Bryant and Pate, 2005).
Para cada entidad VPLS se crea una malla completa de túneles internos (PWs) entre todos los PEs que participan en la entidad VPLS. Gracias a estos, las tramas pueden ser transmitidas directamente desde el PE de entrada hacia el de salida sin pasar por ningún otro PE intermedio. No es necesario entonces implementar ningún protocolo de prevención de bucles, como el *Spanning Tree Protocol* (STP, por sus siglas en inglés), *Multiple Spanning Tree Protocol* (MSTP, por sus siglas en inglés), o *Rapid Ring Protection Protocol* (RRPP, por sus siglas en inglés). Con la aplicación de una simple regla conocida como “Split Horizon” se prevé cualquier lazo que pueda ocurrir en una entidad VPLS. Dicha regla plantea que ningún PE debe re-enviar a través de un PW el tráfico que haya recibido a través de otro PW.
En el PE es donde el VPLS comienza y termina y donde se establecen todos los túneles necesarios para conectar con todos los otros PEs. Sus funcionalidades quedan divididas en dos planos (Huawei, 2007).

Revista Cubana de Ciencias Informáticas
Vol. 7, No. 1, Enero-Marzo, 2013
ISSN: 2227-1899 | RNPS: 2301
Pág. 32-43
http://rcci.uci.cu

Plano de re-envío: realiza el encapsulado, re-envío y desencapsulado de las tramas Ethernet desde que entran a la red del ISP y hasta que salen de la misma respectivamente.

Plano de control: lleva a cabo el descubrimiento de miembros de una entidad VPLS, el cual puede ser implementado a través de una configuración manual o de forma automática a través de la utilización de determinados protocolos. Dicho plano además, se encarga de la señalización, a través de la cual establece, mantiene y elimina los PWs entre PEs pertenecientes a una entidad VPLS. Estas funciones pueden implementarse mediante la utilización de dos protocolos: el BGP (del inglés, *Border Gateway Protocol*) y el LDP (del inglés, *Label Distribution Protocol*). Dichas variantes están reflejadas en los RFC de la IETF 4761 y 4762 respectivamente, dando lugar a dos clasificaciones: VPLS Kompella y VPLS Martini.

La implementación de una entidad VPLS es la solución que más se ajusta y es más factible para la interconexión de los nodos de un red de este tipo a través del *backbone* IP/MPLS de ETECSA. La conexión a nivel dos que esta variante ofrece, garantizará la independencia en el direccionamiento que algunas empresas requieren desde su condición de proveedor de servicios. Por otra parte, dicha variante posibilita la comunicación directa entre los nodos de una red, sin que ello implique que la información tenga que pasar por el nodo central de la misma. Esto se traducirá en una reducción de la carga de operación de los *routers* presentes en este, y por tanto, en un aumento de disponibilidad de ancho de banda para las comunicaciones que obligatoriamente necesiten utilizar el nodo central como medio de acceso, como es en algunos casos la navegación web.

Descripción del *backbone* IP/MPLS de ETECSA

La Empresa de Telecomunicaciones de Cuba ETECSA ha apostado para su desarrollo futuro, al despliegue de una red IP/MPLS (IP sobre, del inglés, *MultiProtocol Label Switching*) como soporte de sus nuevos servicios, la cual abarca todo el territorio nacional. La Figura 1.3 describe la estructura de la misma:

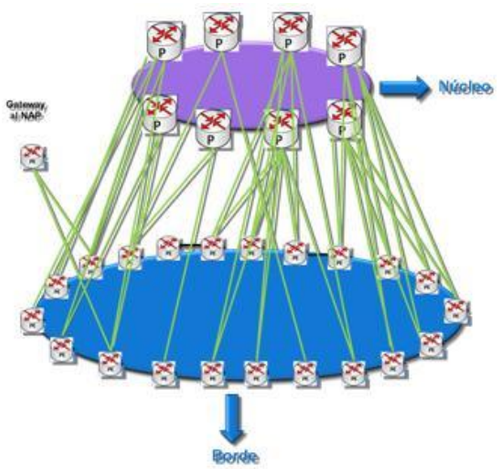

Figura 1. 3. Backbone IP/MPLS de ETECSA.

Dicha red consta de dos niveles. El primero de ellos es el núcleo (*core*, según su denominación en inglés) de la red, el cual está constituido por 8 *routers* modelo NE40-8E del fabricante Huawei. Estos desempeñan el papel de *routers* de núcleo (P), o sea, son *routers* de conmutación de alto de rendimiento basado en etiquetas. En un segundo nivel se encuentran los *routers* de borde (PE). Estos son igualmente del fabricante Huawei, modelo NE40-8 (Figura 3.8). Este equipamiento permite la implementación de entidades VPLS. (Huawei, 2005). Estos *routers* no reciben directamente

Revista Cubana de Ciencias Informáticas
Vol. 7, No. 1, Enero-Marzo, 2013
ISSN: 2227-1899 | RNPS: 2301
Pág. 32-43
http://rcci.uci.cu

el tráfico de usuario. La información de los clientes se concentra en un flujo único que posteriormente es entregado al NE40-8. Para ello se utilizan los DSLAMs (*Digital Subscriber Line Access Multiplexer*).

Descripción de la red de un proveedor de servicios cliente de ETECSA

La redes de los proveedores de servicios que actualmente utilizan el *backbone* IP/MPLS como medio de interconexión de sus nodos cuentan por lo general con un nodo en cada cabecera de provincia. Estos se encuentran generalmente interconectados mediante una topología estrella a través del *backbone* ATM/*Frame Relay* de ETECSA. Estas redes cuentan además con un nodo central desde el que se manejan el resto de los nodos y se accede a servicios internacionales, como por ejemplo la navegación web internacional.

Los equipos del fabricante Cisco son extensamente utilizados en los nodos las redes de los proveedores nacionales. Es por ello que en el estudio se incluyó la configuración requerida en equipos de este tipo, específicamente en los modelos 3725, 3745, 3825, 3845, 7505 y 7513. Estos tienen una estructura modular que permite la adición y sustracción dinámica de interfaces, de forma tal que este pueda ser adaptado a las necesidades específicas de sus usuarios sin que ello implique un cambio total del hardware. Uno de los módulos posibles a añadir son las tarjetas WIC (WAN *Interface Card*), a través de ranuras de expansión específicas para este tipo de tarjetas (Cisco, 2004).

Los enlaces de dichos nodos con ETECSA pueden ser tanto *Frame Relay* como ATM. Estos pueden ser soportados sobre fibra óptica mediante equipos OptiX OSN 3500 que permiten la conexión a la red ASON, o a través de módem telefónicos de tecnología xDSL. Estos últimos se conectan a multiplexores de acceso de línea digital de abonado ATM (DSLAM ATM) y se encargan de concentrar el tráfico de los clientes de la red ATM/Frame Relay. La Figuras 1.4 y 1.5 ilustra lo anteriormente planteado:

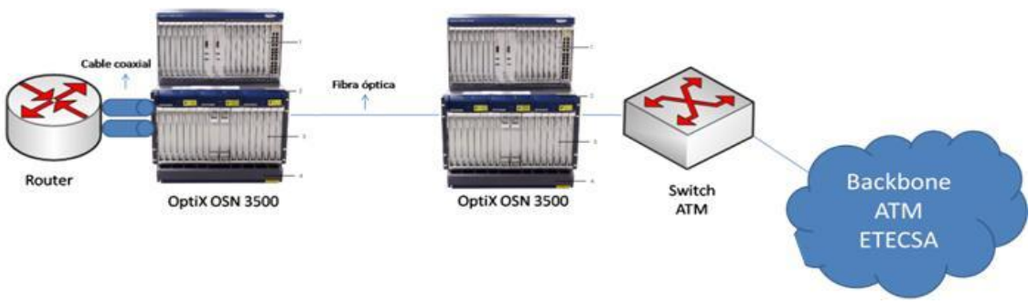

Figura 1. 4. Conexión al backbone ATM/Frame Relay a través de la red ASON.

Figura 1. 5. Conexión al *backbone* ATM/Frame Relay de ETECSA soportada sobre módem SHDSL.

Propuestas para la implementación de una instancia VPLS

Modificaciones en la red del usuario

Revista Cubana de Ciencias Informáticas
Vol. 7, No. 1, Enero-Marzo, 2013
ISSN: 2227-1899 | RNPS: 2301
Pág. 32-43
http://rcci.uci.cu

El primer punto a tener en cuenta es si nuestros *routers* cuentan con interfaces ATM. En la red de acceso del backbone IP/MPLS son utilizados DSLAMs IP. La comunicación con estos está basada en tráfico ATM. Los DSLAM IP re-ensamblan las tramas Ethernet a partir de las celdas ATM recibidas de los usuarios, por lo que resulta imprescindible que nuestros equipos cuenten con interfaces de este tipo. En caso positivo solo se necesita configurar correctamente dichas interfaces, de lo contrarió se necesitará adquirir nuevas interfaces. En los equipos Cisco objetos de estudio, dado su carácter modular, resulta viable la adición de tarjetas de interfaces para redes de área amplia *dual-serial* WIC-2T: *Wide Area Network Interface Card*), típicas del equipamiento Cisco. El autor considera que, mediante la adquisición de tarjetas WIC con funcionalidades de módem SHDSL es posible conectarse a los *routers* PE con una estructura como la descrita en la Figura 1.6:

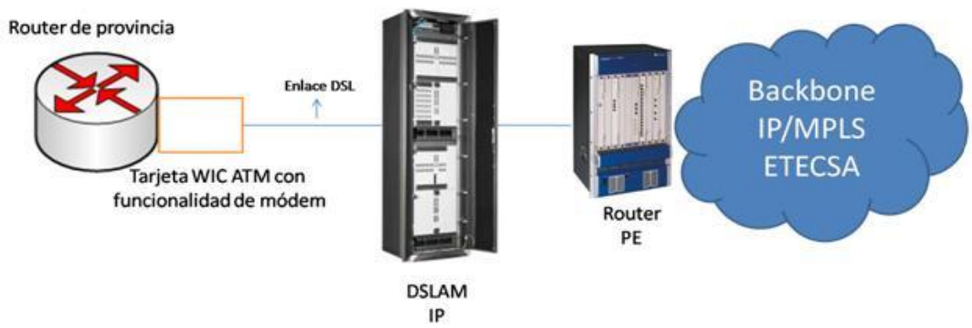

Figura 1.6. Propuesta de conexión sobre línea DSL.

Se propone entonces el uso de la tarjeta *Cisco Symmetric High-Bitrate DSL High Speed WAN Interface Card for Cisco Integrated Services Routers G.SHDSL* (HWIC-4SHDSL). La misma se basa la recomendación G.991.2 de la UIT-T, utilizada igualmente en los DSLAM IP de ETECSA. Por otra parte, cumple con las normas establecidas en el RFC 1483, que estandariza los métodos para el encapsulamiento de tramas Ethernet en celdas ATM. Como cada nodo provincial cuenta con dos enlaces, es factible utilizar una tarjeta que admita la conexión de más de una línea DSL. La HWIC-4SHDSL, variante de 4 pares de hilos, permite la conexión de cuatro líneas de dos hilos, o de dos líneas de cuatro hilos. Se logra, mediante la utilización de los Anexos A y B de la recomendación de la UIT-T G.991.2, alcanzar una velocidad máxima de hasta 2.304 Mbps por cada línea de dos hilos, y hasta 4.608 Mbps por cada línea de 4 hilos. Es posible incluso, mediante la utilización de los Anexos F y G de la recomendación mencionada, alcanzar velocidades desde 768 Kbps hasta 5.696 Mbps por cada línea de dos hilos, y desde 1.563 hasta 11.392 Mbps por cada línea de cuatro hilos. Los DSLAMs IP de ETECSA permiten la combinación de dos líneas de dos hilos como una única línea de 4 hilos, logrando así velocidades superiores para un mismo enlace. El precio de esta tarjeta en el mercado oscila alrededor de los € 600. Lamentablemente, la utilización de las mismas sólo es factible en los *routers* de la serie 3800. Para los pertenecientes a la serie 3700 deberá utilizarse, por tanto, otra tarjeta: la *Cisco Symmetric High-Bit-Rate DSL Interface Card* (WIC-1SHDSLV3). Esta cuenta con funcionalidades similares, con la diferencia de que sólo permite la conexión de una línea. El costo de estas tarjetas está alrededor de los € 400.

Como el envío de información en una entidad VPLS está basado en tramas Ethernet, resulta imperante encontrar una manera de ensamblar el tráfico IP de cada nodo de provincia en tramas Ethernet. Por otra parte, dichas tramas deberán ser ensambladas en celdas ATM para su re-envío a través de la línea DSL. Los IOS de los *routers* Cisco utilizados cuentan con una funcionalidad que permiten implementar la tarea anteriormente mencionada. Es posible, mediante la creación y configuración de sub-interfaces ATM llevar a cabo dichas funciones, utilizando para ello el comando **atm**

Revista Cubana de Ciencias Informáticas
Vol. 7, No. 1, Enero-Marzo, 2013
ISSN: 2227-1899 | RNPS: 2301
Pág. 32-43
http://rcci.uci.cu

route-bridge ip, el cual las realiza siguiendo el método recogido en el RFC 2684 de la IETF. El mismo estandariza el encapsulamiento multiprotocolo sobre la capa de adaptación ATM AAL5. Se creará una sub-interfaz por cada servicio de nivel tres, garantizando así la gestión de los servicios que se prestan. De esta forma se satisfacen los requerimientos anteriormente planteados.

En el caso de que contemos con una conexión a la red ASON, resulta viable enviar directamente tráfico Ethernet sobre dicha interfaz física, gracias a las posibilidades de largas distancias que la misma permite para este tipo de tráfico. Los *routers* utilizados deberán contar con interfaces FastEthernet libres, que puedan ser conectadas a un equipo OptiX OSN 3500, el cual también debe tener interfaces de este tipo disponibles, y de esta forma enlazarse con el equipo correspondiente de la red MPLS de ETECSA. Deberán crearse además sub-interfaces y VLANs (*Virtual LANs*) asociadas a la entidad VPLS. La Figura 1.7 refleja la idea planteada:

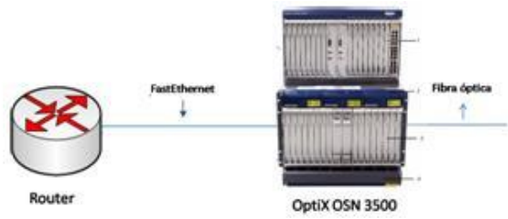

Figura 1.7 Propuesta de conexión de los enlaces ASON. Modificaciones en la red de acceso de ETECSA.

Como el *backbone* IP/MPLS utiliza DSLAMs IP para el acceso de usuario, deberán crearse nuevas facilidades en estos últimos que permitan la conexión de los nodos de nuestra red. Es necesario, además, que dichos equipos retiren el encapsulado ATM, re-ensamblen las tramas Ethernet y posteriormente las re-envíen hacia los PEs correspondientes. Esto se logra mediante la creación de VLANs para la transmisión de información capa dos desde el DSLAM hasta el PE a través de una interfaz Ethernet. Una vez creadas, se hace una multiplexación entre los VPIs/VCIs que se reciben por la línea de cobre y las VLANs anteriormente creadas.

Modificaciones en la red de acceso de ETECSA

Por otra parte, de existir en nuestra red un enlace a través de la red ASON, el equipo de ETECSA que lo atienda deberá conectar una de sus interfaces FastEthernet a un switch Ethernet que se conecte con un PE del *backbone* IP/MPLS. La figura 1.8 ilustra las modificaciones mencionadas:

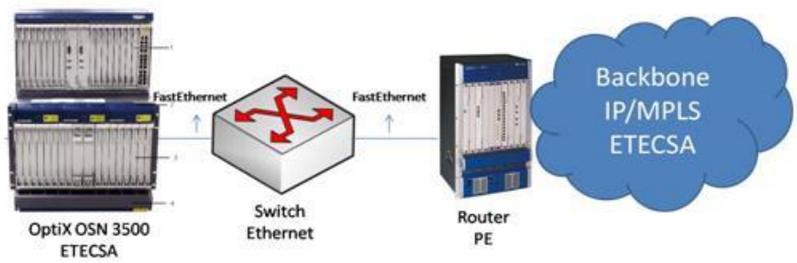

Figura 1.8. Propuesta de conexión de los equipos ópticos de ETECSA.

Pasado este punto, en los PE deberán crearse VLANs que tengan el mismo identificador que las creadas en los DSLAMs y en los *routers* de nuestra red, de forma tal que todo el tráfico recibido con una etiqueta VLAN X que identifica a una VLAN X en el DSLAM o en los *routers*, se identifique en el PE como perteneciente a la VLAN X en

este último. Una vez realizadas las tareas mencionadas, deberán crearse sub-interfaces Ethernet por cada VLAN creada y realizar la asociación VLAN/sub-interfaz Ethernet. Se estará entonces en condiciones de asociar dichas sub-interfaces con los VFT. El fabricante del equipamiento en cuestión, ha denominado a las VFB o VB como entidades de conmutación virtual (VSI: *Virtual Switch Instance*). Por tanto, en lo que sigue, se adoptará dicha nomenclatura para lograr homogeneidad con los comandos que se utilizan.

Configuración de los dispositivos de la red del usuario

La adición de las nuevas tarjetas WIC a los *routers* que las necesiten resulta extremadamente sencilla gracias a la presencia de las ranuras de expansión en la estructura de los mismos que permiten conectar tarjetas de este tipo directamente. Se deberán apagar los equipos y posteriormente conectar las tarjetas. Una vez conectadas se deberá reiniciar el sistema, configurar la interfaz ATM y comprobar la configuración. Una vez realizado este último paso, los *routers* se encuentran listos para utilizar la tarjeta WIC insertada.

En los *routers* que cuenten con enlaces sobre la red ASON se deberá crear la sub-interfaz que se utilizará para el intercambio, crear una VLAN y asociarla a la sub-interfaz creada, y finalmente, asignarle una dirección IP a la misma.

Configuración de los dispositivos de ETECSA

Los DSLAM IP deberán ser configurados de modo que re-ensamblen las tramas Ethernet y posteriormente las envíen al PE correspondiente. Para ello se hace necesario configurar la interfaz utilizada para comunicarse con el PE, crear los PVCs en los enlaces a utilizar, configurar la velocidad de los enlaces y el re-ensamblaje de tramas Ethernet.

Los PEs del *backbone* IP/MPLS de ETECSA utilizan el protocolo LDP para la distribución de etiquetas, por lo que debe implementarse una VPLS Martini. Antes de pasar a la configuración de la entidad VPLS, deben realizarse algunas tareas previas, tales como: configurar los identificadores de LSR (LSR ID), habilitar MPLS en el sistema, habilitar la MPLS L2 VPN en los PEs, establecer sesiones LDP remotas entre los PEs si estos no se encuentran conectados directamente y chequear las configuraciones anteriores. Una vez logradas, se estará entonces en condiciones de configurar propiamente la entidad VPLS, lo cual incluye: crear una VSI y configurar la señalización LDP, crear la VLAN que se corresponda a la utilizada en el DSLAM para transmitir la información del ISP cliente, asociar un VSI con un AC y chequear cada uno de las tareas anteriores.

Los códigos de configuración para los equipos Cisco y los equipos de ETECSA aparecen en la tesis de grado nombrada “Propuesta de configuración de una entidad VPLS como alternativa de interconexión de los nodos de la red de CITMATEL a través del *backbone* IP/MPLS de ETECSA.” (Barreto, 2011).

Ventajas de la propuesta planteada

En la mayoría de los casos, la interconexión actual de los nodos que componen la red de los proveedores de servicios nacionales presupone que todo el tráfico tenga que pasar por su nodo central, incluso si, por ejemplo, un usuario atendido por el nodo de Matanzas desea acceder a un sitio FTP presente en el nodo de Villa Clara. Esto implica una sobrecarga innecesaria para el equipamiento del nodo central. Con la estructura totalmente mallada que se logra con la implementación de la entidad VPLS propuesta, este problema es solucionado. Cada nodo tendrá la posibilidad de

comunicarse directamente con cualquier otro, sin que su tráfico tenga que pasar por el nodo central. Esto influye positivamente en el ancho de banda disponible para algunos servicios, como por ejemplo, los de navegación Web internacional, que por lo general tienen que pasar obligatoriamente por dicho nodo.

Por otra parte, la sustitución de los enlaces Frame Relay por nuevos enlaces ATM en la red de acceso, permitirá aumentar las velocidades de conexión, y con ello potenciar los servicios que se prestan como ISP. A esto se suman las bondades que trae consigo la utilización de ATM como tecnología de nivel de enlace en la última milla, como por ejemplo, la clasificación del tráfico en distintas clases de servicio. Esto permite la priorización de determinados tipos de tráfico, garantizando así una QoS determinada.

Verificación de los resultados

La propuesta de configuración recogida en este artículo, así como los comandos de configuración anteriormente referenciados, fueron sometidos a discusión con ejecutivos del nodo central del backbone IP/MPLS de ETECSA y de la UEB de Operaciones de Internet de CITMATEL, empresa que solicitó nuestra propuesta como base para un proyecto de migración de las conexiones con las que cuenta actualmente. Ambas partes validaron la factibilidad y aplicabilidad de la propuesta, para la cual analizaron tanto las posibilidades reales de implementación como la idoneidad de las configuraciones de los equipos que se proponen.

Conclusiones

La migración de la interconexión actual de las conexiones soportadas sobre el backbone ATM/Frame Relay hacia el *backbone* IP/MPLS resulta inminente, ya que ETECSA propone que este último asuma todos los servicios que se soportan actualmente sobre el *backbone* ATM. El estudio presentado en este artículo constituye un proyecto de diseño que recoge de manera eficiente y certera, los pasos a seguir por el personal administrativo de la red de ETECSA y de un proveedor de servicios para la migración de la interconexión de los nodos que conforman la red de este último a través del *backbone* ATM/Frame Relay de ETECSA, hacia una nueva interconexión de los mismos a través del *backbone* IP/MPLS de dicha empresa. A través de la variante propuesta, el equipo de administración de la red de un proveedor de servicios podrá afrontar el proceso de migración y cumplir con sus expectativas con respecto al manejo de las rutas.

Con el desarrollo de este trabajo, se comprobó la posibilidad real de implementar una entidad VPLS sobre la estructura actual del *backbone* IP/MPLS de ETECSA. Para ello se tuvo en cuenta tanto las capacidades del equipamiento actual para asumir dicho cambio, como la factibilidad de las inversiones necesarias para el mismo.

Referencias

- BARRETO P., O. Propuesta de configuración de una entidad VPLS como alternativa de interconexión de los nodos de la red de CITMATEL a través del *backbone* IP/MPLS de ETECSA. La Habana: CUJAE; 2011.
- BRYANT S., PATE P. RFC 3985: Pseudo Wire Emulation Edge-to-Edge (PWE3) Architecture. 2005. Disponible en: http://tools.ietf.org/html/rfc3985
- CISCO SYSTEM I. Cisco 3700 Series Multiservice Access Router. 2004. Disponible en: http://www.cisco.com/en/US/prod/collateral/routers/ps282/product_data_sheet09186a008009203f.pdf
- DOYLE J. Understanding MPLS VPNs, part I. Revista Digital Network World; 2008 [actualizado 2008; consultado 2011, 12 de febrero]; disponible en: http://www.networkworld.com/community/node/24781

- HUAWEI T. Quidway NetEngine40 Configuration Guide - VPN. 2007.
- HUAWEI T. Quidway NetEngine 40 Series Universal Switching Router. 2005.
- MITCHELL B. Virtual Private Networks Tutorial [consultado el: 12 de febrero de 2011]. Disponible en: [http://compnetworking.about.com/od/vpn/a/vpn_tunneling.htm].
- NETWORKS F. IP/MPLS-Based VPNs: Layer-3 vs. Layer-2. Foundry Networks Magazine. 2008.
- ROSEN E., REKHTER Y. RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs). 2006. Disponible en: http://www.ietf.org/mail-archive/web/ietf-announce/current/msg02120.html