

GESTIÓN DE REDES IP/MPLS

Por: Lic. Johanna García Andricain e Ing. Sybel Alonso Baldor,
Especialistas en Planta Interior, DVSF, ETECSA
johanna.garcia@etecsa.cu, sybel.alonso@etecsa.cu

RESUMEN

MPLS es un mecanismo de transporte de datos y voz de alta velocidad, a través de una sola conexión, orientado a redes de comunicación, tecnología de punta que brinda una mayor fiabilidad y rendimiento al encaminamiento del dato en la red.

Es un importante medio para la gestión de la red MPLS, por lo que en Cuba se realiza dicha supervisión y configuración de la tecnología mediante el sistema iManager U2000 del proveedor chino Huawei. El presente trabajo está orientado a investigar la forma de gestionar redes IP/MPLS analizando a profundidad los principios del estándar. Se describe una evaluación de las áreas funcionales de la plataforma iManager U2000, así como de las principales aplicaciones de MPLS y su implementación en el sistema de Huawei iManager U2000 evaluado.

Palabras clave: BGP, CoS, EIGRP, IP, IS-IS, LDP, LSP, LSR, MPLS, OSPF, QoS, RSVP, TDP, TE, TMN, ToS, VPN, Gestión de redes IP/MPLS

ABSTRACT

MPLS is a high-speed voice and data transfer mechanism by a single connection, oriented to communications networks. It is a state of the art technology that provides greater reliability and performance for data routing in the network.

It is an important means for MPLS Network Management; therefore, in Cuba such technology supervision and setting up is carried out by the iManager U2000 system of the Chinese provider Huawei. This work aims at searching the way of managing IP/MPLS networks to thoroughly analyze standard principles. An assessment of the functional areas of the iManager U2000 platform, as well as the main MPLS applications and its implementation in the evaluated iManager U2000 system of Huawei is described.

Key words: BGP, CoS, EIGRP, IP, IS-IS, LDP, LSP, LSR, MPLS, OSPF, QoS, RSVP, TDP, TE, TMN, ToS, VPN, Networks Managment IP/MPLS

Introducción

El enorme crecimiento de la red Internet ha convertido al protocolo IP —*Internet Protocol*— en la base de las actuales redes de telecomunicaciones, al contar con más de 80% del tráfico cursado. La migración a MPLS como núcleo de las redes multiservicio con soporte de voz, vídeo y datos, se está realizando de forma gradual. MPLS —*Multiprotocol Label Switching*— está basada en el concepto de multiprotocolo de etiquetas conmutadas, en donde la IETF —*Engineering Task Force*— se forma como grupo de trabajo para estandarizar esta nueva tecnología. Hoy en día MPLS es definida por un conjunto de la IETF —*Request for comments* (RFC) — y una serie de especificaciones.

MPLS desempeña un papel importante en el encaminamiento con protección (rutas de respaldo), establecimientos de circuitos, y el envío de paquetes a través de la red de próxima generación para resolver las demandas del servicio garantizadas para los usuarios de la red. Además de ser una tecnología desarrollada para dar soluciones hacia redes de datos de servicios integrados en redes de banda ancha, otorgando así garantías de calidad de servicio. MPLS cuenta con las aplicaciones de esta tecnología, como son ingeniería de tráfico (TE), calidad de servicio (QoS) y clases de servicios (CoS) y redes virtuales privadas (VPNs).

La arquitectura MPLS fue diseñada para soportar la transmisión de datos basada en etiquetas. En esta arquitectura los

routers de conmutación por etiquetas (LSR) —*Label Switching Routers*— son capaces de reconocer los límites de las celdas o paquetes y de procesar sus cabeceras. En estos *routers* se intercambia información sobre la topología de la red y se construyen tablas de encaminamiento, además se establecerán los LSP —*Label Switched Path*— que seguirán los paquetes. Esta arquitectura está siendo ampliada para incluir LSR que no reconocen el plano de salida del paquete ni las fronteras de la celda, por lo tanto, no pueden enviar los datos basándose en la información transportada en las cabeceras. De manera que estos LSRs incluyen dispositivos donde la conmutación está basada en intervalos de tiempo, longitudes de onda o puertos físicos.

Principios MPLS

Las características básicas de MPLS [1] son las siguientes:

- Mecanismo de encaminamiento de paquetes en el cual los paquetes son encaminados basados en etiquetas. (Figura 1).
- Las etiquetas corresponden a destinos IP aunque pueden estar asociadas a otros parámetros como QoS.
- Fue diseñado para soportar otros protocolos, además de los ya existentes.

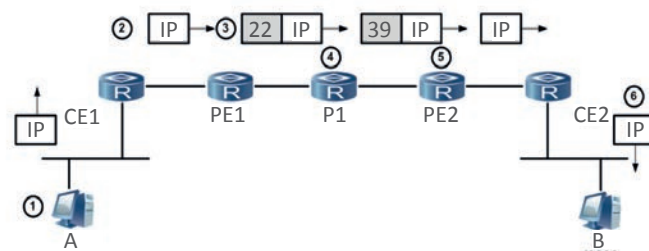


Figura 1. Ejemplo de funcionamiento del protocolo MPLS.
Fuente: Elaboración propia.

MPLS tiene dos componentes principales (Figura 2): el **Plano de Control** que intercambia información de ruteo Capa 3 y contiene mecanismos complejos para intercambiar información de ruteo, tales como OSPF, EIGRP, IS-IS y BGP, y

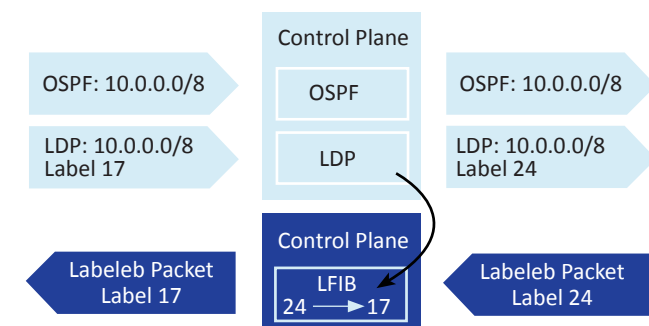


Figura 2. Componentes principales de MPLS. Fuente: Elaboración propia.

para intercambiar etiquetas; como TDP, LDP, BGP y RSVP y el **Plano de Datos** que encamina paquetes basados en etiquetas, provee un mecanismo de encaminamiento simple.

Todas las aplicaciones pueden usar múltiples protocolos en el plano de control, pero todas usan el mismo plano de encaminamiento. Se puede observar en la figura 3 la interrelación entre los planos.

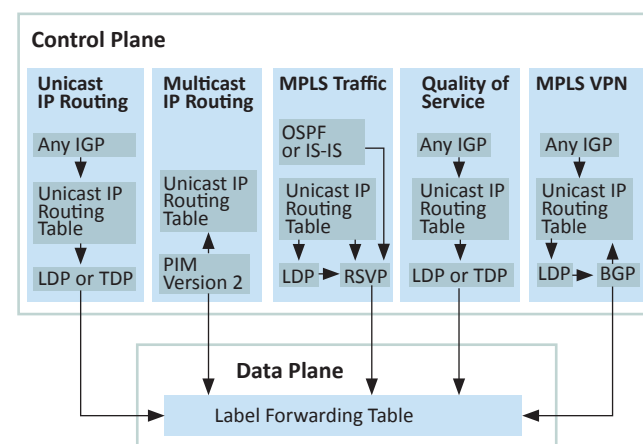


Figura 3. Relación entre los planos. Fuente: Elaboración propia.

Plataforma iManager U2000 de Huawei

La plataforma iManager U2000 [3] (Figura 4) es un Sistema de Gestión de Red Unificado, del proveedor Huawei, el cual es un sistema de gestión integral. Actualmente, se usa para los servicios y equipos de datos, basados en la tecnología MPLS y clientes con servicio de VPN fundamentalmente a empresas. El sistema permite administrar redes heterogéneas de diferentes proveedores y diferentes tecnologías. Asimismo, realiza las funciones de acuerdo con las recomendaciones de la red de gestión de telecomunicaciones (TMN).

Las diferentes áreas funcionales que cubre esta plataforma tienen las siguientes características:

Gestión de configuración: Puede configurar los protocolos necesarios para la configuración correcta del equipo y así lograr un óptimo funcionamiento. Además de las interfaces asociadas a los puertos de la tarjeta del equipo y los anchos de banda disponibles para utilizar.

Gestión de seguridad: Presenta una estructura de la seguridad del sistema como plataforma para la gestión de los elementos (Figura 5). Igualmente, permite administrar las funcionalidades de la seguridad de acceso a la red basada en los derechos de autorización:

- Nivel de acceso (administrador, operador, técnico y supervisor).
- Nivel de dispositivo (escribir, leer y sin acceso).
- Arquitectura de perfil de usuario.

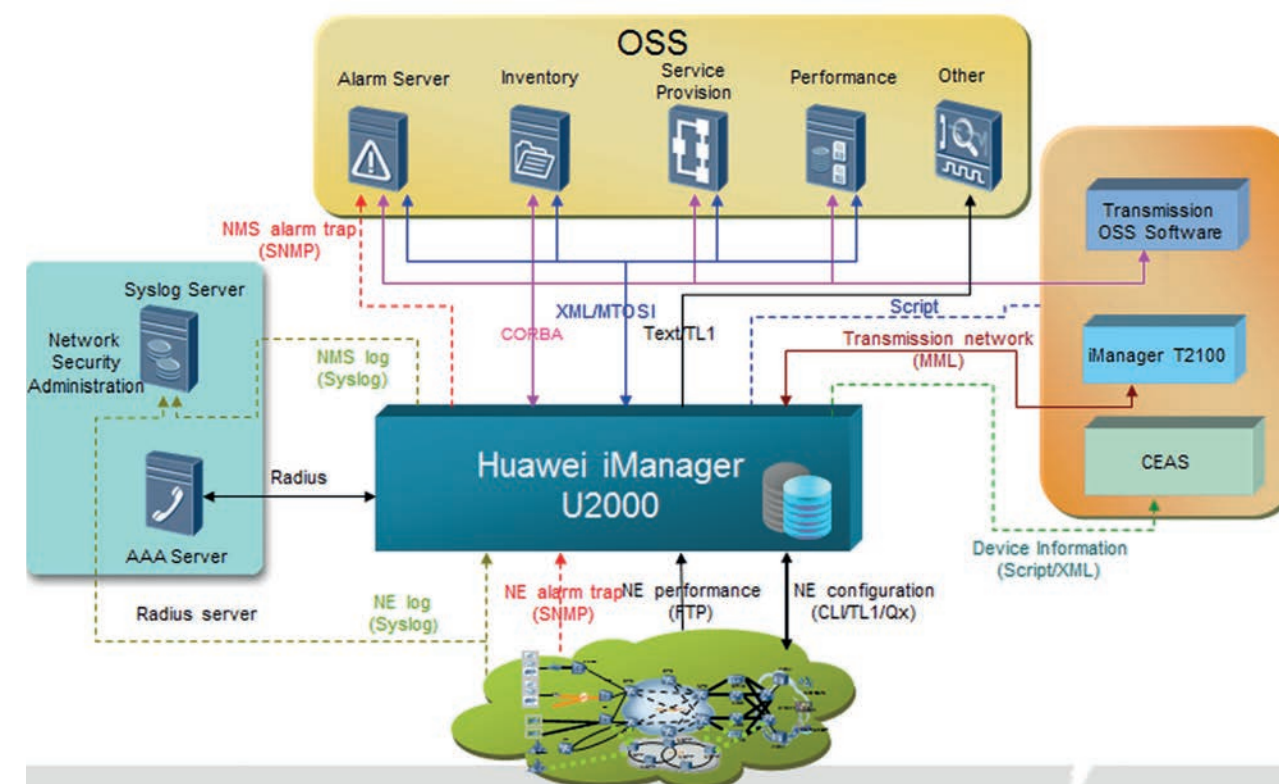


Figura 4. Estructura de la plataforma U2000. Fuente: Elaboración propia.

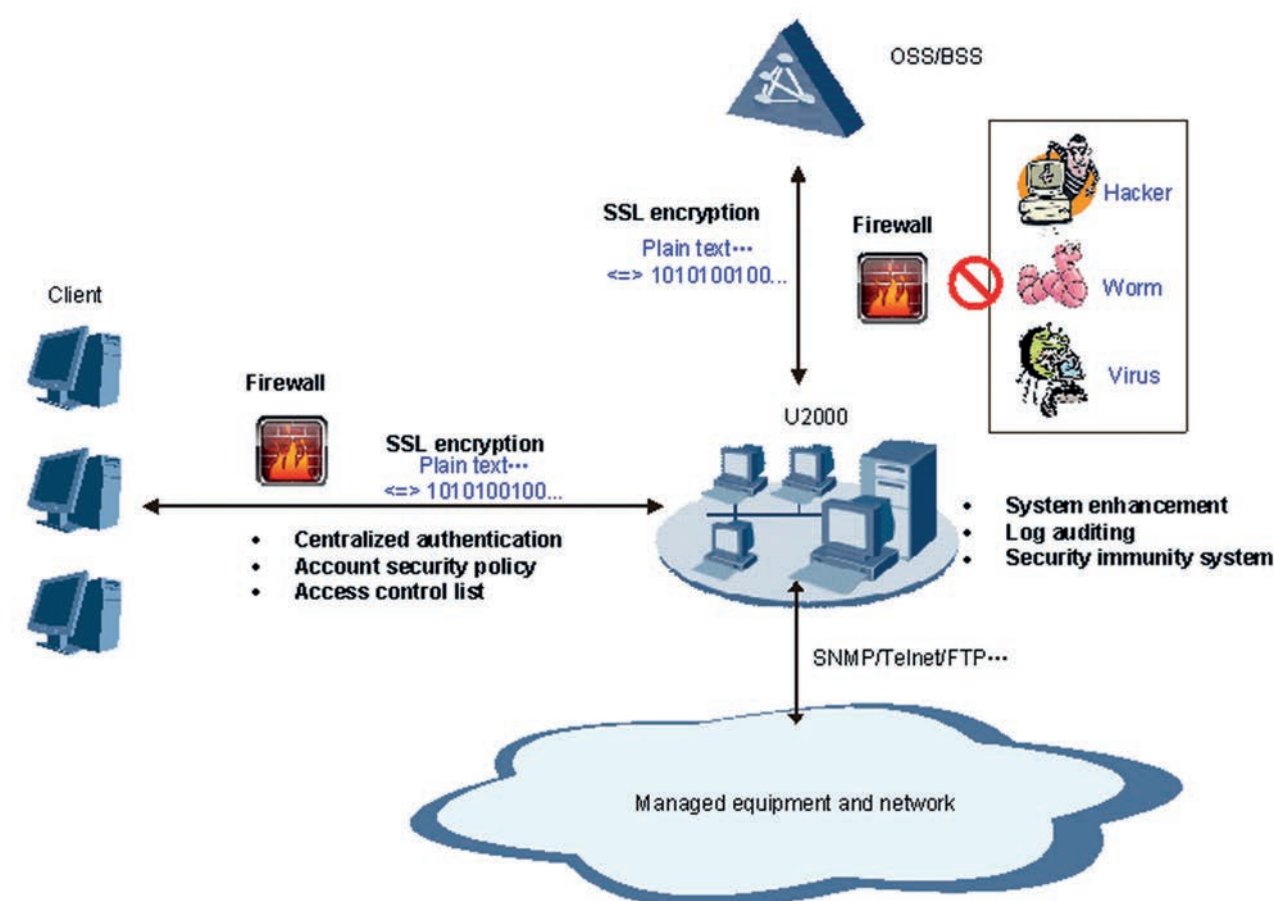


Figura 5. Configuración de seguridad del sistema. Fuente: Elaboración propia.

Gestión de fallas: Función de *backup* y restauración de toda la red que facilita la recuperación tras una pérdida en el servidor. Si la aplicación U2000 levanta y se le puede acceder es muy sencilla y amigable la restauración. Se encarga de un monitoreo constante de la red y todos lo que en ella está, como equipos y servicios. Detecta la dificultad y muestra por una serie de eventos su criticidad con la posible solución y causa.

Gestión de prestaciones: Muestra las alarmas dependiendo del estado del enlace y los umbrales declarados por el mismo sistema o por el operador. Puede registrarse y observar el rendimiento total de la red y las tasas de error. Se pueden definir umbrales para clientes y servicios específicos con diversas variables, tales como tasas de error para la alarma inmediata del estado de la red.

Gestión de contabilidad: No cuenta con esta funcionalidad porque la información brindada por el U2000 es sobre anchos de bandas y facilidades para grandes clientes conectados directamente a los equipos de la red, no facturándose al cliente por esta información.

Para implementar todas las áreas funcionales con la plataforma iManager U2000 [4] y el equipamiento propietario de Huawei se necesita revisar las MIB que permiten su gestión (tabla 1). Actualmente, se gestionan los elementos de la red MPLS de ETECSA con las MIB Propietaria de Huawei según el árbol de registro 1.3.6.1.4.1 IANA —*Registered Private Enterprises*— cuya asignación se puede revisar en: PRIVATE ENTERPRISE NUMBERS. El identificador para Huawei es 2011.

Aplicaciones MPLS

Una de las mayores potencialidades que presenta MPLS son las aplicaciones de esta tecnología, entre las que se encuentran:

• **Ingeniería de tráfico** — *Traffic Engineering* (TE)—: comprende los aspectos necesarios para lograr la optimización del desempeño de una red en estado operativo. El principal objetivo de la TE es facilitar operaciones de red fiables y eficientes en tanto se optimiza simultáneamente el uso de los recursos disponibles y el rendimiento de tráfico. En general, la TE comprende la aplicación de la tecnología y de los principios científicos a la medición, modelado, caracterización y control del tráfico en Internet. Los objetivos más importantes asociados con la TE pueden ser clasificados así:

- **Objetivos de funcionamiento orientados al Tráfico:** comprende los aspectos que mejoran la calidad de servicio de los flujos de tráfico. En redes Best effort, estos parámetros de desempeño vienen dados por minimización del retardo, minimización de pérdidas, maximización del *throughput*, entre otros.

- **Objetivos de funcionamiento orientados a los Recursos:** se refiere a los aspectos que brinden una optimización en el uso de los recursos. Adicionalmente, los mecanismos de la Ingeniería de Tráfico están clasificados en dos tipos básicos, acorde a la escala de aplicación que se quiere abarcar.

- **TE Dependiente de Tiempo:** los algoritmos de control de tráfico son utilizados para optimizar el uso de los recursos de la red en respuesta a variaciones de tráfico medidos en una escala de tiempo muy larga.

- **TE Dependiente del Estado:** los algoritmos o mecanismos de control de tráfico se deben adaptar a los cambios de estado que sufre la red en forma casi instantánea.

- **Calidad de servicio (QoS) y Clases de servicios (CoS):** una de las características clave de MPLS, comparado con redes tradicionales como Frame Relay y ATM, es que está

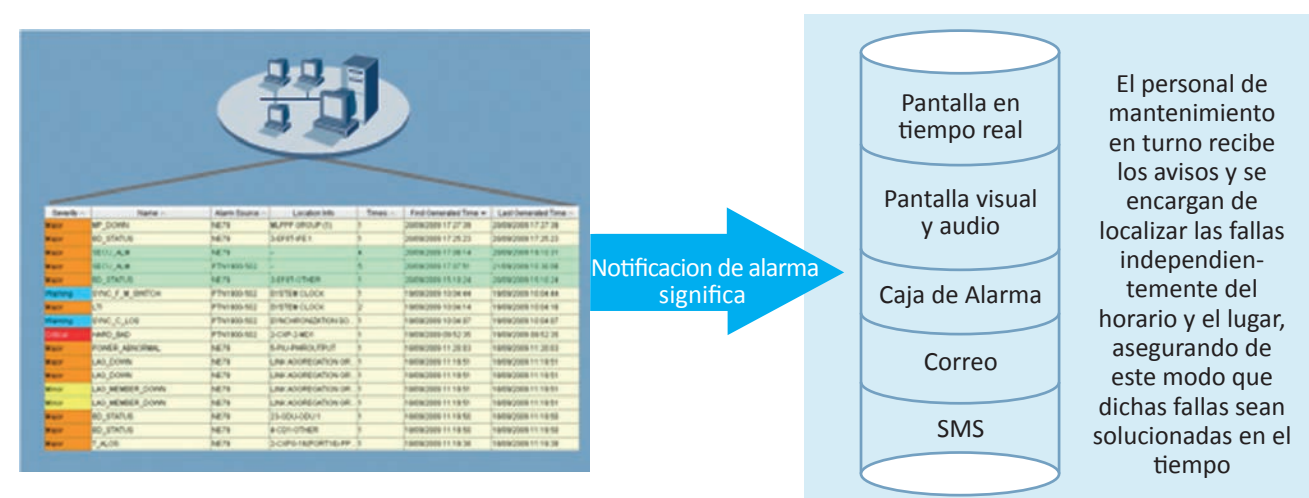
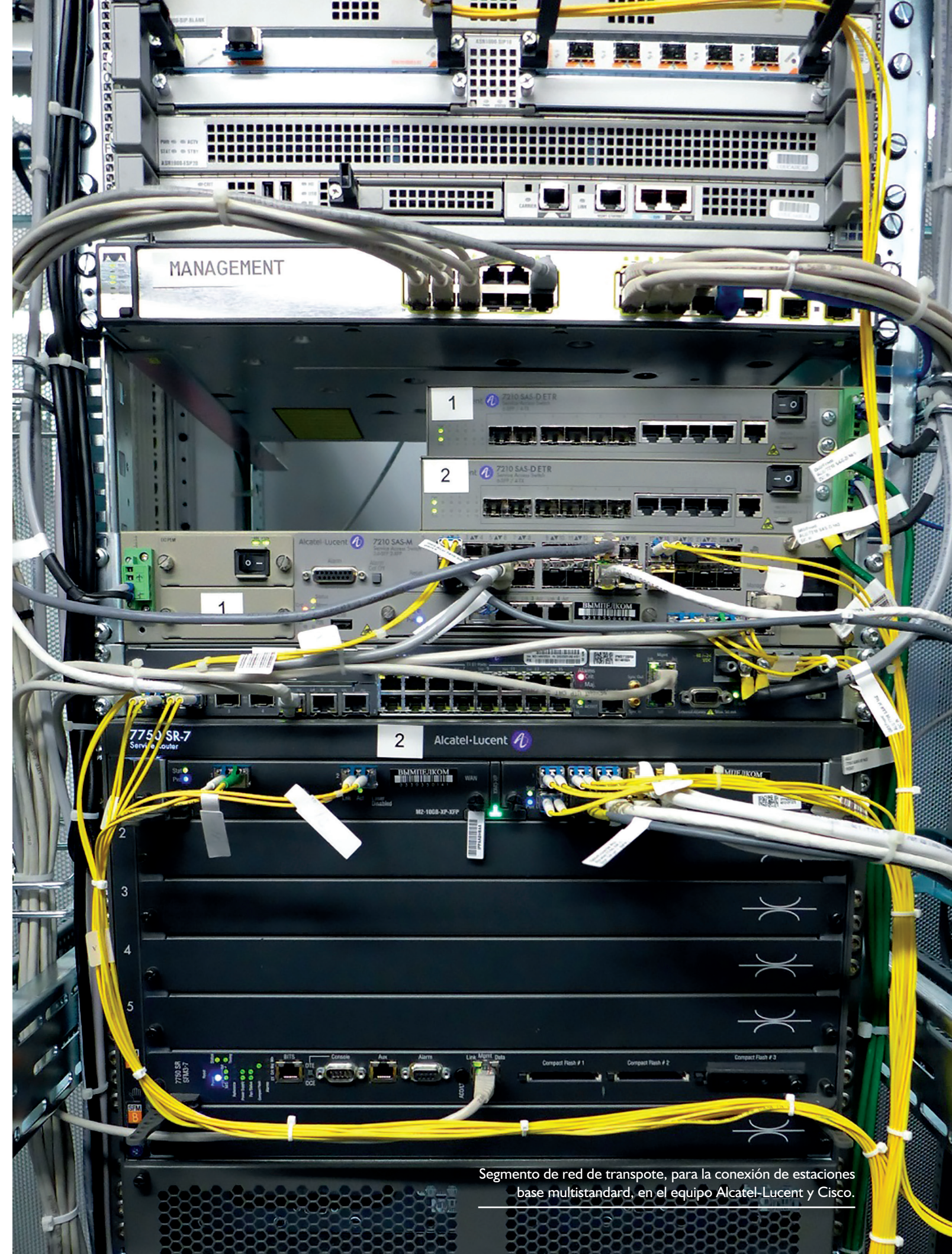


Figura 6. Ejemplo de registro de alarmas y mecanismos de notificación. Fuente: Elaboración propia.



Segmento de red de transpote, para la conexión de estaciones base multistandard, en el equipo Alcatel-Lucent y Cisco.

diseñado para proveer servicios garantizados. Así mismo, está orientado a la conexión por naturaleza lo que garantiza el tráfico IP. Por otra parte, QoS y clases de servicios son factores fundamentales de esta tecnología y pueden ser implementados a través de la Ingeniería de Tráfico. Esta capacidad permite proveer a los distintos usuarios de un servicio de nivel estable SLA —*Service Level Agreements*— en aspectos como ancho de banda, tiempo de demora, y variación del mismo.

Varios mecanismos son los que utiliza MPLS para dar estabilidad de QoS y CoS dentro de su red. En el modelo InterServ —Integrated Services—, RSVP obtiene los requerimientos para establecer un flujo de tráfico con QoS, permitiendo a los distintos LSR las negociaciones necesarias para generar un tráfico garantizado y además parámetros o recursos como ancho de banda y latencia del tipo *end to end*.

El modelo DiffServ —*Differentiated Services*— del IETF define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio (CoS), otorgando un servicio no necesariamente garantizado para el curso del tráfico con diferentes prioridades. Para ello se emplea el campo ToS —*Type of Service*—, en la cabecera de paquete IP para proveer esta clasificación.

VPN

Una VPN [2] —*Virtual Private Network*— es una tecnología en la que se establecen canales seguros de comunicación que ofrecen protección a los datos transmitidos mediante el uso de algoritmos de encriptación y/o autenticación criptográfica. Tecnología punto a punto, ampliamente adopta-

da en ambientes de transacciones financieras, y/o redes que requieren confidencialidad permanente, tanto en redes privadas como entre proveedores de Servicio de Internet y sus clientes. En el mercado existe una gran variedad de soluciones VPN; sin embargo, aquí solo se discutirá VPN MPLS. Las VPN permiten la interconexión de oficinas y sucursales de un entorno corporativo, interconectadas vía VPN usando la Internet como *backbone* de su red. Los servicios de seguridad de IPSec —*Internet Protocol Security*— son ampliamente utilizados para la implementación de VPN.

En la plataforma que analizamos permite la configuración y administración de las VPN, servicio dirigido principalmente hacia las empresas del país con el objetivo de brindar conectividad entre las oficinas o sucursales del propio organismo con representación a nivel nacional. (Figura 7).

Conclusiones

En el momento actual, todos los proveedores de servicios tienen ante sí el enorme reto de gestionar redes cada vez más complejas y extensas, con una mayor gama de servicios y con creciente demanda de ancho de banda, calidad y garantías. MPLS abre a los proveedores IP la oportunidad de ofrecer nuevos servicios que no son posibles con las técnicas actuales de encaminamiento IP.

MPLS es el último paso en la evolución de las tecnologías de conmutación multinivel. La idea básica de separar el plano de control y el de envío permite que cada una de ellas se pueda implementar y modificar de manera independiente, lo que crea una poderosa herramienta para poder gestionar de mejor forma las redes y a su vez permite que pueda funcionar sobre cualquier tecnología de transporte

facilitando de modo significativo la migración para las redes de próxima generación.

MPLS es una red bastante segura ya que no permite que los datos entren o salgan del LSP por lugares que no han sido establecidos por el administrador de la red, además, cuando los datos entran en el dispositivo para conmutarse no son vistos por capas superiores más que por el módulo de envío MPLS, esto crea un entorno riguroso y a la vez

flexible con lo cual se puede implementar redes virtuales y privadas MPLS, mediante la construcción de túneles con etiquetas apiladas.

Con la plataforma iManager U2000 podemos concluir que se puede administrar las tres potencialidades que brinda el estándar MPLS, lo que evidencia la presencia de las áreas funcionales para una eficiente administración de cada componente configurado.

Referencias bibliográficas

- [1] Web Wikipedia, California, 20 de mayo del 2001, RFC 3031, MPLS.
- [2] Peter Tomsu, Gerhard Wieser. MPLS-Based VPNs Designing Advanced Virtual Networks. Prentice Hall. Revista de Telecomunicaciones de Alcatel Lucent – No.1
- [3] HedEx iManager U2000_V100R006C00_03_en_31185393 de Huawei.
- [4] HedEx iManager U2000_V100R006C00_02_en_31185395 de Huawei.
- [5] J. Witters, J. De Clercq, S. Khandekar, Tutorial técnico del vpls, Revista de Telecomunicaciones de Alcatel - 4º trimestre de 2004.

(Artículo recibido en septiembre de 2016 y aprobado en noviembre de 2016)

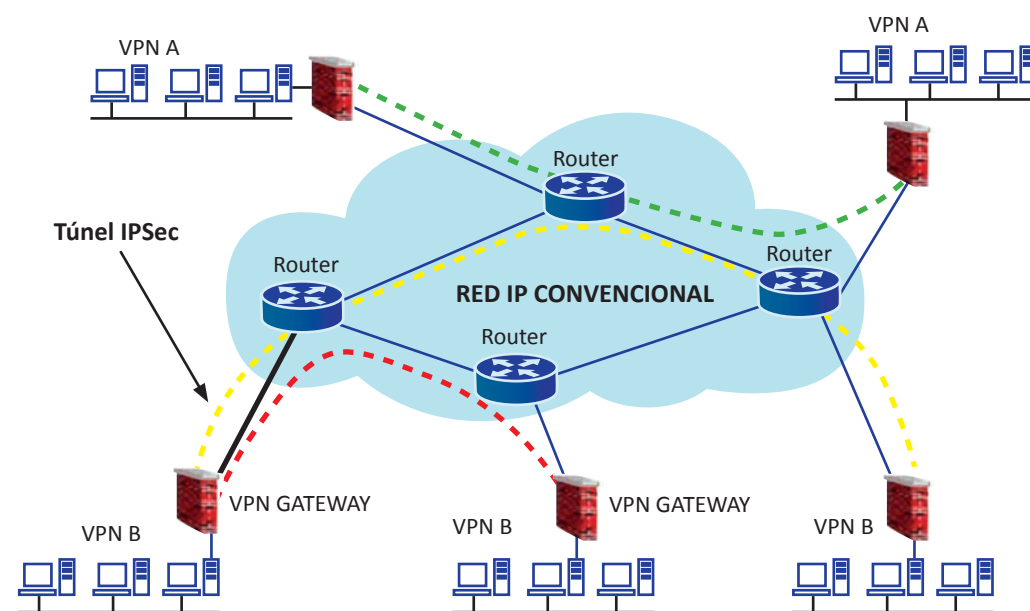


Figura 7. Ejemplo de interconexión de redes por VPN utilizando red MPLS. Fuente: Elaboración propia.