Aplicaciones de MPLS, Transición de IPv4 a IPv6 y Mejores Prácticas de Seguridad para el ISP Telconet

Aguirre L. * **González F.** * **Mejía D.** *

* *Escuela Politécnica Nacional, Facultad de Ingeniería Electrica y Electrónica Quito, Ecuador (e-mail: lizeth.aguirre@ieee.org ; {fabio.gonzalez ; david.mejia}@epn.edu.ec)*

Resumen: *El presente proyecto propone mejoras a la red de Telconet S.A. a fin de optimizar el uso de sus recursos con la implementación de las aplicaciones de MPLS, brindar soporte a IPv4 e IPv6 de manera simultánea y establecer una red segura en base a las mejores prácticas de seguridad para IPv6; logrando así ofrecer servicios de calidad. Se describen los principales componentes y aplicaciones de MPLS, los mecanismos de transición de IPv4 a IPv6 y las mejores prácticas de seguridad en IPv6. Finalmente, se presentan los resultados obtenidos de un prototipo que implementa una parte de la red.*

Palabras clave: *MPLS, Aplicaciones de MPLS, Ingeniería de Tráfico, QoS, VPN, Transición IPv4-IPv6, Mejores Prácticas de Seguridad.*

Abstract: *This project proposes improvements to the network of Telconet S.A. to optimize the use of resources by implementing MPLS applications, to support IPv4 and IPv6 simultaneously and to establish a secure network based on IPv6 security best practices; thus achieving deliver quality services. It describes the main components and MPLS applications, the transition mechanisms from IPv4 to IPv6 and security best practices in IPv6. Finally, it shows the results obtained from a prototype that implements part of the network.*

Keywords:*MPLS, MPLS Applications, Traffic Engineering, QoS, VPN, Transition from IPv4 to IPv6, Security Best Practices.*

1. INTRODUCCIÓN

Las redes de comunicaciones han sufrido varios cambios durante las últimas décadas. Debido a las nuevas aplicaciones y servicios, los ISP (*Internet Service Provider*) han tenido que adaptar nuevas y mejores tecnologías para ofrecer calidad, seguridad y confiabilidad a sus clientes.

MPLS (*Multiprotocol Label Switching*) [10] es una tecnología de transporte que utiliza etiquetas de tamaño fijo y pequeño para establecer la conmutación y brindar rapidez en el reenvío de paquetes. Fue estandarizada por la IETF (*Internet Engineering Task Force*) en el RFC (*Request for Comments*) 3031 en el año 2001 y opera entre las capas enlace de datos y red del modelo OSI. Esta tecnología presenta como ventajas la velocidad de envío de la capa enlace de datos y la inteligencia de enrutamiento de la capa de red. Se han desarrollado varias aplicaciones para MPLS como VPN (*Virtual Private Networks*) [7], Ingeniería de Tráfico y Calidad de Servicio [5].

El ISP Telconet S.A., ante el agotamiento de las direcciones IPv4 (*Internet Protocol version* 4), la necesidad de soportar los protocolos IPv4 e IPv6 (*Internet Protocol version* 6) de forma simultánea en la red, el incremento de tráfico debido a las aplicaciones de los clientes y la implementación de un Centro de Datos, requiere alternativas que le permitan seguir siendo un ISP competitivo, ofreciendo a sus clientes servicios de calidad.

El presente documento presenta el prototipo de red implementado para Telconet S.A., en el cual se muestran las ventajas de emplear las aplicaciones de MPLS y el soporte de IPv4 e IPv6 de forma simultánea en la red, así como también el empleo de las mejores prácticas de seguridad para IPv6.

2. MPLS

Una red MPLS está constituida por dispositivos de borde conocidos como routers LER (*Label Edge Router*) o PE (*Provider Edge*) y dispositivos de núcleo conocidos como

routers LSR (*Label Switching Router*) o P (*Provider*). En la Fig. 1 se muestran los componentes de una red MPLS.

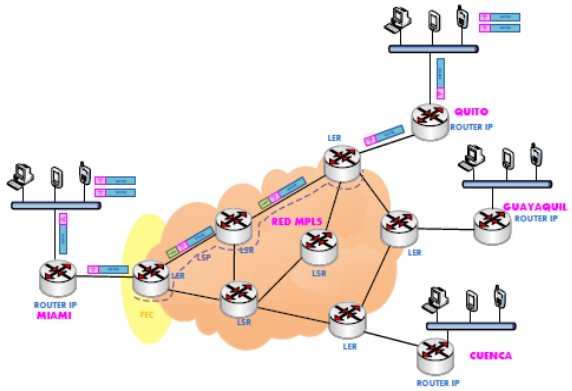

Figura 1. Componentes de la red MPLS.

Entre los routers LER se forma una malla de túneles unidireccionales conocidos como LSP (*Label Switched Path*), la cual permite que cuando un paquete ingrese a la red a través de un LER de ingreso (*ingress* LER), pueda ser transportado hasta el LER de egreso (*egress* LER) apropiado. El router LER de ingreso asocia los paquetes por primera y única vez a una determinada FEC (*Forwarding Equivalence Class*) a través de la asignación de una etiqueta; es por ello que los paquetes que pertenecen a un mismo flujo, recibirán el mismo tratamiento de transporte aunque sus destinos finales puedan ser diferentes.

MPLS ofrece un mecanismo para manipular el tráfico de diferentes aplicaciones con requerimientos de Calidad de Servicio QoS (*Quality of Service*), optimización del uso de recursos mediante Ingeniería de Tráfico TE (*Traffic Engineering*) y seguridad mediante Redes Privadas Virtuales VPN (*Virtual Private Network*) [2].

2.1 Redes Privadas Virtuales

Las VPN de MPLS son las implementaciones más populares de las aplicaciones de la tecnología MPLS, ya que ofrecen escalabilidad, son sencillas de administrar y permiten dividir la red del proveedor, en redes más pequeñas con tablas de enrutamiento separadas. Se definen dos tipos de conexiones VPN: VPN de MPLS de capa 2 y VPN de MPLS de capa 3.

2.2 Calidad de Servicio

Es el mecanismo que permite priorizar diferentes aplicaciones que circulan por la red, garantizando uno o varios de los parámetros que las definen, como son: ancho de banda, retardo, jitter y pérdida de paquetes [3].

Las CoS (*Class of Service*) permiten diferenciar el tráfico que circula por la red en: crítico, como la voz y el vídeo; y no tan crítico, como el correo electrónico y la transferencia de archivos. Para determinar el tratamiento que reciben los paquetes durante su retransmisión en la red, se definen los mecanismos de envío y encolamiento a través de los PHB (*Per-Hop Behaviors*) previamente establecidos. Los PHB son, comportamientos que se realizan en cada router.

2.3 Ingeniería de Tráfico

La Ingeniería de Tráfico permite reducir el costo de las operaciones mediante el control de tráfico y la optimización del uso de los recursos, previniendo situaciones en las que partes de la red se encuentren sobreutilizadas (congestionadas) mientras otras, están siendo subutilizadas. El concepto del mejor camino en Ingeniería de Tráfico no implica escoger el camino más corto, sino aquel que para determinado momento está disponible y es el más rápido independientemente de la distancia.

3. MECANISMOS DE TRANSICIÓN DE IPV4 A IPV6

La migración completa de las redes a IPv6 no es aún una solución viable debido a los altos costos que esto implica. Se presentan tres posibles mecanismos de transición [12]:

3.1 IPv6 sobre Circuitos de Transporte en MPLS

Es un mecanismo de transición que emplea túneles de capa 2 configurados en los routers LER permitiendo la ejecución nativa de IPv6 en redes MPLS. Una de las ventajas más significativas es que no se requieren cambios en los routers LSR, por lo que se considera un mecanismo fácil de implementar y transparente para el usuario. Sin embargo, presenta limitaciones relacionadas a la escalabilidad debido a que cuando la red crezca, la malla compuesta por los enlaces dedicados será más tediosa de implementar y gestionar.

3.2 IPv6 con Túneles en los routers CE

En este mecanismo se implementan túneles tradicionales configurados en los routers CE (*Customer Edge*), los cuales soportan tanto IPv4 como IPv6. El funcionamiento de la red MPLS no se ve alterado ya que los paquetes IPv6 serán encapsulados en paquetes IPv4 para su transporte en la red. El principal inconveniente se presenta en la escalabilidad ya que si la red empieza a crecer, la cantidad de túneles que el administrador debe configurar también se incrementa.

3.3 IPv6 Provider Edge Routers (6PE)

Permite transportar paquetes IPv6 a través de la red MPLS mediante MP-BGP (*Multiprocol-Border Gateway Protocol*). 6PE [8] es un mecanismo escalable, dinámico y excelente para trabajar en redes grandes y pequeñas, ya que no requiere cambios en las configuraciones de

los routers LSR. Sin embargo, necesita que los routers LER tengan soporte tanto del protocolo IPv4 como del protocolo IPv6. Si a este mecanismo se implementan VPN de capa 3 en IPv6, se lo denomina 6VPE (IPv6 VPN *Provider Edge*).

4. MEJORES PRÁCTICAS DE SEGURIDAD EN IPV6

Las mejores prácticas de seguridad de una red buscan definir una estrategia de seguridad adecuada en IPv6 [6, 13], a fin de minimizar las amenazas que atenten contra la confidencialidad, la integridad y la disponibilidad de la información de la empresa; así como prevenir los posibles ataques a la misma. A continuación se mencionan tres de las mejores prácticas de seguridad:

(1) **VLAN:**Son la manera más sencilla de brindar seguridad en capa 2, ya que permiten dividir la red en segmentos más pequeños independientes lógicamente.
(2) **Listas de Control de Acceso:** Son filtros que permiten o deniegan el acceso a los recursos de la red. El filtro puede definirse en base a: las direcciones IP, los protocolos de capa superior y los puertos. IPv6 solo tiene soporte para las ACL (*Access Control List*) extendidas nombradas.
(3) **Acceso Remoto Seguro:** SSH (*Secure Shell*) [4] permite el acceso remoto a dispositivos a través de la red, haciendo uso de conexiones seguras, implementando autenticación y proporcionando terminales con sesiones cifradas.

5. PROPUESTA DE MEJORAS PARA LA RED DE TELCONET S.A.

Telconet S.A se ha caracterizado por ser un proveedor muy competitivo en el mercado ecuatoriano; sin embargo, requiere adaptar un mecanismo que, adicionalmente, le permita brindar servicios en IPv6.

Con 6PE/6VPE no se requiere cambios en el núcleo de la red, por lo que se considera uno de los mecanismos de transición más empleados, ya que utilizan el protocolo MP-BGP para establecer sesiones entre los routers LER sin alterar las configuraciones de los routers LSR. En 6PE se definen las familias de direcciones: IPv4 e IPv6; mientras que en 6VPE, se establece la comunicación con las familias de direcciones: VPNv4 (96 bits), VPNv6 (128 bits), IPv4 e IPv6 asociadas a cada VRF (*Virtual Routing and Forwarding*).

La implementación de las VPN en MPLS resulta sencilla, ya que no se requiere ningún protocolo adicional a LDP (*Label Distribution Protocol*) para la distribución de las etiquetas en la red. Para las VPN de capa 2, el ISP brinda el transporte de los paquetes pero no su enrutamiento; es por ello que se utiliza la encapsulación MPLS para el establecimiento de los pseudowires. Las VPN de capa 2 se deben configurar solo en las interfaces y subinterfaces de los routers LER, y se debe especificar la dirección IP remota con el VC (*Virtual Circuit*) establecido y la encapsulación de MPLS. Mientras que para las VPN de capa 3 se deben definir los valores RD (Route Distinguisher) y RT (*Route Target*) y levantar las sesiones MP-BGP para cada VRF. Una VRF puede incluir una o más interfaces, pero la interfaz solo puede pertenecer a una VRF.

La Calidad de Servicio se establece a través de mapas de políticas que permitan limitar el tráfico y controlar la congestión. Se define una política para limitar el tráfico y se la configura en las interfaces de los routers LER que controla las velocidades de los clientes a través del mecanismo traffic policing. Posteriormente, se configura un mapa de políticas para definir el mapa de correspondencias entre los campos DSCP (*Differentiated Services Code Point*) y EXP (renombrado como el campo TC - *Traffic Class*) [1] de los paquetes. Se marca el campo EXP de la cabecera MPLS con el PHB respectivo para que cada router de la red lo identifique y lo asocie a una clase. Se designaron 6 Clases de Servicios para Telconet:

- La clase Routing en la que se incluye los protocolos de enrutamiento usados en la red a fin de mantener activas las sesiones aun cuando exista congestión.
- La clase *Platinum* garantiza preferencia al tráfico de voz.
- La clase *Gold* se encarga de dar preferencia a las aplicaciones de vídeo.
- La clase *Silver* se orienta al tráfico de los clientes corporativos VIP con altas prestaciones de acceso.
- La clase *Bronze* se orienta al tráfico de los clientes corporativos.
- La clase *Best-Effort* no recibe ningún trato preferencial e incluye las aplicaciones que no han sido marcadas en las clases anteriores

En la Tabla 1 se detallan las CoS definidas para la red, los PHB establecidos, las aplicaciones incluidas y el porcentaje de ancho de banda (BW – *Bandwitdh*) asignado para cada una de ellas.

El esquema de QoS [9] permitirá brindar tratamiento diferencial a las Clases de Servicios y en caso de congestión, garantizar prioridad a las aplicaciones más críticas de la red.

Posteriormente, se crea un mapa de políticas adicional para el manejo de la congestión de los dispositivos de la capa núcleo, a fin de brindar tratamientos diferenciales a los paquetes de cada clase durante su transmisión por la red MPLS. Como mecanismo de encolamiento se seleccionó LLQ (*Low-Latency Queuing*), gracias a que garantiza una cola prioritaria y varias colas con prioridades personalizadas y como mecanismo de evasión de la congestión, se seleccionó WRED (*Weighted Random Early Detection*)

porque permite descartar los paquetes probabilísticamente evitando, en lo posible, que las colas se llenen. Para el manejo de la congestión en las capas distribución y acceso, se confían en los valores que vienen marcados en el subcampo DSCP y se utiliza como mecanismo de encolamiento SRR (*Shared/Shaped Round Robin*), porque permite obtener la máxima eficiencia de un sistema de encolamiento.

Para la Ingeniería de Tráfico se requiere previamente disponer de los protocolos: OSPF (*Open Shortest Path First*), CEF (*Cisco Express Forwarding*) y LDP. Para el balanceo de carga en TE se establecen túneles explícitos y dinámicos con prioridades y anchos de banda iguales entre los routers LER, a fin de que el tráfico pueda distribuirse entre dos o más túneles hacia un mismo destino.

Tabla 1: *Per-Hop Behaviors.*

CoS	PHB	Aplicaciones	BW
Routing	CS7, CS6	Protocolos de enrutamiento: OSPF, BGP y LDP	5% Prioritario
Platinum	EF	Voz	10% Prioritario
Gold	AF41	Videoconferencia	15%
Silver	AF31	Datos de los clientes corporativos VIP	35%
Bronze	AF21	Datos de los clientes corporativos	30%
Best-Effort	0	Protocolos: SMTP, ICMP, HTTP, DNS, etc.	-

Además, se pueden proteger los enlaces de la red mediante el mecanismo Fast Re-Route que ofrece protección de enlaces reenrutando el tráfico del túnel principal por un túnel de respaldo previamente configurado.

Para la encapsulación de los enlaces troncales en las VLAN se emplea el protocolo IEEE 802.1Q, que permite compartir un medio físico entre varias redes. No se recomienda emplear el valor por defecto de la VLAN de administración nativa (VLAN 1) sino cambiarla por otro valor.

La implementación de las ACL en IPv4 e IPv6 debe limitar el tráfico en los equipos de la red de los protocolos: HTTP (80), HTTPS (443), FTP (20), FTP-data (21) y TFTP (69). Para la gestión de los dispositivos se establecerá el acceso remoto seguro SSH en IPv4 e IPv6. Además, se utiliza: el algoritmo de cifrado RSA con llaves de 1.024 bits, la versión 2 de SSH y se limita el número de reintentos de autenticación a 1 y el tiempo de conexión sin actividad a 30 segundos.

6. PROTOTIPO DE RED

El prototipo de red MPLS tiene como objetivo demostrar las propuestas planteadas en una red de baja escala. El prototipo está conformado por 9 dispositivos: 2 routers LER, 3 routers LSR, 2 switches de acceso y 2 routers CE, como se indica en la Fig. 2. Los equipos LSR (P) tienen por nombre: PDATACENTER, PGOSSEAL y PGYE, los equipos LER (PE) son PE1MUROS y PE1GOSSEAL, los switches de acceso son SW1COLON y SW1PLAZATOROS y los equipos CE son CE1PLAZATOROS_ CLIENTE y CE1COLON_ CLIENTE; además, se dispone de un equipo que permite generar tráfico (IXIA 400T).

Se han considerado tres routers LSR en el prototipo a fin de tener enlaces redundantes que permitan presentar las funcionalidades de Ingeniería de Tráfico. El PGYE simula la red de la matriz Guayaquil, y permitirá ofrecer un camino redundante para el tráfico de la red de Quito.

Por otro lado, se definen 4 VLAN: la VLAN 11 que simula un cliente con servicios en IPv4, la VLAN 22 que simula un cliente con servicios en IPv4 e IPv6, la VLAN 169 nativa para administración y la VLAN 100 que permitirá simular un cliente con servicios de transporte de capa 2 (VPN de capa 2). Los detalles de la configuración y pruebas realizadas se encuentran en [11].

(1) **Configuración básica:** Después de interconectar los dispositivos como se indica en la Fig. 2, se debe establecer la configuración básica de red en los equipos de conectividad, como: los nombres de los equipos, la contraseña del modo EXEC, el mensaje del día, la contraseña de consola, la contraseña de las líneas de terminal virtual y las direcciones IP de las interfaces, entre otros. Además, se debe definir un protocolo de enrutamiento dinámico como OSPF, con el SA correspondiente a Telconet (AS27947). Las sesiones OSPF serán identificadas mediante los router-id que estarán asociados a la dirección IP de la interfaz loopback0 definidos en cada dispositivo de red. Finalmente, se debe configurar la tecnología MPLS para lo cual, es necesario habilitar CEF y LDP.

(2) **Mecanismo de transición IPv4 a IPv6:** 6PE/6VPE se habilita con la configuración del protocolo BGP mediante la creación de las familias de direcciones establecidas entre los routers LER de la red, sin alterar las configuraciones de los LSR. Por ejemplo, en la Fig. 3 se detallan las sesiones IPv4 y VPNv4 establecidas con el PE1GOSSEAL (5.5.5.5).

Para verificar que las sesiones en 6PE fueron establecidas, se debe aprender, mediante el protocolo BGP, las direcciones IPv6 del LER remoto y almacenarlas en la tabla de enrutamiento IPv6. En la Fig. 4 se puede apreciar que la red 2001:29:2:41::/64 que pertenece al PE1MUROS, fue aprendida y almacenada en la tabla de enrutamiento general del PE1GOSSEAL, gracias a la sesión BGPv6 establecida entre ambos equipos. Es importante señalar que a pesar de que los LSR se encuentran inmersos en este proceso, su responsabilidad será solo de transporte.

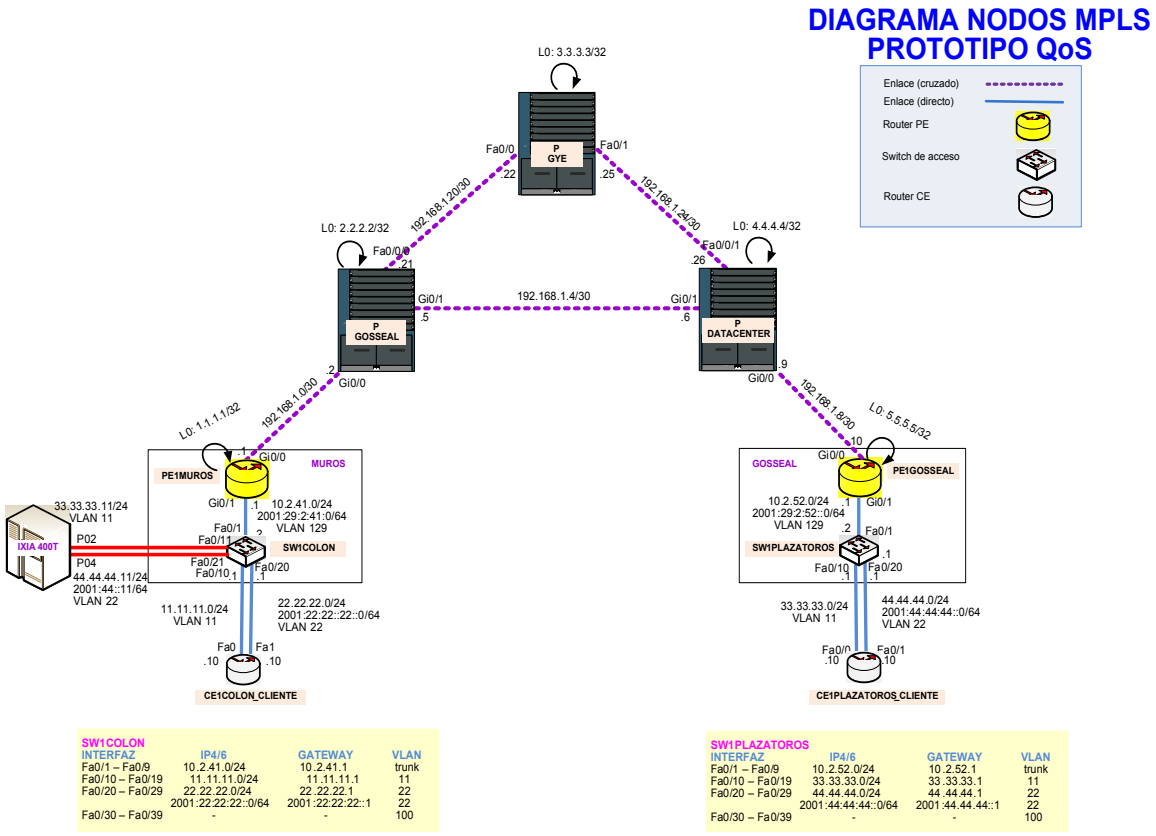

Figura 2. Prototipo de red MPLS

Mientras que en 6VPE, las direcciones IPv6 serán aprendidas, a través del protocolo BGP y de manera independiente almacenadas en la tabla de enrutamiento de la VRF establecida. En la Fig. 5, se indica la tabla de enrutamiento de la VRF INTERNET donde la red 2001:44:44:44::/64, perteneciente a la VLAN 22 (CE1PLAZATOROS), fue aprendida mediante el protocolo BGPv6 y almacenada en la tabla de la VRF creada.

```
PE1MUROS#sh ip bgp all summ
For address family: IPv4 Unicast
BGP router identifier 1.1.1.1, local AS number 27947
BGP table version is 30, main routing table version 30
7 network entries using 840 bytes of memory
7 path entries using 364 bytes of memory
4/4 BGP path/bestpath attribute entries using 496 bytes of memory
3 BGP extended community entries using 104 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1804 total bytes of memory
BGP activity 20/8 prefixes, 26/14 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
5.5.5.5         4        27947       9       9       30    0    0 00:00:52        4

For address family: VPNv4 Unicast
BGP router identifier 1.1.1.1, local AS number 27947
BGP table version is 15, main routing table version 15
4 network entries using 576 bytes of memory
4 path entries using 208 bytes of memory
4/4 BGP path/bestpath attribute entries using 528 bytes of memory
3 BGP extended community entries using 104 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 1416 total bytes of memory
BGP activity 20/8 prefixes, 26/14 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
5.5.5.5         4        27947       9       9       15    0    0 00:00:53        2
PE1MUROS#
```

Figura 3: Verificación de las sesiones BGP establecidas

(3) **VPN de MPLS:** Las VPN de capa 2 se configuran en los routers LER estableciendo la ruta de transporte pero, debido a que el enrutamiento de estas VPN está a cargo de los clientes, no habrá solapamiento de las redes utilizadas entre el proveedor y el cliente. En la Fig. 6, se muestra el estado de una VPN de capa 2 establecida entre los PE de la red, a través de los router-id. Por el contrario, las VPN de capa 3 se pueden establecer en IPv4 e IPv6 simultáneamente, a través de las VRF configuradas de doble pila en los routers LER.

```
PE1GOSSEAL#sh ipv6 route
IPv6 Routing Table - default - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
B   2001:29:2:41::/64 [200/0]
     via 1.1.1.1%default, indirectly connected
C   2001:29:2:52::/64 [0/0]
     via GigabitEthernet0/1.129, directly connected
L   2001:29:2:52::1/128 [0/0]
     via GigabitEthernet0/1.129, receive
L   FF00::/8 [0/0]
     via Null0, receive
PE1GOSSEAL#
```

Figura 4: Tabla de enrutamiento general en IPv6

Para verificarlas, se realizan pruebas de conectividad (mediante envío de paquetes ICMP) a las direcciones IP incluidas en las VRF y aprendidas en las tablas de enrutamiento de las VRF como se indica en la Fig. 5.

(4) **Calidad de Servicio:** Las ventajas de QoS se comprueban saturando los enlaces, para ello se utiliza un generador de tráfico que envía paquetes marcados con cada una de las seis clases configuradas.

```
PE1MUROS#sh ipv6 route vrf INTERNET
IPv6 Routing Table - INTERNET - 4 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, HA - Home Agent, MR - Mobile Router, R - RIP
       I1 - ISIS L1, I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary
       D - EIGRP, EX - EIGRP external, ND - Neighbor Discovery
       O - OSPF Intra, OI - OSPF Inter, OE1 - OSPF ext 1, OE2 - OSPF ext 2
       ON1 - OSPF NSSA ext 1, ON2 - OSPF NSSA ext 2
C   2001:22:22:22::/64 [0/0]
     via GigabitEthernet0/1.22, directly connected
L   2001:22:22:22::1/128 [0/0]
     via GigabitEthernet0/1.22, receive
B   2001:44:44:44::/64 [200/0]
     via 5.5.5.5%default, indirectly connected
L   FF00::/8 [0/0]
     via Null0, receive
PE1MUROS#
```

Figura 5. Tabla de enrutamiento en IPv6 de la VRF INTERNET

```
PE1MUROS#sh policy-map interface gi0/0
 GigabitEthernet0/0

  Service-policy output: POLITICA_MPLS_TO_MPLS_OUT

    queue stats for all priority classes:

      queue limit 64 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 8673001/12172678892

    Class-map: CLASE_ROUTING_MPLS (match-any)
      2466 packets, 758365 bytes
      30 second offered rate 1000 bps, drop rate 0 bps
      Match: ip precedence 6  7
        2299 packets, 746269 bytes
        30 second rate 1000 bps
      Match: mpls experimental topmost 6  7
        167 packets, 12096 bytes
        30 second rate 0 bps
      Priority: 5% (500 kbps), burst bytes 12500, b/w exceed drops: 0

    Class-map: CLASE_PLATINUM_MPLS (match-any)
      8670532 packets, 397161188468 bytes
      30 second offered rate 1037934000 bps, drop rate 0 bps
      Match: mpls experimental topmost 5
        8670532 packets, 397161188468 bytes
        30 second rate 1037934000 bps
      Priority: 10% (1000 kbps), burst bytes 25000, b/w exceed drops: 0

    Class-map: CLASE_GOLD_MPLS (match-any)
      4528105 packets, 212382818517 bytes
      30 second offered rate 683763000 bps, drop rate 0 bps
      Match: mpls experimental topmost 4
        4528105 packets, 212382818517 bytes
        30 second rate 683763000 bps
      Queueing
      queue limit 100 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 4528109/6357458626
      bandwidth 15% (1500 kbps)

    Class-map: CLASE_SILVER_MPLS (match-any)
      4527127 packets, 210023845163 bytes
      30 second offered rate 675456000 bps, drop rate 0 bps
      Match: mpls experimental topmost 3
        4527127 packets, 210023798046 bytes
        30 second rate 675456000 bps
      Queueing
      queue limit 100 packets
      (queue depth/total drops/no-buffer drops) 0/0/0
      (pkts output/bytes output) 4527131/6356079104
      bandwidth 35% (3500 kbps)

    Class-map: CLASE_BRONZE_MPLS (match-any)
      3764081 packets, 175340822205 bytes
      30 second offered rate 49526000 bps, drop rate 0 bps
      Match: mpls experimental topmost 2
        3764081 packets, 175340822205 bytes
        30 second rate 49526000 bps
      Queueing
      queue limit 100 packets
      (queue depth/total drops/no-buffer drops) 0/2352315/0
      (pkts output/bytes output) 1411767/1982117022
      bandwidth 30% (3000 kbps)
      shape (average) cir 4000000, bc 40000, be 40000
      target shape rate 4000000

    Class-map: class-default (match-any)
      4445498 packets, 199973383846 bytes
      30 second offered rate 591388000 bps, drop rate 14809000 bps
      Match: any
      Queueing
      queue limit 100 packets
      (queue depth/total drops/no-buffer drops) 42/2569393/0
      (pkts output/bytes output) 1876110/2633396454
        Exp-weight-constant: 9 (1/512)
        Mean queue depth: 41 packets
        dscp      Transmitted       Random drop      Tail drop          Minimu
      Maximum     Mark
                  pkts/bytes     pkts/bytes       pkts/bytes          thresh
     thresh     prob
```

Figura 6. Verificación de la política de salida en gi0/0

```
CE1COLON_CLIENTE#
CE1COLON_CLIENTE#ping 33.33.33.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 33.33.33.10, timeout is 2 seconds:
.!!..
Success rate is 40 percent (2/5), round-trip min/avg/max = 112/114/116 ms
CE1COLON_CLIENTE#
```

Figura 7: Verificación del envío de paquetes sin QoS

Se puede verificar que si se realiza una prueba de envío de paquetes ICMP hacia la red remota sin hacer uso de QoS, algunos paquetes se perderán como se muestra en la Fig. 7; mientras que si se envían paquetes ICMP de forma continua pero marcados en la clase PLATINUM (que corresponde al PHB EF, el cual está asociado al las Type of Service 184), se obtendrán resultados exitosos como se muestra en la Fig. 8.

Para realizar las pruebas de conectividad entre las VLAN en IPv6, se envían paquetes ICMP continuos. Cabe aclarar que para tener soporte del protocolo IPv6, es necesario disponer de switches que soporten la plantilla "sdm prefer dual-ipv4-and-ipv6 default".

(5) **Ingeniería de Tráfico:** El balanceo de carga simétrico se establece mediante túneles TE con anchos de banda y prioridades iguales, en la Fig. 9 se presenta la salida del comando "show ip route" que verifica las rutas propuestas. Se realizará el balanceo del tráfico tanto para el túnel 1 como en el túnel 2, en la misma proporción. Además, con Fast Re-Route se brinda redundancia de enlaces, a través de la creación de túneles de respaldo. Se debe configurar la interfaz protegida para reenrutar el tráfico por el túnel de respaldo previamente definido.

Para comprobar el funcionamiento, se envían paquetes ICMP de forma continua y se desconecta la interfaz protegida, se perderán un par de paquetes mientras se realiza la activación automática del camino redundante. En las pruebas realizadas se llegaban a perder menos del 0.1% de 2500 paquetes enviados como se indica en la Fig. 10. El estado del túnel de respaldo pasará de "listo" a "activo", como se indica en la Fig. 11.

(6) **Mejores Prácticas de Seguridad:** Al implementar en una red simultáneamente dos protocolos IP no compatibles, es importante analizar su seguridad tanto para IPv4 como para IPv6. Es por ello que, la creación de ACL y sesiones SSH deben ser establecidas, para ambos protocolos.

```
PE1MUROS#
PE1MUROS#ping vrf CLIENTE
Protocol [ip]:
Target IP address: 33.33.33.10
Repeat count [5]: 100
Datagram size [100]:
Timeout in seconds [2]:
Extended commands [n]: y
Source address or interface:
Type of service [0]: 184
Set DF bit in IP header? [no]:
Validate reply data? [no]:
Data pattern [0xABCD]:
Loose, Strict, Record, Timestamp, Verbose[none]:
Sweep range of sizes [n]:
Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 33.33.33.10, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/2/4 ms
```

Figura 8: Verificación del envío de paquetes ICMP marcados

Las ACL en IPv6 se configuran de manera similar a las ACL extendidas nombradas en IPv4 y se comprueban verificando que el tráfico generado por determinado protocolo, sea permitido o denegado.

Por ejemplo, en la Fig. 13 se limita el tráfico HTTP, HTTPS, FTP y TFTP para ciertas redes.

```
PE1MUROS#sh ip route 5.5.5.5
Routing entry for 5.5.5.5/32
  Known via "ospf 27947", distance 110, metric 4, type intra area
  Last update from 5.5.5.5 on Tunnel2, 00:00:47 ago
  Routing Descriptor Blocks:
    5.5.5.5, from 5.5.5.5, 00:00:47 ago, via Tunnel1
      Route metric is 4, traffic share count is 1
  * 5.5.5.5, from 5.5.5.5, 00:00:47 ago, via Tunnel2
      Route metric is 4, traffic share count is 1
PE1MUROS#_
```

Figura 9: Balanceo de carga simétrico con TE

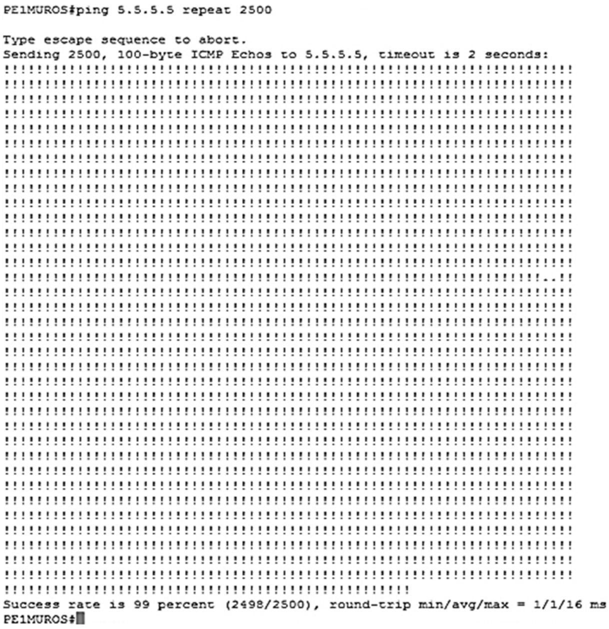

Figura 10: Prueba de envío de 2500 paquetes ICMP

Las VLAN serán imperceptibles para un protocolo de capa 3 como IP, aunque para su uso con direcciones IPv6 administrativas, será necesaria la plantilla de doble pila SDM indicada en la Fig. 12.

```
PGOSSEAL#sh mpls traffic-eng fast-reroute database
Headend frr information:
Protected tunnel              In-label Out intf/label     FRR intf/label    Status

LSP midpoint frr information:
LSP identifier                In-label Out intf/label     FRR intf/label    Status
1.1.1.1 1 [46]                30       Gi0/1:16           Tu10:16           active
```

Figura 11. Verificación del estado del túnel de respaldo en activo

```
SW1COLON(config)#sdm prefer dual-ipv4-and-ipv6 default
```

Figura 12. Plantilla de doble pila "sdm prefer dual-ipv4-and-ipv6"

```
PDATACENTER(config-ext-nacl)#ipv6 access-list ACLV6GESTION_MPLS
PDATACENTER(config-ipv6-acl)#permit tcp 2001:29:2:41::0/64 any eq www
PDATACENTER(config-ipv6-acl)#deny tcp any any eq www
PDATACENTER(config-ipv6-acl)#permit tcp 2001:29:2:41::0/64 any eq 443
PDATACENTER(config-ipv6-acl)#deny tcp any any eq 443
PDATACENTER(config-ipv6-acl)#permit tcp any host 2001:29:2:41::11 eq ftp
PDATACENTER(config-ipv6-acl)#deny tcp any any eq ftp
PDATACENTER(config-ipv6-acl)#permit tcp any host 2001:29:2:41::11 eq ftp-data
PDATACENTER(config-ipv6-acl)#deny tcp any any eq ftp-data
PDATACENTER(config-ipv6-acl)#permit udp any host 2001:29:2:41::11 eq tftp
PDATACENTER(config-ipv6-acl)#deny udp any any eq tftp
PDATACENTER(config-ipv6-acl)#permit ip any any
PDATACENTER(config-ipv6-acl)#deny ip any any
```

Figura 13. Configuración de la ACL IPv6

Finalmente, para el control de acceso remoto seguro se implementa tanto el protocolo SSH así como las ACL tanto en IPv6 como en IPv4. Se comprueba el establecimiento de sesiones SSH hacia cada componente de la red, y probando que no es posible acceder desde determinadas partes de la red según lo presentado en la Fig. 15.

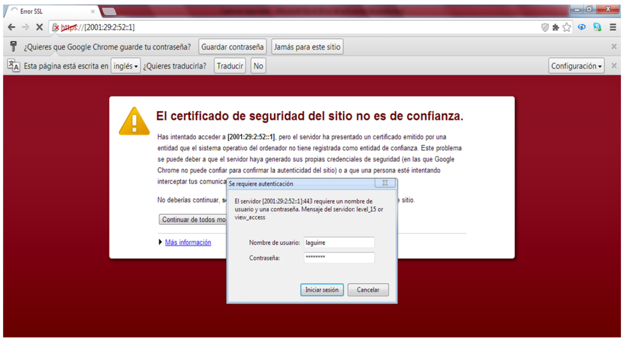

Figura 14. Acceso HTTPS IPv6 permitido

Por ejemplo, para comprobar que las sesiones SSH están permitidas entre los PE del prototipo pero denegadas a través de Telnet, se deben configurar las líneas vty solo con SSH como se indica en la Fig. 16. Las ACL permitirán limitar el tráfico para las redes del ISP. En la Fig. 17 se muestra la gestión remota en IPv6 entre los equipos PE1MUROS y PE1GOSSEAL del prototipo, con el resultado fallido para telnet y exitoso para SSH, como se esperaba.

```
PE1MUROS#sh run | b login
 login local
line aux 0
line vty 0 4
 access-class 1 in
 exec-timeout 30 0
 ipv6 access-class ACLV6GESTION_SSH in
 logging synchronous
 login local
 transport input ssh
 transport output telnet ssh
line vty 5 15
 access-class 1 in
 exec-timeout 30 0
 ipv6 access-class ACLV6GESTION_SSH in
 logging synchronous
 login local
 transport input ssh
 transport output telnet ssh
!
scheduler allocate 20000 1000
end
```

Figura 16. Configuración de las sesiones SSH y Telnet (PE1MUROS)

```
PE1MUROS#telnet 2001:29:2:52::1
Trying 2001:29:2:52::1 ...
% Connection refused by remote host

PE1MUROS#ssh 2001:29:2:52::1

Password:

**************************************************************

                         ADVERTENCIA
                         ===========
 ACCESO RESTRINGIDO SOLO A PERSONAL AUTORIZADO DE TELCONET S.A.
--------------------------------------------------------------
Usted se ha conectado a un Sistema Monitoreado de TELCONET S.A.
Las Violaciones a este sistema son penalizadas por la LEY DE
COMERCIO ELECTRONICO ECUATORIANA y demas LEYES INTERNACIONALES.

**************************************************************
```

Figura 17. Sesiones SSH y Telnet en IPv6 establecidas entre dos PE

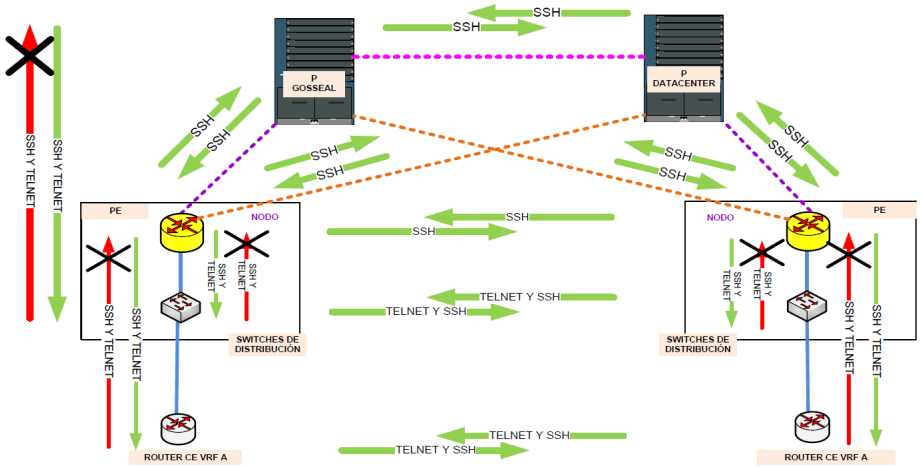

Figura 15. Accesos remotos

7. CONCLUSIONES

Las redes de los ISP como Telconet requieren mejoras substanciales ante el crecimiento continuo de clientes y aplicaciones, sobre todo considerando la implementación de un Centro de Datos; sin embargo, su objetivo sigue siendo el mismo, seguir ofreciendo servicios de calidad y lograr alta confiabilidad en los clientes a nivel nacional.

Por otro lado, se presenta el agotamiento de las direcciones IPv4 y con ello, la necesidad de adoptar un mecanismo de transición a IPv6 que brinde: un mayor número de direcciones, encabezado reducido, mayor velocidad, diferenciación de servicios, autenticación, seguridad, entre otras características. No es una solución migrar toda una infraestructura de red a IPv6 ya que esta debe ser progresiva con el tiempo y los costos; pero si, adaptar un mecanismo de transición como 6PE/6VPE.

La seguridad en las redes de datos es y será siempre de vital importancia, sobretodo en presencia de protocolos nuevos como IPv6; es por ello que, implementar las mejores prácticas de seguridad, permitirá fortalecer la red del proveedor.

Finalmente, es importante brindar un prototipo a otros proveedores que puedan usarlo como guía para mejorar su infraestructura.

8. AGRADECIMIENTOS

Este trabajo fue realizado gracias al apoyo del personal de Telconet S.A., del departamento de OM Plataformas IP-MPLS de la CNT y del Proyecto 3G de Huawei Technologies Co. Ltd.

REFERENCIAS

[1] A. Loa, R. Asati, “RFC 5642”, IETF, Feb. 2009.

[2] A. Vivek, “Advanced MPLS Design and Implementation”. Ed. Cisco Press, USA, 2001.

[3] Anónimo, “Implementing Cisco Quality of Service”, Student Guide Cisco Systems, Inc., 2nd ed., vol. 1 y 2, USA, 1998.

[4] Anónimo, “SSH Support Over IPv6”. Cisco Systems, Inc. [Online], Jul. 2012. Available: `http://www.cisco.com/en/US/docs/iosxml/ios/ipv6_nman/configuration/15-2mt/ip6-ssh.pdf`

[5] B. Davie, “MPLS: Technology and Applications”, 1st ed., Ed. Morgan Kauffman, USA, 2000.

[6] E. Vyncke, “”IPv6 Security Best Practices”, Cisco, `http://www.cisco.com/web/SG/learning/ipv6_seminar/files/02Eric_Vyncke_Security_Best_Practices.pdf`

[7] I. Pepelnjak y J. Guichard, “MPLS and VPN Architectures”, 1st ed., Ed. Cisco Press, USA, 2000.

[8] J. De Clercq, D Ooms, S. Prevost, y F. Le Faucheur, “Connecting IPv6 Islands over IPv4 MPLS using IPv6 Provider Edge Routers (6PE)” Internet Engineering Task Force RFC 4798, 2007; `http://tools.ietf.org/html/rfc4798`.

[9] L. B. Nieto Porras, “Diseño y Configuración de Calidad de Servicio en la Tecnología MPLS para un Proveedor de Servicios de Internet”, Proyecto de Titulación de Ingeniería, FIEE, EPN, Quito, Ecuador, May. 2010.

[10] L. Ghein, “MPLS Fundamentals”, 1st ed., Ed. Cisco Press, USA, 2006.

[11] L. P. Aguirre Sánchez, “Rediseño de la red MPLS con soporte de IPv6 empleando las Mejores Prácticas de Seguridad para el sistema autónomo de Telconet S.A. de la ciudad de Quito”, Proyecto de Titulación de Ingeniería, FIEE, EPN, Quito, Ecuador, Feb. 2013.

[12] P. Grayeli, S. Sarkani y T. Mazzuchi, “Performance Analysis of IPv6 Transition Mechanisms over MPLS”

in International Journal of Communication Networks and Information Security (IJCNIS), Vol. 4, 2012, pp. 91-103.

[13] S. Convery y D. Miller, "IPv6 and IPv4 Threat Comparison and Best Practice Evaluation (v1.0)", Cisco; http://www.cisco.com/web/about/security/security_services/ciag/documents/v6-v4-threats.pdf