

“Migración de las redes de distribución y núcleo de Telconet de un esquema plano capa 2 Ethernet e IP a un diseño capa 2 802.1Q e IP + MPLS”

Carlos Montero Lucio⁽¹⁾ Ing. Sergio Flores⁽²⁾
Facultad de Ingeniería Eléctrica y Computación (FIEC)
Escuela Superior Politécnica del Litoral (ESPOL)
Campus Gustavo Galindo Km. 30,5 vía Perimetral, Apartado 09-01-5863. Guayaquil, Ecuador
camontero@telconet.net⁽¹⁾
Escuela Superior Politécnica del Litoral, Ecuador, 1973, Ingeniero Electrónico⁽²⁾
sflores@fiec.espol.edu.ec⁽²⁾, 1973 profesor en la ESPOL

Resumen

El crecimiento tecnológico obliga a las empresas proveedoras de acceso a Internet y portadores de datos a mejorar su infraestructura para satisfacer la demanda de sus clientes.

Este artículo tiene como finalidad explicar el proceso que permitió cambiar la tecnología de Telconet S.A. para brindar nuevos y mejores servicios de redes capa 2 y 3 utilizando tecnología MPLS y evidenciar los resultados.

En el segundo semestre del año 2005, Telconet S.A. tomó la decisión de realizar mejoras fundamentales en su red de distribución y núcleo; esto es, en la infraestructura tecnológica medular de la empresa con la finalidad de mejorar su posición en el mercado y ofrecer mejores esquemas de conectividad y mayor ancho de banda para sus usuarios.

Dicha implementación tuvo la colaboración de Cisco Systems, líder mundial en el mercado de equipos de redes de datos. A través de una extensa consultoría y de los recursos humanos y profesionales que laboramos en Telconet S.A. procedimos a diseñar e implementar una nueva red con mayor capacidad y mejores prestaciones tecnológicas.

Al margen de los indicadores y las explicaciones descritas en este artículo, la mejora en la calidad del servicio de Telconet S.A. es la mejor evidencia de que se tomaron decisiones acertadas y que los servicios prestados satisfacen o exceden los requerimientos del mercado corporativo ecuatoriano.

Palabras Claves: Red, distribución, núcleo, Telconet, Cisco, MPLS.

Abstract

The technological growth forces Internet Access Providers and data carriers to upgrade their platform in order to satisfy their customers' expectations.

The purpose of this article is to explain the technological change of Telconet S.A. in order to offer new and improved services for layer 2 and 3 networks using MPLS technology and to show the results.

During the second semester 2005, Telconet S.A. decided to make fundamental improvements in its distribution and core networks, that is, to improve the main technological infrastructure of the company in order to get a better position in the market and to offer better connectivity solutions and more bandwidth for its users.

This implementation had the helping hand of Cisco Systems, world leader in the data networking market. Through an extensive consulting service and the professional and human resources of those who work in Telconet S.A. we designed and implemented a new network with improved capacity and better technological services.

Besides numbers and explanations described in this article, the improvement in the quality of TelconetS.A.'s services is the best proof that appropriate decisions were taken and that the offered services satisfy or exceed the requirements of the Ecuadorian corporate market.

I. Introducción

En el año 2005 la red de transmisión de datos de Telconet S.A. estaba posicionándose como una de las más rápidas del país. Los clientes de Telconet contaban con un servicio que les ofrecía capacidades muy altas de transmisión y recepción de datos, además de tiempos de respuesta (latencia) muy bajos, gracias a la implementación de la red de fibra óptica. Sin embargo, el modelo tecnológico no podía sustentarse en el tiempo. La escalabilidad de la red no era la apropiada y las técnicas de tunelización empleadas, si bien cumplían su cometido, no eran la práctica más segura para la provisión de circuitos virtuales.

Con esta preocupación en mente, se decidió realizar una profunda actualización de la red para soportar una mejor escalabilidad, mejoras en la seguridad de los circuitos y capacidades troncales que permitan agregar abonados con una muy alta demanda de ancho de banda, esto es, 10 Gbps o más en las principales ciudades del Ecuador.

En resumen, la visión del negocio, la cual consiste en proveer de enlaces de datos de alta disponibilidad, seguros y con soporte para muy altas capacidades motivó a que un grupo de miembros de la empresa nos demos a la tarea de diseñar e implementar la nueva red de Telconet S.A.

Tuve la oportunidad de iniciar mi colaboración en este proyecto en el mes de Octubre del año 2005, cuando ejercía las funciones de Jefe de Soporte Técnico en Guayaquil. Durante el 2do semestre de dicho año, Telconet adquirió la asesoría de Cisco Systems para el rediseño de la red y la recomendación de los sistemas operativos que funcionarían tanto en los equipos nuevos como en los legados.

1. Esquema inicial en capa 2 ethernet e IP

El esquema inicial de la red de Telconet S.A. se caracterizaba por:

- Un solo dominio de capa 2 conmutado para todos los CPEs de los abonados.
- Una pareja de enrutadores redundantes para servir a todos los abonados. La redundancia se manejaba mediante los protocolos OSPF, BGP y HSRP como protocolo LAN de primer salto.
- Todo el transporte se realizaba únicamente mediante el protocolo IP.
- Se utilizaban técnicas de tunelización exclusivamente. Esta era la única forma de enmascarar y ocultar el direccionamiento del abonado.
- Los enrutadores en todas los niveles manejaban 1 sola tabla de rutas.
- Se tenía una limitante de 1024 vlans por ciudad o dominio de capa 2.
- Los enlaces entre switches de acceso se hacían de

tal forma que se formen anillos. Sin embargo, estos anillos carecían de un orden lógico que permita predecir el flujo de tráfico ante eventos como cortes de fibra óptica o daño de alguno de los switches del anillo.

Básicamente cada ciudad se comportaba como un switch grande con dos enrutadores conectados a ellos. La comunicación interurbana era posible gracias a 2 anillos de fibra óptica armados con switches Cisco 2970.

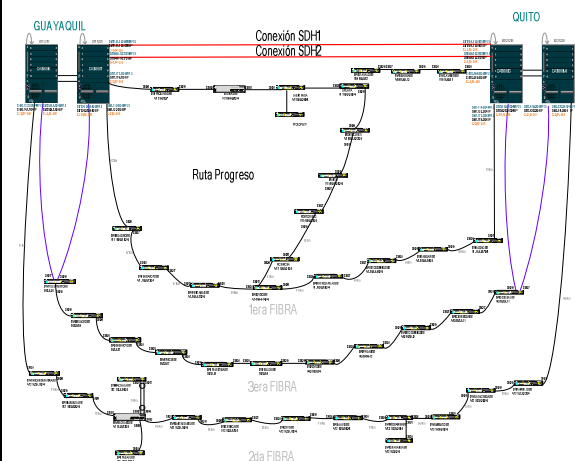


Figura 1. Red Interurbana

La principal ventaja de este diseño era la simplicidad. Los puntos críticos eran pocos y bien definidos, esto es, los enrutadores de cada ciudad.

Otro factor a favor de este diseño era la posibilidad de tener conectividad directa en capa 2 entre cualquier par de puntos dentro de la ciudad; esto nos permitía, por ejemplo, tener un CPE en el norte de Guayaquil dentro del mismo segmento de red que un CPE en el sur de Guayaquil o en el centro de Eloy Alfaro (Durán).

Las desventajas son notorias, principalmente:

- Escalabilidad: El protocolo spanning tree y la administración del crecimiento de los anillos no eran efectivos para un lugar con más de 200 switches de acceso como es el caso de Guayaquil.
- Falta de seguridad y confidencialidad: Producida por el compartimiento de la vlan de acceso. Si bien el acceso es conmutado (tipo switch y no hub) los flujos tipo broadcast podían ser vistos en varios puntos de la red simultáneamente a pesar de pertenecer a clientes diferentes.
- Escasa predictibilidad de los flujos de tráfico: Debido al crecimiento del número de switches de acceso.
- "Unicast flooding" y tormentas de broadcast

con impacto global.

- El servicio estaba limitado a usar técnicas de tunelización.
- No existía una implementación tipo “pseudowire” para conectar clientes en capa 2 cuyos puntos estén en dominios distintos, por ejemplo un punto en Guayaquil y el otro en Quito.

Estos fueron los principales motivos para, en conjunto con personal de Cisco Systems, buscar un nuevo diseño que permita crecer ordenadamente mejorando los servicios para los abonados de Telconet. La decisión fue a favor de implementar MPLS en la red de núcleo de tal forma que se puedan proveer servicios de VPN a los abonados incrementando los niveles de seguridad, disponibilidad y confidencialidad.

2. Requerimientos del nuevo diseño

Se plantearon los siguientes requerimientos:

- Soportar al menos 900 vlans y 900 vrfs dentro de cada dominio de capa 2
- Manejar enrutamiento dinámico con MultiProtocol BGP centralizado en Route Reflectors
- Capacidad de escalar el hardware para adaptarse a nuevas tecnologías y mayores densidades de puertos
- Capacidad de asignar a cada cliente una vlan y una vrf exclusiva
- Capacidad de interconectar 2 o más VPNs de clientes
- Capacidad de entregar circuitos de capa 2
- Capacidad de ofrecer niveles de servicio diferenciados al tráfico de los clientes
- Eliminar BGP de la red de núcleo de modo que únicamente exista conmutación por etiquetas
- Capacidad de la red de núcleo para manejar hasta 10 Gbps.

El nivel jerárquico de los equipos seleccionado fue la estructura clásica en redes MPLS, esto es, routers tipo P en la red de núcleo y routers tipo PE manejando el borde de la red de acceso y distribución.

Luego del análisis de capacidades y, en conjunto con personal de Cisco Systems, la plataforma elegida fue la siguiente:

Enrutadores tipo P: Cisco Catalyst 6500, SUP-720.

Enrutadores tipo PE: Cisco 7609 con RSP-720, Cisco 7606 con SUP-32, Cisco 7206VXR con NPE-G2 y Cisco 2821.

Enrutadores tipo Route Reflector: Cisco 7206VXR con NPE-G2.

La variedad en los enrutadores tipo PE se debe a que cada equipo dirige el tráfico para una ciudad o cantón. Dadas las capacidades de ancho de banda comercializadas en ciertos lugares del territorio ecuatoriano, consideramos que colocar un equipo de iguales prestaciones en todo el

territorio es una forma ineficiente de utilizar el recurso económico. Por ejemplo, comparar el tráfico comercializado en Guayaquil, con el tráfico de Quevedo o Naranjal, arroja una relación aproximada de 80:1 en el primer caso y 400:1 en el segundo.

El nuevo diseño mantiene altos niveles de redundancia con anillos mucho más pequeños agregados en enrutadores con funcionalidad tipo PE.

El siguiente diagrama muestra el diseño básico que se está implementando en las ciudades con más de 25 switches de acceso:

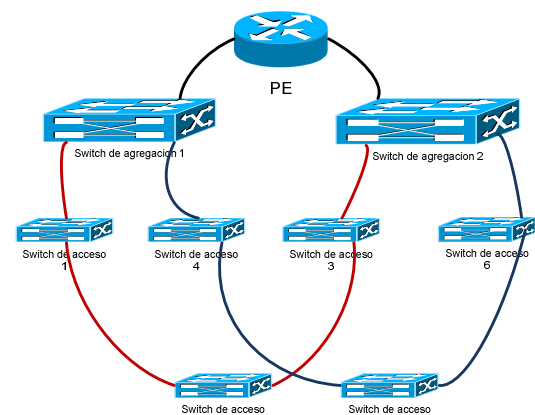


Figura 2. Red capa 2 modificada

3. Etapa de pruebas

La etapa de pruebas se realizó en el año 2008 utilizando la infraestructura nueva y sin clientes, es decir, inicialmente las pruebas no tocaron ningún equipo en producción. Fue durante esta etapa cuando se afinaron los números que definieron las capacidades de cada modelo de enrutador PE.

Dichas pruebas consistieron en configurar varios servicios de VPN, tanto capa 2 como capa 3 y verificar las siguientes funcionalidades:

- Importación y exportación de prefijos
- Compatibilidad con protocolos IGP
- Consideraciones para el aprovisionamiento
- Desempeño de las cajas

Para ambos tipos de VPN tuvimos una etapa de pruebas exitosas donde se consiguió otorgar conectividad entre redes utilizando la nueva infraestructura. Con la información extraída de esta primera etapa de pruebas se procedieron a elaborar las aplicaciones de aprovisionamiento para las nuevas VPNs (ver figura) de tal forma que la asignación de direcciones IP, route distinguisher y la configuración de los dispositivos involucrados se realice de forma

automática.

4. Puesta en producción

La puesta en producción inició en el segundo semestre del año 2008. Se capacitó al personal de operaciones para que entienda y de soporte a la nueva infraestructura, también, se actualizaron los instructivos y se hicieron varias demostraciones de la nueva aplicación de manejo de VPNs. Adicionalmente se comercializaron las primeras VPNs capa 2, lo que permitió que se pueda ofrecer un producto tipo “extensión LAN” entre cualquier punto que tenga cobertura MPLS. De esta forma un abonado puede pasar sus propias vlans con un tamaño máximo de 1520 bytes por frame sin tener que depender de enrutamiento provisto por Telconet.

5. Transición de clientes durante la migración

La siguiente tabla resume la diferencia entre los servicios de clientes luego de la mejora hecha a las redes de distribución y núcleo de Telconet

Tabla 1. Comparación de servicios

<i>Servicio Anterior</i>	<i>Servicio post MPLS</i>
Túnel IP	VPN capa 3
Túnel IPSec	Túnel IPSec sobre VPN capa 3
VRF Lite	VPN capa 3
Acceso a Internet	Acceso a Internet (con opción a hacerlo sobre VRF privada)
	VPN capa 2 (pseudowire)

6. VRF por cliente

El esquema VRF por cliente es la culminación de la migración al esquema de VPN MPLS capa 3 y capa 2. En este modelo cada cliente posee una tabla de enrutamiento privada y única dentro de la red de núcleo de Telconet. De esta forma se elimina la necesidad de contar con técnicas de tunelización para, entre otros fines, proteger y aislar el direccionamiento IP del cliente final. Esta y todas las VRFs importan 1 prefijo de una VRF reservada por Telconet para

monitoreo; de la misma forma exportan sus prefijos a esta VRF de monitoreo. Esto significa que el direccionamiento externo de los CPEs (el que se conecta a la red de acceso) es gobernado por Telconet. Así podemos garantizar que monitoreamos una dirección única por dispositivo sin que exista oportunidad para cruces o duplicidad de direcciones.

7. Interconexión de clientes

La interconexión de clientes cambia completamente. Antes se levantaba un túnel IP entre los CPEs de aquellos clientes que manifestaban su necesidad de interconectarse. En las VPNs MPLS L3 simplemente importamos y exportamos los prefijos relevantes entre las VRFs de estos clientes.

8. Superioridad de productos finales en la actualidad

Los siguientes puntos por describir son considerados clave para proveer una solución más flexible y escalable a los abonados de Telconet:

- Topología full mesh real.
- Uso de protocolos de enrutamiento entre cliente y proveedor

8.1 Topología full mesh real

En una VPN MPLS capa 3 la topología por omisión es full mesh, se elimina el concepto tradicional de proveer ancho de banda entre un punto A y otro B, punto A y punto C, etc. para proveer simplemente un ancho de banda para transmisión y recepción de datos. Si el punto A y el punto B necesitan intercambiar datos lo harán a través de su respectivo enrutador PE. Lo mismo sucederá entre punto A y C o punto B y C. Puede argumentarse que el tráfico no sigue un camino directo entre los CPEs del cliente y es correcto. Este esquema full mesh hace referencia a que cualquier punto de datos que se incorpore a la VRF del cliente es incluido en la tabla de enrutamiento, a menos que se solicite lo contrario. De esta forma es posible la conexión entre todos los puntos sin necesidad de configurar túneles adicionales o sin forzar a que el punto de paso obligatorio sea único como es el caso de una topología estrella, conocida también como “Hub & spoke”. Tampoco hay necesidad de contratar la suma completa de ancho de banda para el CPE que estaba en el centro de la estrella

ejemplo un peso de 3 5 6 significa que por cada 3 paquetes desencolados de la cola 1, se desencolan 5 y

8.2 Protocolos de enrutamiento cliente-proveedor (CE-PE) sobre VRF

En el esquema inicial, los protocolos de enrutamiento entre los puntos de los abonados podían correr únicamente dentro de las interfaces tipo túnel. Esto se debía a restricciones de seguridad que no permitían el tráfico multicast, normal en los IGP, dentro de una vlan; más aun si consideramos que esta vlan estaba compartida entre los CPEs de los abonados, las razones son evidentes. Esto quiere decir que el aprendizaje de rutas es dinámico entre los CPEs, pero a nivel de los enrutadores de proveedor, todo es estático.

Con la solución de VPN MPLS en capa 3 Telconet ha eliminado esta restricción y soporta los siguientes protocolos de enrutamiento:

- RIPv2
- OSPF
- EIGRP
- BGP

De esta forma la información de enrutamiento entre abonado y proveedor puede ser dinámica. Las vlans son independientes para cada abonado así como las VRFs; no existe posibilidad de cruce de información entre dominios de enrutamiento independientes.

9. Provisión de QoS nativo en las redes de distribución y núcleo

La nueva topología fue el momento adecuado para implementar políticas de calidad de servicio (QoS) dentro de las redes de distribución y núcleo.

En las plataformas Cisco, la forma de implementarlo es dependiente no solamente de la plataforma, sino también de las tarjetas que se emplean en ellas. Las tarjetas utilizadas en la red son las siguientes:

Enrutadores tipo P: WS-X6704-10GE y WS-X6516A-GBIC

Enrutadores tipo PE: WS-X6704-10GE

Las características en cuanto al manejo de colas son:

WS-X6704-10GE; TX: 1p7q8t; RX: 1q8t

WS-X6516A-GBIC; TX: 1p2q2t; 1p1q4t

La nomenclatura XpYqZt significa:

Xp: X colas de prioridad

Yq: Y colas estándares

Zt: Z umbrales

Esto quiere decir que podemos asignar cierto tráfico a la cola de prioridad, otro tráfico a una de las colas normales y a uno de varios umbrales disponibles antes de que el paquete sea elegido para descarte en momentos de congestión.

Definimos varias marcas válidas a través de la información DSCP de los paquetes IP. De esta forma creamos un estándar que fue comunicado a los clientes para que marquen los paquetes apropiadamente en función de la calidad de servicio que requerían para cada tipo de tráfico.

Los valores de DSCP se mapean a valores COS de Ethernet

y EXP de MPLS para tener consistencia en los diferentes dominios por donde pasa el tráfico. Dado que el algoritmo escogido para el encolamiento de salida es WRR (weighted round robin) se asignan pesos y límites para cada cola; por ejemplo un peso de 3 5 6 significa que por cada 3 paquetes desencolados de la cola 1, se desencolan 5 paquetes en la cola 2 y 6 paquetes de la cola 6. Adicionalmente se fijó un límite máximo para estos flujos de tráfico para casos de congestión. Se decidió usar tan solo un umbral tanto para las tarjetas con interfaces a 10 Gbps como para las tarjetas de 1 Gbps.

10. IPv6

La aplicación del protocolo IPv6 se realiza mediante la implementación de 6VPE.

6VPE es la introducción de una "address family" de tipo IPv6 dentro de las VRFs que manejan los enrutadores tipo PE. De esta forma se crea la nueva "address family" VPNv6, análoga a la VPNv4 que se usa para las VPNs IPv4. Esta familia VPNv6 es muy similar a VPNv4 ya que usa también route distinguishers para crear prefijos extendidos únicos.

La señalización de MPLS en la red de núcleo sigue funcionando sobre IPv4, pero los prefijos IPv6 son aprendidos vía BGP por los enrutadores PE. De esta manera se propaga la información tanto IPv4 como IPv6 de los abonados que requieran este servicio manteniendo la independencia y confidencialidad respecto a las otras VRFs.

Los protocolos de enrutamiento CE-PE soportados para esta implementación son:

- OSPFv3
- BGP

A nivel de la red de núcleo, se hicieron las actualizaciones de configuración BGP para soportar las nuevas "address family" sin contratiempos.

11. Multicast

Con la migración de tecnología se permitirá el flujo de tráfico multicast nativo. Anteriormente el tráfico multicast solo podía permitirse de forma tunelizada directamente dentro de los CPEs de los abonados. Dado que los enrutadores PE tienen la característica de manejar una VRF por cada abonado, es posible que exista un intercambio de paquetes multicast directamente y sin riesgo de que se propaguen a otro abonado ya que se contienen en la vlan respectiva.

Para optimizar la operación multicast sobre la red se habilitarán varias tecnologías:

IGMP snooping: Nos permite optimizar el transporte de tráfico multicast en la red de acceso (capa 2) mediante la inspección de este tipo de flujo de datos.

De esta forma eliminamos la propagación de los frames multicast a todos los puertos de acceso para una vlan particular.

MLD snooping: Es una solución muy similar a la anterior pero trabaja exclusivamente con MLDv1 y MLDv2 (multicast listener discovery), esto es, únicamente para IPv6.

PIM-SSM: Es el protocolo escogido para la red de núcleo (Protocol Independent Multicast-Source Specific Multicast) debido a que los árboles multicast se construyen sobre una raíz única lo que permite un despliegue más seguro y escalable en la arquitectura P-PE de Telconet.

Cada VRF tendrá configurado un MDT (multicast distribution tree) en el enrutador PE más cercano a la fuente. Como lo expresa el texto de esta sección, la implementación de IP multicast aún se encuentra en proceso de ejecución.

12. Minimización de la inteligencia del CPE

Como se ha manifestado anteriormente, el diseño de este tipo de redes permite desplazar ciertas funciones de los CPEs hacia la red de distribución. La eliminación del esquema de tunelización permite que los enrutadores asignados a los abonados se dediquen a tareas elementales como envío de tráfico y marcado de paquetes para efectos de aplicación de políticas de calidad de servicio.

Adicionalmente un servicio de tipo “pseudowire” como la VPN MPLS capa 2 permite entregar simplemente “un cable” al abonado en 2 ubicaciones diferentes de tal forma que enlace sus equipos directamente, virtualmente sin pasar por dominios de enrutamiento externos.

Otro factor es la posibilidad de utilizar protocolos sumamente elementales y sencillos como RIPv2, el cual es un protocolo soportado en enrutadores de bajo costo, ideales para ser instalados en pequeñas empresas que tengan personal de sistemas o telecomunicaciones de experiencia limitada.

Expansiones futuras a nivel de servicios permitirán ofrecer servicios de encriptación en el enrutador PE mediante IPSEC, lo que permitirá eliminar esta funcionalidad en los CPEs que actualmente se usan para este tipo de servicios.

13. Flexibilidad en la gestión del CPE

Tradicionalmente, la política de Telconet es instalar CPEs propios para el servicio de sus abonados. Sin embargo existen casos donde es el propio abonado quien desea colocar sus equipos y gestionarlos. Migrarlos a un esquema de vlans 802.1Q y MPLS/IP permite que Telconet revise este tema y en la mayoría de los casos apruebe la instalación de cualquier marca o modelo de enrutador provisto por el abonado.

De esta forma, el abonado puede utilizar la plataforma de enrutamiento de su predilección siempre y cuando los parámetros técnicos contractuales sean compatibles entre su plataforma y la nuestra; esto es, conexión en interfaz ethernet

, manejo de protocolo IP y cualquiera de los protocolos de enrutamiento mencionados.

14. Conclusiones y recomendaciones

1. La mejora de los servicios provistos a los abonados y la jerarquización de la nueva red son evidentes.
2. La inversión realizada permite comercializar una capacidad de ancho de banda mucho mayor, servicios mucho más avanzados que ofrecen mejores prestaciones a los abonados de Telconet; IPv6, IPTV, VPNs capa 2 y capa 3, entre otras.
3. El proceso de transición aún está corriendo. Se ha migrado una cantidad importante de clientes, alrededor del 40%, pero dado que el proceso involucra cambiar configuraciones en los CPEs y, por lo tanto, una interrupción en el servicio, se lo ha ejecutado de forma programada y consensuada con los abonados para minimizar las molestias por estos cambios.
4. Los indicadores mostrados evidencian también que las mejoras implementadas han permitido incrementar la disponibilidad de la red de forma que se incurren en menos penalidades económicas y la satisfacción del servicio, naturalmente, crece.
5. MPLS y 802.1Q son tecnologías que han permitido mejorar la calidad del servicio y la disponibilidad la red de Telconet a nivel nacional.

Es criterio del autor de este artículo que las decisiones tomadas en su momento fueron muy acertadas, las bases de diseño al día de hoy son válidas y se proyectan adecuadamente para la provisión de nuevos servicios en la red. La naturaleza modular de las mismas nos permiten crecer tanto en capacidad de manejo de ancho de banda como en la inteligencia que se puede otorgar al tratamiento de paquetes de datos.

15. Agradecimientos

Un sincero agradecimiento a Dios, mi familia, al Ing. Sergio Flores por su guía y paciencia para la culminación de este proyecto.

Un agradecimiento muy especial al Ing. Tomislav Topic por su valiosísima contribución para documentar este proceso.

