

ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL.

Facultad de Ingeniería en Electricidad y Computación

**∞Migración de la 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∞**

INFORME DE TRABAJO PROFESIONAL

Previo a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por

Carlos Alberto Montero Lucio

Guayaquil - Ecuador

2010

AGRADECIMIENTO

Sobre todo a Dios, a mi esposa, a mis padres y hermano por su apoyo constante.

Un agradecimiento muy especial para los ingenieros Tomislav Topic y Sergio Flores por su
colaboración.

TRIBUNAL DE SUSTENTACIÓN

Ing. Jorge Aragundi

Subdecano

Ing. Sergio Flores M.

Director

Ing. Juan C. Avilés

Miembro Principal

DECLARACIÓN EXPRESA

La responsabilidad del contenido de esta Tesis de Grado, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral

Carlos Alberto Montero Lucio

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 informe de trabajo profesional tiene como finalidad documentar el proceso que permitió cambiar la tecnología de Telconet S.A. para brindar nuevos y mejores servicios de redes capa 2 y 3 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 informe, el éxito de Telconet S.A. en el mercado de telecomunicaciones es la mejor evidencia de que se tomaron decisiones acertadas y que los servicios prestados satisfacen o exceden los requerimientos del mercado corporativo ecuatoriano.

INDICE GENERAL

1. DISEÑO Y MIGRACIÓN	1
1.1 CONCEPTOS BÁSICOS DE REDES	1
1.1.1 ETHERNET	1
1.1.2 IEEE 802.1Q	2
1.1.3 REDES IP	2
1.1.4 REDES MPLS	3
1.1.5 VPNs CAPA 2 Y CAPA 3	4
1.2 ESQUEMA INICIAL EN CAPA 2 ETHERNET E IP	6
1.2.1 CARACTERISTICAS	6
1.2.2 VENTAJAS	10
1.2.3 DESVENTAJAS	10
1.2.4 TIPOS DE CLIENTES	12
1.3 DISEÑO EN CAPA 2 802.1Q E IP + MPLS Y MIGRACION	12
1.3.1 REQUERIMIENTOS DEL DISEÑO	12
1.3.2 JERARQUIA, SELECCIÓN Y DIMENSIONAMIENTO DE EQUIPOS	13
1.3.3 ADAPTACIÓN DE LA TOPOLOGÍA FÍSICA DE LA RED	15

1.3.4 RESULTADOS ESPERADOS DEL DISEÑO.....	20
2. IMPLEMENTACION DEL NUEVO DISEÑO Y PROCESO DE TRANSICION	21
2.1 ETAPA DE PRUEBAS.....	21
2.2 PUESTA EN PRODUCCION.....	24
2.3 COMPARACION ENTRE ESQUEMA ANTERIOR CONTRA ESQUEMA ACTUAL DE CLIENTES..	25
2.3.1 MIGRACION DE TUNELES IP A TUNELES IP SOBRE VRF	25
2.3.2 VRF POR CLIENTE	26
2.3.3 INTERCONEXIÓN DE CLIENTES	29
3. RESULTADOS DE LA IMPLEMENTACION	31
3.1 MEJORAS ECONOMICAS.....	31
3.1.1 INDICADORES DE CALIDAD DURANTE Y DESPUES DE LA MIGRACION.....	31
3.1.2 INFLUENCIA DEMOSTRADA CON ESTADISTICAS DE INDICADORES	32
3.2 MEJORAS TECNICAS	37
3.2.1 ESCALABILIDAD.....	37
3.2.2 TOPOLOGIA FULL MESH REAL.....	37
3.2.3 PROTOCOLOS DE ENRUTAMIENTO CLIENTE-PROVEEDOR (CE-PE) SOBRE VRF	39
3.2.4 PROVISIÓN DE QoS NATIVO EN LAS REDES DE DISTRIBUCIÓN Y NÚCLEO	41
3.2.5 IPV6	44

3.2.6 MULTICAST	45
3.2.7 MINIMIZACION DE INTELIGENCIA DEL CPE	46
3.2.8 FLEXIBILIDAD EN LA GESTION DEL CPE.....	47
CONCLUSIONES Y RECOMENDACIONES	48
ANEXOS	50

ÍNDICE DE TABLAS

Tabla I.I	Tipos de enrutadores PE.....	14
Tabla II.I	Comparación de servicios.....	25
Tabla III.I	Disponibilidad de la red entre Nov 05 y Feb 09.....	34
Tabla III.II	Datos sobre los anchos de banda vendidos entre 2006 y 2009.....	36
Tabla IV.I	Diseño QoS.....	43

ÍNDICE DE FIGURAS

Figura 1.1	Enlaces Interurbanos de Fibra Óptica.....	9
Figura 1.2	Esquema de red capa 2 inicial.....	16
Figura 1.3	Esquema de red capa 2 modificado.....	17
Figura 1.4	Nuevo esquema de red interurbana.....	19
Figura 2.1	Aplicación de aprovisionamiento VPNs MPLS.....	22
Figura 2.2	Aplicación de aprovisionamiento VPNs MPLS, clientes.....	23
Figura 3.1	Disponibilidad promedio entre Noviembre 2005 y Febrero 2009.....	35
Figura 3.2	Ancho de banda promedio por acceso.....	36
Figura 3.3	Implementación “full mesh”VPN capa3 MPLS.....	38
Figura 3.4	Implementación de túneles IP en topología Hub and Spoke (estrella).....	39

ABREVIATURAS Y SIGLAS

ATM: Asynchronous Transfer Mode/Modo de transferencia asíncrono

BGP: Border Gateway Protocol/ Protocolo de pasarela de borde

CIR: Committed information rate / Tasa de información convenida.

CPE: Customer Premises Equipment / Equipo en las premisas del cliente

DWDM: Dense wavelength division multiplexing / Multiplexación por división de longitud de onda densa

EIGRP: Enhanced Interior Gateway Routing Protocol / Protocolo de enrutamiento de pasarela interior mejorado.

GBPS (GBit/s): Gigabits per second / Gigabits por segundo

IEEE: Institute of electrical and electronics engineers / Instituto de ingenieros eléctricos y electrónicos

IP: Internet Protocol / Protocolo de Internet

IPTV: IP Television / Televisión IP

IPV4: IP version 4 / IP versión 4

IPV6: IP version 6 / IP versión 6

LAN: Local Area Network / Red de área local

MBPS (Mbit/s): Megabits per second / Megabits por segundo

MPLS: Multiprotocol label switching / Conmutación por etiquetas multiprotocolo

OSI: Open system interconnection / Interconexión de sistema abierto

OSPF(v3): Open shortest path first (version 3) / Camino más corto primero (versión 3)

RIP(v2): Routing Information protocol (version 2) / Protocolo de información de enrutamiento
(versión 2)

SDH: Synchronous Digital Hierarchy / Jerarquía digital síncrona.

TDM: Time division multiplexing / Multiplexación por división de tiempo

UTP: Unshielded twisted pair / Par trenzado sin recubrimiento

VPN: Virtual private network / Red privada virtual

VRF: Virtual routing forwarding / Enrutamiento – encaminamiento virtual

TERMINOLOGIA BÁSICA

ADDRESS FAMILY: Dentro de BGP, un protocolo ruteado, por ejemplo IPv4.

BIT: Dígito binario.

BROADCAST: Difusión. Dirección que representa a todos los miembros de una subred.

BYTE: Conjunto de 8 bits

ENRUTADOR P: Enrutador en el núcleo del proveedor, cuya función es encaminar el tráfico en función de las etiquetas distribuidas en una implementación MPLS.

ENRUTADOR PE: Enrutador en el borde entre el proveedor y la última milla del cliente, cuya función es encaminar el tráfico mediante conmutación de etiquetas y también mediante la dirección IP destino en una implementación MPLS.

FULL MESH: Topología de red en la que cada elemento se enlaza con otro.

GRE: Generic Routing Encapsulation. Encapsulamiento de datagramas capa 3 dentro de datagramas IP.

HUB AND SPOKE: Topología de red en la que los elementos satélite (spoke) se enlazan exclusivamente con un elemento central (hub). También se la conoce como topología estrella.

IMPORT MAP: Definición de las subredes que se pueden importar de una VRF a otra.

IPinIP: Encapsulamiento de datagramas IP dentro de otros datagramas IP.

MULTICAST: Difusión múltiple basada en la pertenencia a grupos. La dirección ip multicast representa a todos los miembros de un grupo.

NPEG2/RSP-720/SUP 32: Procesadores de los enrutadores Cisco 7200 y 7600

ROUTE DISTINGUISHER: Campos de dirección que permiten convertir una dirección IP en una dirección VPN, por ejemplo de IPv4 a VPNv4. Su longitud es de 64 bits

ROUTE TARGET: Definición de los prefijos (subredes) que una VRF puede importar de otra.

SPANNING TREE: Protocolo de eliminación de lazos en un segmento conmutado (capa 2). También provee convergencia en caso de fallas de enlace.

UNICAST: Un solo elemento. Dirección IP que representa a un solo elemento de la red.

VPNv4: Dirección tipo VPN compuesta por un route distinguisher más la dirección IPv4. Su longitud es 96 bits.

INTRODUCCIÓN

El presente informe resume los cambios realizados en las redes de núcleo y distribución de la red de datos de Telconet S.A.

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.

Junto con el ingeniero Nicolás Rigo, encargado por Cisco Systems a nuestro caso, se formó un comité de diseño y planeación integrado por:

- Gerencia Técnica Nacional, Ing. Servio Lima
- Gerencia de Proyectos, Ing. Alexandra Alvarado
- Jefe de Seguridades Informáticas, Ing. Alfonso Aranda
- Jefe de Soporte Técnico, Carlos Montero

En este informe se ha documentado la última versión aplicada a la red que fue producto de numerosas y extensas reuniones de diseño hasta llegar al consenso avalado por el Ing. Rigo (Cisco Systems).

Dada la naturaleza de la empresa, los cambios se realizaron con extrema planeación y cuidado, minimizando las interrupciones de servicio de tal forma en que los abonados de Telconet S.A. se afecten en la menor medida posible.

Puedo resumir mis funciones de la siguiente forma:

- Miembro del comité de diseñadores de la nueva red

- Creación del producto EoMPLS (L2VPN) para la provisión de circuitos capa 2 punto a punto.
- Creación del esquema de monitoreo de los clientes aislados en una VRF (L3VPN) a través de los NOCs en Quito y Guayaquil.
- Migración de varias ciudades de tecnología solo IP a IP+MPLS.
- Creación del esquema de soporte de calidad de servicio en las redes de acceso y distribución

1. DISEÑO Y MIGRACIÓN

1.1 CONCEPTOS BÁSICOS DE REDES

A continuación se detallan las tecnologías más relevantes en la realización de este trabajo.

Al final de este informe puede consultarse más detalle en el “Anexo de teoría”.

1.1.1 ETHERNET

Protocolo de comunicación diseñado para redes de área local. Define estándares en los niveles 1 y 2 del modelo OSI. Su nombre proviene del concepto físico de ether.

Es una red tipo bus que define el acceso al medio por disputa a través de CSMA/CD (Carrier Sense Multiple Access with Collision Detection). A partir de Ethernet, la IEEE definió, en 1985, el estándar 802.3

A través del tiempo Ethernet se convirtió en la tecnología LAN de mayor implementación y sufrió ajustes a medida que los avances tecnológicos mejoraban las velocidades y el modo de operación pasó del original half-duplex a full-duplex.

1.1.2 IEEE 802.1Q

Es un estándar de la IEEE utilizado para etiquetar tramas Ethernet como pertenecientes a diferentes segmentos de red virtuales (VLANs). Esto permite que múltiples redes compartan el mismo medio físico sin ocasionar interferencias (trunking).

802.1Q añade un campo de 4 bytes al frame Ethernet; este campo conocido como "TAG" se coloca entre la dirección origen y el campo "tipo" o "longitud", según sea el tipo de frame usado.

1.1.3 REDES IP

IP (Internet Protocol) es un protocolo de telecomunicaciones no orientado a conexión usado tanto por el origen como por el destino para la comunicación de datos a través de una red de paquetes conmutados (datagramas). Su dominio se encuentra en el nivel 3 del modelo OSI.

El Protocolo de Internet provee un servicio de datagramas no fiable (*best effort*). IP no provee ningún mecanismo para determinar si un paquete alcanza o no su destino y únicamente proporciona seguridad (mediante checksums o sumas de comprobación) de sus cabeceras y no de los datos transmitidos. Por ejemplo, al no garantizar nada sobre la recepción del paquete,

éste podría llegar dañado, en otro orden con respecto a otros paquetes, duplicado o simplemente no llegar.

Las redes IP son el estándar hoy en día, siendo IP versión 4 (IPv4) el protocolo más implementado, sin embargo debido a las limitaciones de escalabilidad (direcciones de 32 bits, $2^{32} = 4.294.967.296$ direcciones IP) se ha acelerado la implementación de IPv6 el cual maneja direcciones de 128 bits. Esto es: $2^{128} = 3.4 \times 10^{38}$ direcciones IP.

El tráfico IP se direcciona a diferentes segmentos a través de dispositivos conocidos como ruteadores o enrutadores. Estos equipos, en su modo más básico de operación, dirigen los datagramas leyendo la dirección destino del datagrama y revisando una entrada apropiada en una tabla de rutas.

IP es el estándar de nivel 3 en Internet y ha permitido que sobre su infraestructura se corran las más variadas aplicaciones incluyendo comunicación en tiempo real. Todos los sistemas operativos modernos ofrecen soporte para este protocolo incluyendo a dispositivos móviles, computadores personales, teléfonos, equipos de video conferencia, etc.

1.1.4 REDES MPLS

MPLS (Multiprotocol label switching; Conmutación multi-protocolo por etiquetas) es un método de conmutar paquetes a través de una red usando información contenida en etiquetas adjuntas

a datagramas IP. Estas etiquetas se insertan entre las cabeceras de los protocolos de nivel 2 y 3 para el caso de tecnologías basadas en tramas (frames) y se encuentran en los campos VPI (virtual path identifier) y VCI (virtual channel identifier) para las tecnologías basadas en celdas como es el caso de ATM.

MPLS combina tecnologías de conmutación de nivel 2 con tecnologías de enrutamiento de nivel 3. El objetivo principal es crear un esquema flexible que provea alto desempeño y estabilidad. Esto incluye ingeniería de tráfico y capacidades de red privada virtual (VPN).

En un esquema básico MPLS, un dispositivo conocido como LSR (label switched router) asigna una etiqueta a los paquetes de entrada. Estos paquetes se enrutan a lo largo de un LSP (label switched path) donde cada LSR toma la decisión del camino a usar para direccionar el tráfico basándose únicamente en el contenido de la etiqueta. En cada salto, el LSR remueve la etiqueta actual y aplica una nueva, la cual le dice al siguiente salto como debe direccionarse el paquete. Al llegar al último LSR de borde, se remueve la etiqueta actual y se entrega el paquete en el protocolo transportado, usualmente, IP.

1.1.5 VPNs CAPA 2 Y CAPA 3

Las VPNs (Virtual Private Networks; Redes Privadas Virtuales) son enlaces de datos que cruzan infraestructuras de telecomunicaciones de dos o más entidades. Es el caso típico en que una

empresa contrata a un portador para enlazar 2 o más de sus oficinas. Estos enlaces se manejan en capa 2 o capa 3, según se haya contratado el servicio.

Como ejemplo de VPNs capa 2 tenemos las redes basadas en TDM (líneas dedicadas), en Frames (X.25, Frame Relay) o en Celdas (ATM). Este tipo de implementación no intercambia información de enrutamiento (capa 3) con el portador. Se puede establecer una conexión punto a punto o multipunto mediante la creación de circuitos virtuales que aíslan el tráfico de cada cliente.

Las VPNs capa 3 orientadas a conexión, son la base del modelo de VPN tunelizada. Las tecnologías tipo túnel (IPinIP, GRE o IPSec) proveen un modelo de enlaces punto a punto sobre la infraestructura del portador o sobre una red de acceso público como Internet. La ventaja de IPSec sobre las otras tecnologías es la seguridad que ofrece en el proceso de transporte de datos, puesto que la información está encriptada desde que sale del CPE y hasta que llega al extremo remoto.

Mediante la implementación de túneles, es posible que un abonado, cliente o suscriptor maneje información de enrutamiento entre las localidades interconectadas; esto incluye el manejo de protocolos de enrutamiento como RIP, OSPF, BGP, etc. Sin embargo, el portador suele ser el administrador del CPE, por lo que cualquier implementación de este tipo se coordina con el.

Otro modelo de VPN capa 3 es el NO-orientado a conexión. Las VPNs MPLS son un claro ejemplo de ello. En este modelo se crea una “visión todos contra todos” entre los CPEs de un

cliente; esto es, una topología lógica full-mesh. El cliente puede intercambiar información de enrutamiento con el portador y este la distribuirá únicamente entre los equipos asociados a la VPN de este cliente, esto es, a la tabla de rutas (VRF, virtual router and forwarding) propia y exclusiva para el abonado en cuestión.

1.2 ESQUEMA INICIAL EN CAPA 2 ETHERNET E IP

1.2.1 CARACTERISTICAS

El esquema inicial 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 desde donde se habilitaban puertos en las siguientes ciudades y cantones:

- Guayaquil
- Milagro
- Babahoyo
- Patricia Pilar
- Ventanas
- Quevedo
- Pichincha
- Portoviejo
- Montecristi
- Manta
- Quito
- Santo Domingo

- Latacunga
- Ambato
- Riobamba
- Guaranda
- Cuenca
- Naranjal
- Machala
- Pasaje
- Huaquillas
- Progreso
- Salinas
- Puerto López
- Jipijapa

Posteriormente se desplegó una tercera ruta de Fibra Óptica donde se agregaron:

- Vinces
- Balzar
- Palestina

Adicionalmente esta fibra óptica sirvió como redundancia para los otros caminos de fibra.

Un esquema se puede observar en el siguiente diagrama:

Nótese que no todos los puntos de amplificación tenían un enrutador. Ciertos nodos simplemente regeneraban la señal a través de los switches Cisco 2970.

1.2.2 VENTAJAS

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).

Puede considerarse una ventaja el hecho de que ciertos flujos de tráfico no necesitaban pasar por los enrutadores principales de cada ciudad, sino que directamente se pasaban paquetes de datos entre CPEs. Desde el punto de vista de control y seguridad este caso no es siempre deseable por lo que se lo anota como una ventaja relativa en este diseño original.

1.2.3 DESVENTAJAS

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.

1.2.4 TIPOS DE CLIENTES

En este esquema inicial se manejaban básicamente 2 tipos de servicio:

- Acceso a Internet: Otorgando desde 1 dirección IP pública hasta varias clases C, de acuerdo a la necesidad y justificación de uso provista por el abonado.
- Comunicación de datos vía túneles IP: Utilizando enrutadores Cisco o servidores Linux mediante el uso de encapsulamiento GRE o IPinIP.

En casos excepcionales se brindaba acceso a una vlan de tal forma que el abonado podía conectar directamente en capa 2 dispositivos homologados por Telconet.

Como veremos más adelante, todos los productos tienen su equivalente en el diseño 802.1Q + MPLS de tal forma que la conectividad no solo se preserva sino que se mejoran sus características.

1.3 DISEÑO EN CAPA 2 802.1Q E IP + MPLS Y MIGRACION

1.3.1 REQUERIMIENTOS DEL 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
- Conseguir una sencilla escalabilidad de servicios y tecnologías (actualizaciones de software o módulos intercambiables) usando la nueva infraestructura.

1.3.2 JERARQUIA, SELECCIÓN Y DIMENSIONAMIENTO DE EQUIPOS

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.

Los criterios se resumen en el siguiente cuadro:

<i>Enrutador</i>	<i>Capacidad (máxima)</i>	<i>VRFs (máximo)</i>
7609-RSP720	500 Gbps	5000
7606-SUP32	20 Gbps	4000
7206-NPEG2	1 Gbps	1500
2821	70 Mbps	600

Tabla 1.1 – Tipos de enrutadores PE

Es decir, cuando un sector (ciudad, cantón, etc) llega al 80% de su capacidad máxima, es migrado al modelo superior. No se descarta la posibilidad de introducir otros modelos cuando se necesiten capacidades intermedias a las mostradas en este cuadro.

1.3.3 ADAPTACIÓN DE LA TOPOLOGÍA FÍSICA DE LA RED

La topología física predominante en el 2008 era una capa plana donde todos los CPEs dependían de una pareja de enrutadores redundantes por cada ciudad. En este modelo, se compartía un gran segmento capa 2 conmutado y se accedía a estos equipos desde cualquier lugar de la red.

El siguiente diagrama ejemplifica esta descripción.

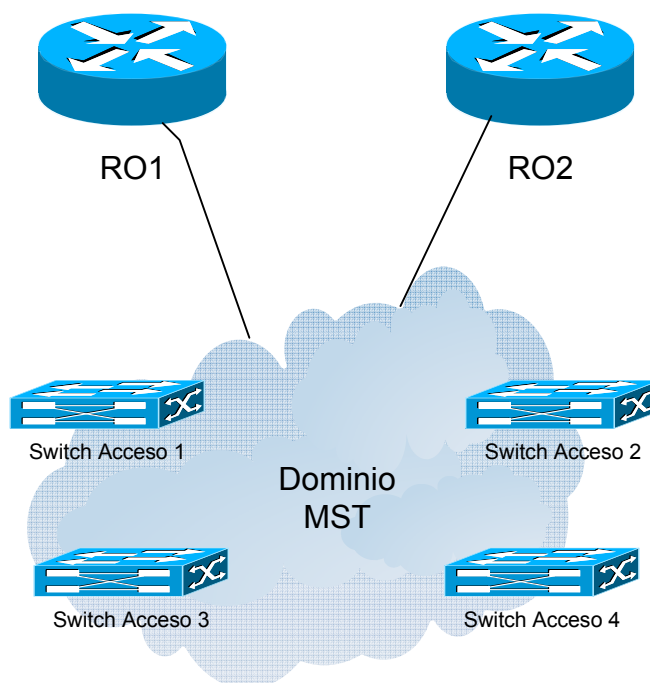


Figura 1.2 – Esquema de red capa 2 inicial

En este esquema plano, todos los switches pertenecen a la misma instancia MST (multiple spanning-tree). Las conmutaciones se manejaban de forma automatizada en los anillos principales, y, en ciertos nodos, con conmutaciones manuales.

El principal problema de este diseño es su escalabilidad. Al aumentar el número de switches de acceso y al enlazarlos sin una estructura jerárquica se pierde el control sobre el flujo de tráfico y se dificulta encontrar un problema. Adicionalmente el protocolo spanning tree no es apropiado para manejar esta cantidad de dispositivos (más de 200 en el caso de Guayaquil).

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:

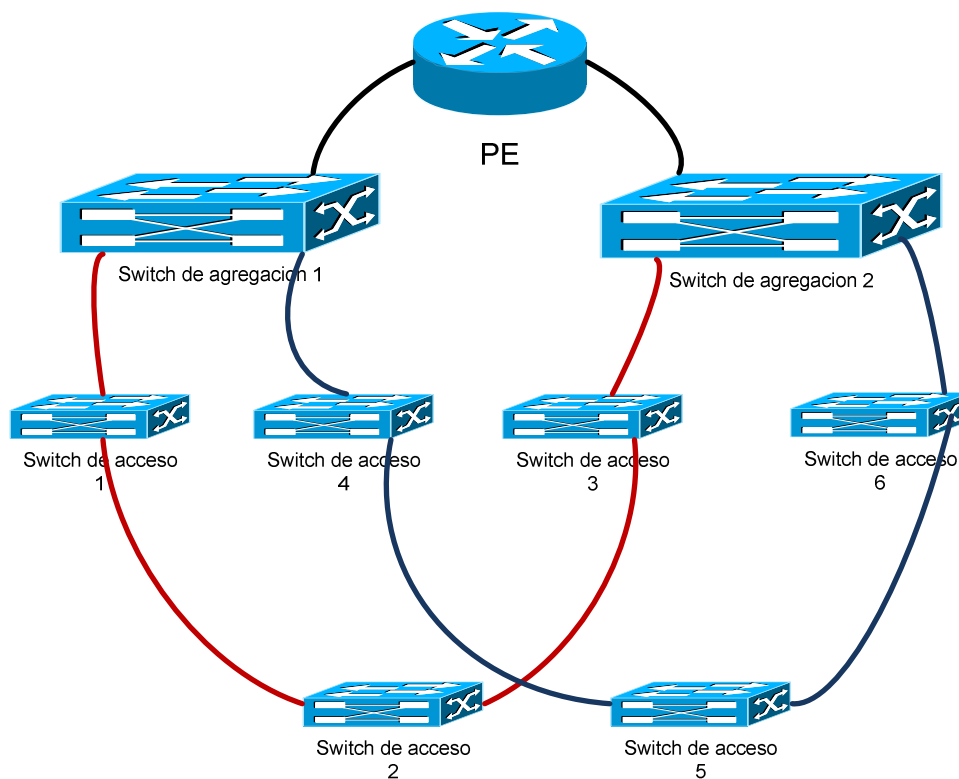


Figura 1.3 – Esquema de red capa 2 modificado

En este esquema un máximo de 15 switches conforman un anillo que termina en un enrutador PE. Este enrutador posee características de switch, con lo cual se cierra un anillo efectivo entre

los switches de acceso, agregación y el PE. De esta forma todos los CPEs conectados a la red de acceso pueden ver a su PE en capa 2. Como se aprecia en la figura cada PE maneja más de 1 anillo. La máxima cantidad de anillos propuestos en el diseño es 4.

Estos anillos están separados a nivel lógico por vlans, es decir, cada anillo maneja un rango de vlans que está excluido en el resto.

Para llegar a este diseño ordenado y escalable fue necesario un profundo cambio en la forma de planear el tendido de cables entre switches además de una modificación profunda del cableado existente. Planta externa en conjunto con el área de Networking y la Gerencia Técnica hicieron el rediseño del cableado existente para avanzar con la implementación de esta topología.

Para la red de núcleo, las conexiones físicas (cables) permanecen iguales; sin embargo la tecnología de transporte y la topología de la red han cambiado de Ethernet sobre SDH a Ethernet sobre DWDM en las ciudades más importantes. Estas conexiones son punto a punto redundantes entre enrutadores tipo PE y P.

El siguiente diagrama muestra la topología interurbana a la cual se está migrando:

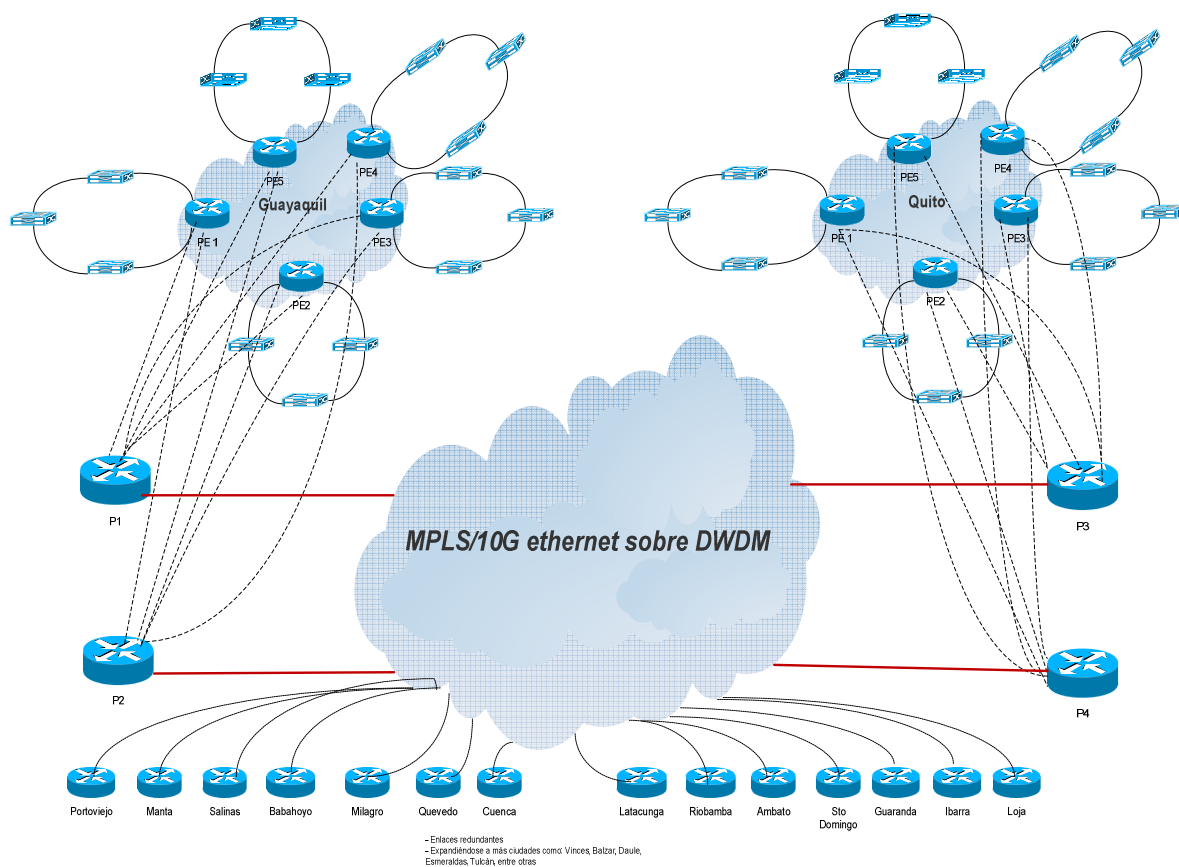


Figura 1.4 – Nuevo esquema de red interurbana

El diagrama incluye varias ciudades donde ya se ha implementado esta tecnología. Este trabajo continúa a medida que la cobertura de la red DWDM crece.

Los enrutadores tipo P están concentrados en Guayaquil (2) y Quito (2), cada uno en un nodo diferente. De esta forma se tienen 4 ubicaciones diferentes para enrutadores P.

1.3.4 RESULTADOS ESPERADOS DEL DISEÑO

La expectativa principal al implementar estas tecnologías era mantener un gran nivel de escalabilidad tanto en capacidades como servicios.

Resultados esperados adicionales fueron:

- Gestión y solución más rápida a los problemas que pudiesen presentarse en las redes de núcleo o distribución.
- Mejor y más fácil gestión de los equipos CPE.
- Mejor y más fácil monitoreo de los equipos CPE.
- Interconexiones entre clientes más sencillas.
- Mejores tiempos de convergencia para las redes de núcleo y distribución.
- Incremento en la comercialización de ancho de banda debido a las nuevas capacidades que la red podía manejar.

Obviamente todo esto se traducía en mejores ingresos económicos para la empresa, lo que se puede evidenciar en la sección 3.1 de este informe.

2. IMPLEMENTACION DEL NUEVO DISEÑO Y PROCESO DE TRANSICION

2.1 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.

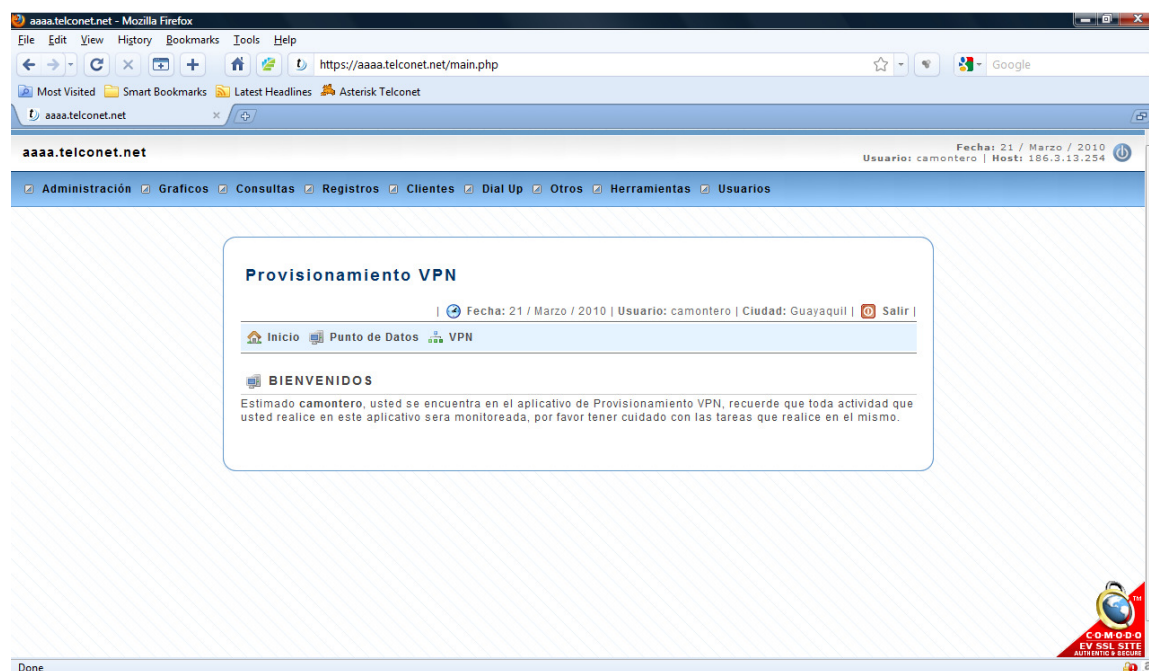
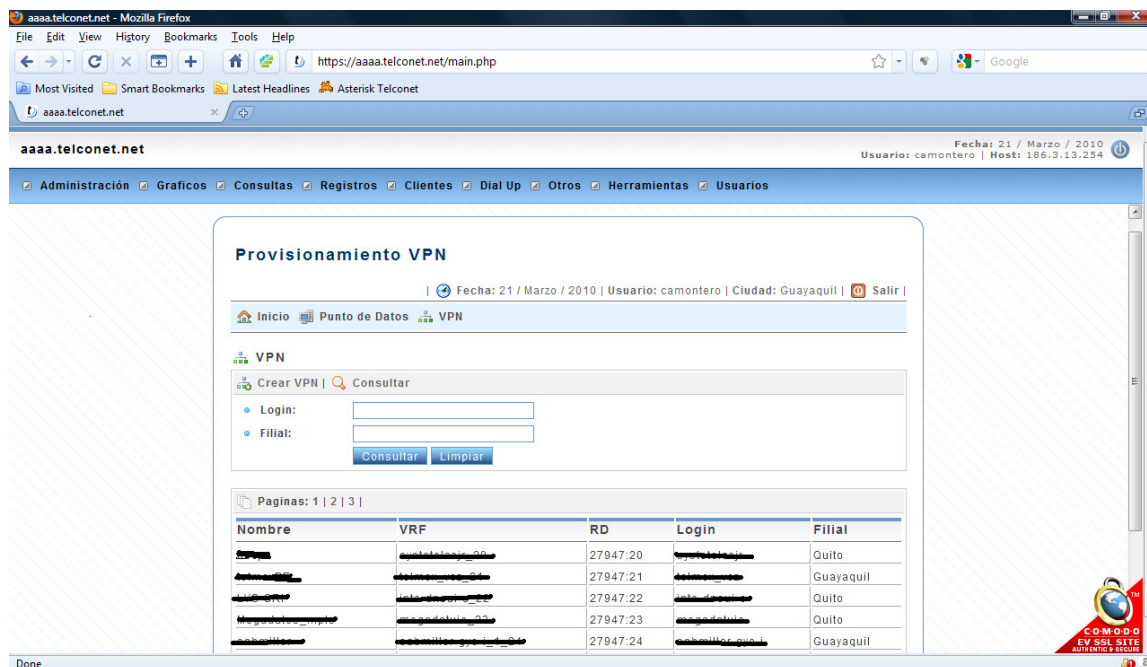


Figura 2.1 – Aplicación de aprovisionamiento VPNs MPLS

Luego de probar las aplicaciones, mediante acuerdos realizados a través del departamento comercial, empezamos a brindar el nuevo servicio con un número pequeño de clientes. El gráfico muestra otra pantalla de la aplicación creada. Se han tachado algunos nombres para proteger la confidencialidad acordada con los clientes de Telconet.

El hecho de conservar estos clientes y haber aumentado el despliegue de la solución, es la mejor prueba que podemos tener de que el nuevo esquema de VPNs funciona cumpliendo todas las necesidades de conectividad acordadas con los abonados.



The screenshot displays the 'Provisionamiento VPN' web application. The browser window shows the URL 'https://aaaa.telconet.net/main.php'. The application header includes the site name 'aaaa.telconet.net' and user information: 'Fecha: 21 / Marzo / 2010', 'Usuario: camontero', and 'Host: 166.3.13.254'. A navigation menu contains items like 'Administración', 'Graficos', 'Consultas', 'Registros', 'Clientes', 'Dial Up', 'Otros', 'Herramientas', and 'Usuarios'. The main content area is titled 'Provisionamiento VPN' and includes a search form with fields for 'Login' and 'Filiat', and buttons for 'Consultar' and 'Limpiar'. Below the form is a table with the following data:

Nombre	VRF	RD	Login	Filiat
...	...	27947.20	...	Quito
...	...	27947.21	...	Guayaquil
...	...	27947.22	...	Quito
...	...	27947.23	...	Quito
...	...	27947.24	...	Guayaquil

Figura 2.2 – Aplicación aprovisionamiento VPNs MPLS , clientes

2.2 PUESTA EN PRODUCCION

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.

En esta etapa se habilitaron los siguientes equipos:

- Enrutadores PE Guayaquil: Nodos Telepuerto, Kennedy y PPG
- Enrutadores PE Quito: Nodos Gosseal y Muros
- Enrutador PE Quevedo
- Enrutadores P Guayaquil: Nodos Telepuerto y Kennedy
- Enrutadores P Quito: Nodos Gosseal y Muros
- Enrutadores Route Reflector Guayaquil: Telepuerto y Kennedy
- Enrutadores Route Reflector Quito: Gosseal y Muros

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. El no soportar jumbo frames se debe a una limitante en los switches de la red de acceso.

2.3 COMPARACION ENTRE ESQUEMA ANTERIOR CONTRA ESQUEMA ACTUAL DE CLIENTES

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.

<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)

Tabla II.1 – Comparación de servicios

2.3.1 MIGRACION DE TUNELES IP A TUNELES IP SOBRE VRF

Esta etapa se pensó como un hito intermedio para pasar a un servicio completamente VPN capa 3.

Originalmente se pensó en que esta etapa iba a ser considerablemente larga y que necesitaríamos cambiar el direccionamiento IP de muchos CPEs, pero estudios posteriores y la

forma en que rediseñamos el aprovisionamiento y migración hicieron que apliquemos este esquema de forma global manteniendo las direcciones intactas y en una sola jornada de trabajo programado. Simplemente incluimos a todo el universo de clientes en una sola VRF. Protegimos su direccionamiento IP mediante las mismas técnicas de tunelización, IPinIP o GRE, esto quiere decir que se replica el estado original de los clientes pero se tiene tecnología MPLS en la capa de núcleo.

De esta forma se implementó la VRF “datos” sobre la cual aplicamos tunelización en los CPEs.

Algunos clientes que aún no están en la etapa final se mantienen de esta forma.

2.3.2 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.

El siguiente es un ejemplo de una VRF para un cliente:

```
ip vrf systotelcojr_20
rd 27947:20
route-target export 27947:20
route-target export 27947:2
```

```
route-target import 27947:20
route-target import 27947:1
```

La subinterfaz correspondiente es:

```
interface TenGigabitEthernet1/3.133
 encapsulation dot1Q 133
 ip vrf forwarding systotelcojr_20
 ip address 10.11.16.201 255.255.255.248
 no ip redirects
 no ip unreachable
 no ip proxy-arp
 arp timeout 300
```

Configuración BGP para la VRF:

```
address-family ipv4 vrf systotelcojr_20
 no synchronization
 redistribute connected
 redistribute static
 neighbor 10.11.16.204 remote-as 65351
 neighbor 10.11.16.204 description XXXXX
 neighbor 10.11.16.204 update-source TenGigabitEthernet1/3.133
 neighbor 10.11.16.204 version 4
 neighbor 10.11.16.204 activate
 neighbor 10.11.16.204 send-community
 neighbor 10.11.16.204 weight 900
 neighbor 10.11.16.204 soft-reconfiguration inbound
 neighbor 10.11.16.204 maximum-prefix 1000 warning-only
 neighbor 10.11.16.205 remote-as 65353
 neighbor 10.11.16.205 description YYYYYY
 neighbor 10.11.16.205 update-source TenGigabitEthernet1/3.133
 neighbor 10.11.16.205 version 4
 neighbor 10.11.16.205 activate
 neighbor 10.11.16.205 send-community
 neighbor 10.11.16.205 weight 900
 neighbor 10.11.16.205 soft-reconfiguration inbound
 neighbor 10.11.16.205 maximum-prefix 1000 warning-only
 neighbor 10.11.16.206 remote-as 65360
 neighbor 10.11.16.206 description ZZZZZZZ
 neighbor 10.11.16.206 update-source TenGigabitEthernet1/3.133
 neighbor 10.11.16.206 version 4
```

```
neighbor 10.11.16.206 activate
neighbor 10.11.16.206 send-community
neighbor 10.11.16.206 weight 1000
neighbor 10.11.16.206 soft-reconfiguration inbound
neighbor 10.11.16.206 maximum-prefix 1000 warning-only
exit-address-family
```

Como se aprecia en las configuraciones, se definen todos los elementos necesarios para proveer el servicio, esto es:

- Nombre de la vrf
- Route Distinguisher
- Vlan
- Direccionamiento IP
- Enrutamiento en BGP

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.

2.3.3 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. Nótese el siguiente ejemplo:

```
ip vrf client1
  rd 27947:29
  route-target export 27947:29
  route-target export 27947:2
  route-target import 27947:29
  route-target import 27947:1

!
ip vrf cliente2
  rd 27947:24
  route-target export 27947:24
  route-target export 27947:2
  route-target import 27947:24
  route-target import 27947:1
```

Estos clientes están aislados; el primero exporta con un route-target igual a 27947:29 y 27947:2; el segundo lo hace con 27947:24 y 27947:2. De igual forma solo importan los prefijos de la VRF de monitoreo (27947:1) y sus propios prefijos (27947:29 y 27947:24 respectivamente).

La interconexión involucra cambiar estas VRFs de la siguiente forma:

```
ip vrf client1
  rd 27947:29
  route-target export 27947:29
  route-target export 27947:2
  route-target import 27847:24
```

```
route-target import 27947:29
route-target import 27947:1

!
ip vrf cliente2
rd 27947:24
route-target export 27947:24
route-target export 27947:2
route-target import 27947:29
route-target import 27947:24
route-target import 27947:1
```

Se han agregado a cada VRF las líneas de configuración que permiten importar los prefijos del cliente con quien desean interconectarse.

Podemos ser más granulares con los prefijos a importar mediante el uso de import-maps; por ejemplo pudiese importarse una sola dirección IP (/32) o solo una subred; esto se realiza de acuerdo a los requerimientos de los clientes.

3. RESULTADOS DE LA IMPLEMENTACION

3.1 MEJORAS ECONOMICAS

3.1.1 INDICADORES DE CALIDAD DURANTE Y DESPUES DE LA MIGRACION

La gerencia general de Telconet mantiene 2 indicadores claves para monitorear el desempeño del negocio; estos son:

- Disponibilidad de la red (en porcentaje)
- Notas de crédito por penalidades

La disponibilidad de la red se define como la relación llevada a porcentaje del tiempo en que la red está operativa para dar servicio sobre el tiempo total en el período de medición, esto es:

$$\text{Disponibilidad} = \frac{\text{tiempo de red disponible}}{\text{tiempo total}} \times 100\%$$

El período de medición es mensual.

Las notas de crédito por penalidades son descuentos en las facturas de los abonados debido a que no se ha cumplido con los niveles de servicio acordados con los mismos. Si bien existen clientes con niveles de servicio negociados de forma personalizada, los valores por defecto son:

- Servicio de acceso a internet: 99.5%
- Servicio de transmisión de datos: 99.6%

En el siguiente numeral se muestran los datos relacionados a la disponibilidad de la red. Las notas de crédito están categorizadas como información confidencial por el área financiera.

Adicionalmente se presentará información sobre el incremento de ancho de banda de los abonados antes, durante y después de la reestructuración de la red.

3.1.2 INFLUENCIA DEMOSTRADA CON ESTADISTICAS DE INDICADORES

El último trimestre del año 2005 es importante ya que no se realizaron cambios en la red hasta Mayo del 2006 pero tuvimos las primeras revisiones de diseño en conjunto con el personal de Cisco Systems.

Este indicador es una disponibilidad promedio de equipos considerados críticos en la red; es decir, al tener una disponibilidad menor al 100% no implica que toda la red estuvo fuera de servicio durante un tiempo. Puede deberse a que algún equipo crítico no estuvo disponible y dicha indisponibilidad afecta al promedio como lo refleja el indicador.

MES / AÑO	% DISPONIBILIDAD
NOV 05	97.16
DIC 05	95.65
ENE 06	99.15
FEB 06	97.96
MAR 06	98.84
ABR 06	98.28
MAY 06	99.37
JUN 06	99.06
JUL 06	99.26
AGO 06	99.39
SEP 06	99.38
OCT 06	98.95
NOV 06	99.75
DIC 06	98.91
ENE 07	99.05
FEB 07	99.41
MAR 07	98.84
ABR 07	97.84
MAY 07	99.37
JUN 07	99.80
JUL 07	99.74
AGO 07	99.72
SEP 07	99.86
OCT 07	99.80
NOV 07	99.87
DIC 07	99.94
ENE 08	99.90
FEB 08	99.83
MAR 08	99.88
ABR 08	99.89
MAY 08	99.96
JUN 08	99.87
JUL 08	99.89
AGO 08	99.93
SEP 08	99.97
OCT 08	99.94

NOV 08	99.95
DIC 08	99.94
ENE 09	99.96
FEB 09	99.90

Tabla III.I – Disponibilidad de la red entre Nov 2005 y Feb 2009

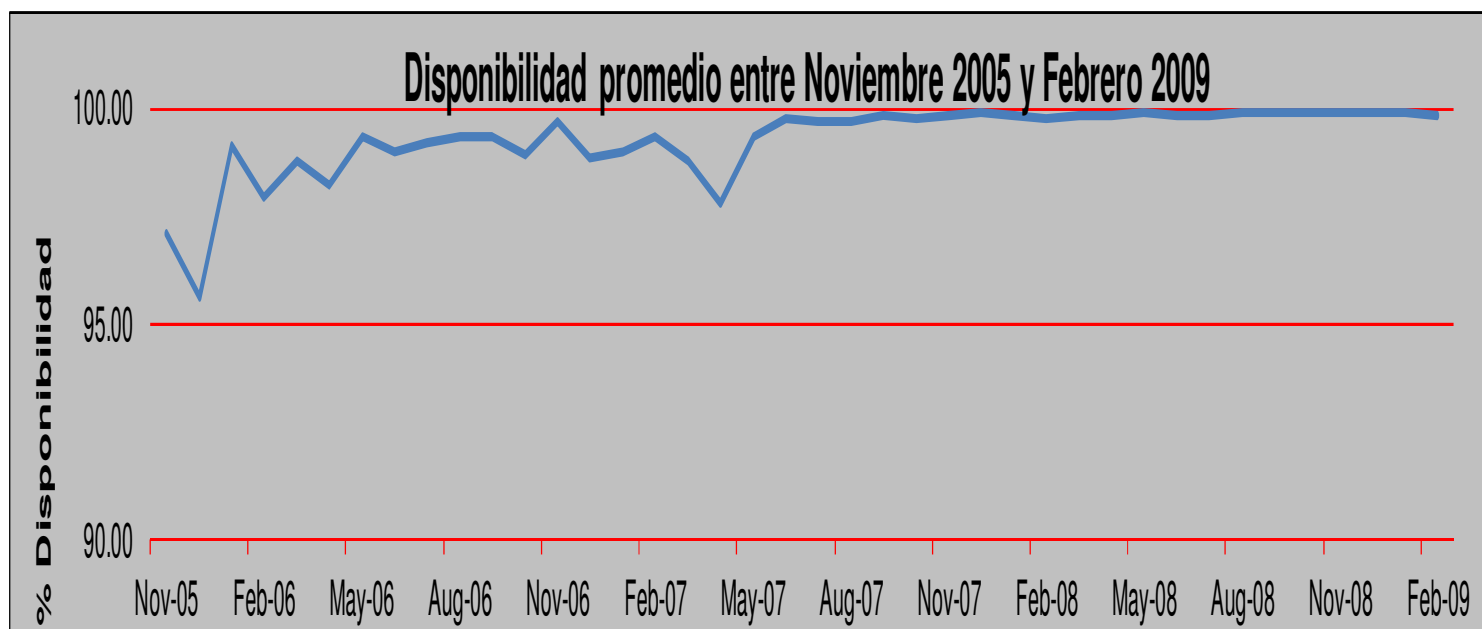


Figura 3.1 – Disponibilidad promedio entre Noviembre 2005 y Febrero 2009

Incrementos de ancho de banda entre los años 2006 y 2009:

Los años 2006 y 2007 solo presentan un ancho de banda de "acceso", es decir, no existe registro si corresponde a servicio de datos o internet. Esto si está clasificado en los años 2008 y 2009.

Año	BW promedio Datos	BW promedio Internet	BW promedio "Acceso"	Min BW "Acceso"	Max BW "Acceso"	Min BW Internet	Max BW Internet	Min BW Datos	Max BW Datos
2006	N/A	N/A	380.955	20	22528	N/A	N/A	N/A	N/A
2007	N/A	N/A	1340.277	20	169088	N/A	N/A	N/A	N/A
2008	1391.524	970.744	1265.873	16	169088	16	46080	20	169088
2009	4481.494	3284.723	3883.108	25	716800	25	465000	32	716800
Todas las cantidades están dadas en kilobits por segundo (kbps)									
Entiéndase por "Acceso" BW comercializado sin distinción del tipo de servicio									

Tabla III.II Datos sobre los anchos de banda vendidos entre 2006 y 2009

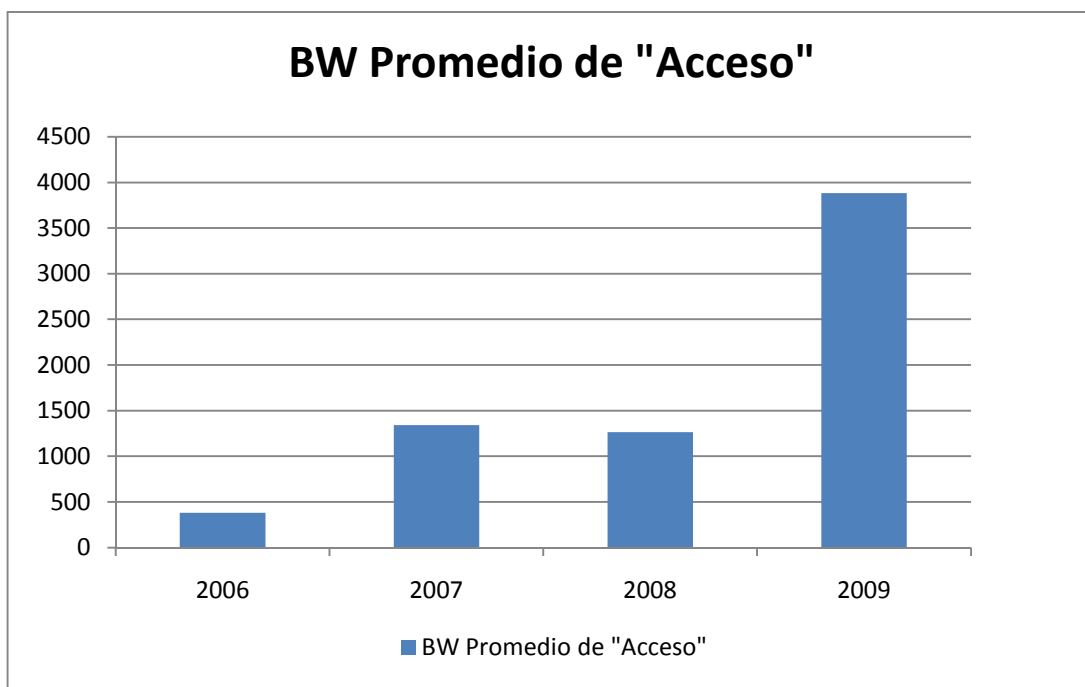


Figura 3.2. Ancho de banda promedio por acceso

Como se aprecia en los datos mostrados existe mucha más cantidad de información utilizando la red actualizada. El ancho de banda promedio de acceso se multiplicó por 10 entre los años 2006 y 2009. La red del año 2005 no hubiese podido manejar más usuarios y con más ancho de banda cada uno.

3.2 MEJORAS TECNICAS

3.2.1 ESCALABILIDAD

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

3.2.2 TOPOLOGIA 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.

El siguiente diagrama lo ejemplifica:

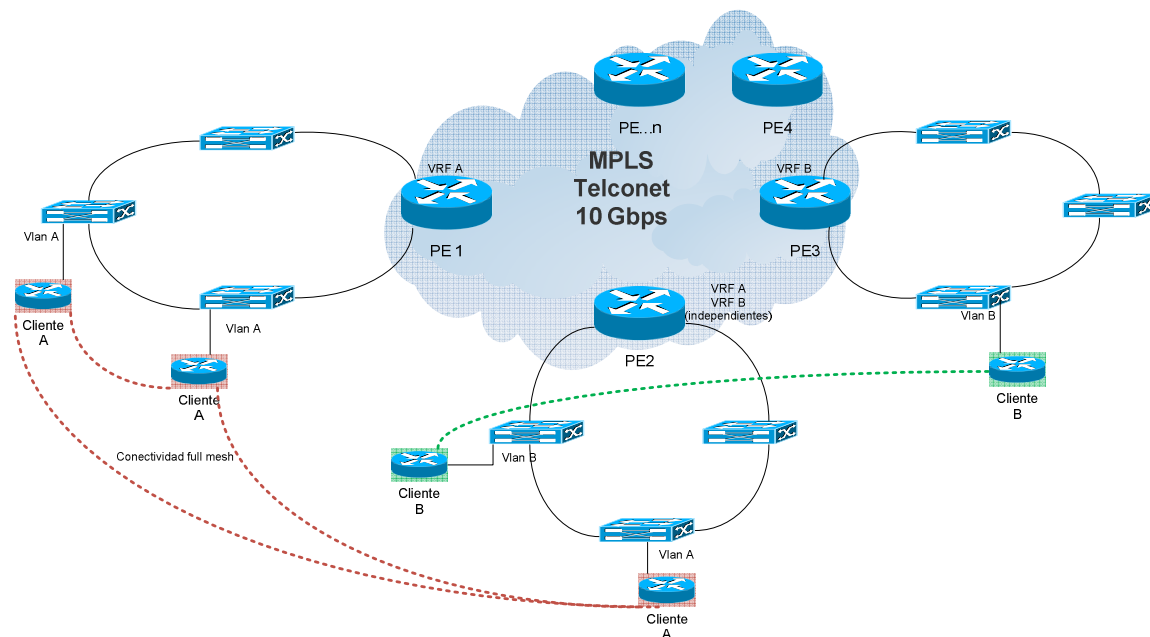


Figura 3.3 – Implementación "full mesh"VPN capa 3 MPLS

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 como se evidencia en la siguiente figura:

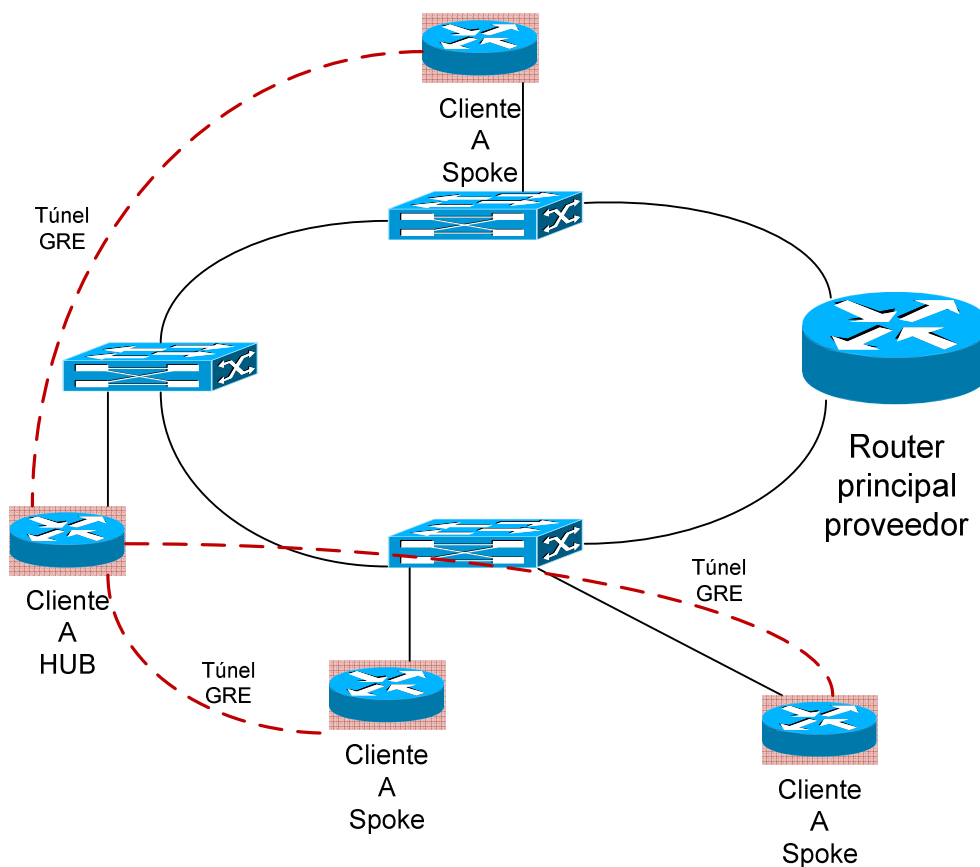


Figura 3.4 – Implementación de túneles IP en topología hub and spoke (estrella)

3.2.3 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 IGPs, 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. A continuación se muestra una configuración de ejemplo para un abonado corriendo EIGRP en su vrf:

```
router eigrp 27947
  no auto-summary
  !
  address-family ipv4 vrf pmatriz_1_30
    autonomous-system 65000
    network 10.21.16.161 0.0.0.0
    no auto-summary
    redistribute bgp 27947 metric 2 2 2 2 2
  exit-address-family
```

El aprendizaje entre enrutadores PE sigue siendo vía BGP, como se aprecia en las líneas:

```
address-family ipv4 vrf pmatriz_1_30
  no synchronization
  redistribute connected
  redistribute static
  redistribute eigrp 65000
exit-address-family
```

3.2.4 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.

La siguiente tabla define el tratamiento que se le da esos paquetes tanto a la entrada (clasificación y marcado) como a la salida (encolamiento):

INTERFACES 10G											
DSCP	DSCP dec	EXP	COS	COLA	PESO	LIMITE	T1 min	T1 max	CIR Ingreso	Exceed-action	Violate-action
EF, AF41	46, 34	5	5	8	N/A	25%	80%	100%	800 Mbps	set-policed-dscp	set-policed-dscp
AF31	26	3	3	7	35	10%	80%	100%	600 Mbps	set-policed-dscp	set-policed-dscp
CS3	24	6	6	6	12	5%	80%	100%	500 Mbps	set-policed-dscp	set-policed-dscp
AF21	18	2	2	3	20	11%	80%	100%	600 Mbps	set-policed-dscp	set-policed-dscp
AF11	10	1	1	2	15	20%	80%	100%	600 Mbps	set-policed-dscp	set-policed-dscp
DE	0	0	0	1	30	25%	80%	100%	N/A	N/A	N/A
CS7	56	4	4	4	10	4%	80%	100%	N/A	N/A	N/A
INTERFACES 1G											
DSCP	DSCP dec	EXP	COS	COLA	PESO	LIMITE	T1 min	T1 max	CIR Ingreso	Exceed-action	Violate-action
EF, AF41	46, 34	5	5	3	N/A	40%	80%	100%	400 Mbps	set-policed-dscp	set-policed-dscp
AF31	26	3	3	2	75	30%	80%	100%	100 Mbps	set-policed-dscp	set-policed-dscp
CS3	24	6	6	2					50 Mbps	set-policed-dscp	set-policed-dscp
AF21	18	2	2	2					100 Mbps	set-policed-dscp	set-policed-dscp
CS7	10	4	4	2					N/A	N/A	N/A
AF11	0	1	1	1	25	30%	80%	100%	80 Mbps	set-policed-dscp	set-policed-dscp
DE	56	0	0	1					N/A	N/A	N/A

Tabla III.III – Diseño QoS

Las acciones de “exceed” y “violate” son iguales. En el caso de Telconet se sobre escribe el DSCP con el valor 0 cuando el tráfico de entrada ha superado el CIR correspondiente.

Dada la plataforma usada en la red de acceso, es posible replicar esta configuración mapeando los valores de DSCP a COS cuando los paquetes IP entran al dominio de capa 2 de la red de acceso. De esta forma mantenemos QoS de punta a punta entre los CPEs de los abonados los cuales son una parte imprescindible para la correcta implementación de este servicio; las redes

de distribución y núcleo no marcan el tráfico, solo lo clasifican. Los CPEs son los encargados de poner las marcas correctas.

3.2.5 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.

3.2.6 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.

3.2.7 MINIMIZACION DE 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.

3.2.8 FLEXIBILIDAD EN LA GESTION 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 en la sección 3.2.3.

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.
6. La adaptabilidad tecnológica de la plataforma es excelente en los equipos de rango alto tanto en software como en hardware. Evidencia de esto es la adición de módulos de seguridad en los equipos para contrarrestar ataques distribuidos de denegación de servicio. Otra posibilidad que se analiza es la implementación de tarjetas de firewall

(cortafuegos) para brindar servicios personalizados a cada cliente mediante instancias virtuales o contextos de firewall. En resumen, las plataformas están listas para ser actualizadas de forma rápida y sencilla de modo que brinden nuevos servicios. En aquellas ciudades con enrutadores de menores características es necesario un cambio de equipo a plataforma 7600 para conseguir la implementación de nuevas prestaciones.

7. Es criterio del autor de este informe 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. Por ejemplo, se destaca que las plataformas escogidas para ruteo y conmutación (switching) de nuestro proveedor de equipos continúan ofreciendo la mejor relación costo/beneficio. 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.
8. La implementación de 802.1Q y MPLS son un estándar de la industria. Lo descrito en este informe puede y debe ser aplicado por empresas portadoras de datos para mantener un nivel competitivo en el mercado y mejorar sus prestaciones de servicios. Ambas tecnologías permiten escalar a un gran número de clientes manteniendo niveles satisfactorios de seguridad y calidad siempre y cuando se escojan los equipos apropiados para cada implementación particular.

ANEXO 1

CONCEPTOS

ETHERNET

Las principales revisiones de Ethernet son:

- Ethernet experimental 1972 (patentado en 1978) 2,85 Mbit/s sobre cable coaxial en topología de bus.
- Ethernet II (DIX v2.0) 1982 10 Mbit/s sobre coaxial fino (thinnet) - La trama tiene un campo de tipo de paquete. El protocolo IP usa este formato de trama sobre cualquier medio.
- IEEE 802.3 1983 10BASE5 10 Mbit/s sobre coaxial grueso (thicknet). Longitud máxima del segmento 500 metros - Igual que DIX salvo que el campo de Tipo se substituye por la longitud.
- 802.3a 1985 10BASE2 10 Mbit/s sobre coaxial fino (thinnet o cheapernet). Longitud máxima del segmento 185 m
- 802.3b 1985 10BROAD36
- 802.3c 1985 Especificación de repetidores de 10 Mbit/s
- 802.3d 1987 FOIRL (Fiber-Optic Inter-Repeater Link) enlace de fibra óptica entre repetidores.
- 802.3e 1987 1BASE5 o StarLAN
- 802.3i 1990 10BASE-T 10 Mbit/s sobre par trenzado no apantallado (UTP). Longitud máxima del segmento 100 metros.

- 802.3j 1993 10BASE-F 10 Mbit/s sobre fibra óptica. Longitud máxima del segmento 1000 metros.
- 802.3u 1995 100BASE-TX, 100BASE-T4, 100BASE-FX Fast Ethernet a 100 Mbit/s con auto-negociación de velocidad.
- 802.3x 1997 Full Duplex (Transmisión y recepción simultáneas) y control de flujo.
- 802.3y 1998 100BASE-T2 100 Mbit/s sobre par trenzado no apantallado(UTP). Longitud máxima del segmento 100 metros
- 802.3z 1998 1000BASE-X Ethernet de 1 Gbit/s sobre fibra óptica.
- 802.3ab 1999 1000BASE-T Ethernet de 1 Gbit/s sobre par trenzado no apantallado
- 802.3ac 1998 Extensión de la trama máxima a 1522 bytes (para permitir las "Q-tag") Las Q-tag incluyen información para *802.1Q VLAN y manejan prioridades según el estándar 802.1p.
- 802.3ad 2000 Agregación de enlaces paralelos (Trunking).
- 802.3ae 2003 Ethernet a 10 Gbit/s ; 10GBASE-SR, 10GBASE-LR
- IEEE 802.3af 2003 Alimentación sobre Ethernet (PoE).
- 802.3ah 2004 Ethernet en la última milla.
- 802.3ak 2004 10GBASE-CX4 Ethernet a 10 Gbit/s sobre cable bi-axial.
- 802.3an 2006 10GBASE-T Ethernet a 10 Gbit/s sobre par trenzado no apantallado (UTP)
- 802.3ap en proceso (borrador) Ethernet de 1 y 10 Gbit/s sobre circuito impreso.
- 802.3aq en proceso (borrador) 10GBASE-LRM Ethernet a 10 Gbit/s sobre fibra óptica multimodo.

- 802.3ar en proceso (borrador) Gestión de Congestión
- 802.3as en proceso (borrador) Extensión de la trama

La trama de nivel 2 de Ethernet está definida de la siguiente forma:

Trama IEEE 802.3	Preámbulo	SOF	Destino	Origen	Longitud	Datos	Relleno	FCS
	7 bytes	1 byte	6 bytes	6 bytes	2 bytes	0 - 1500 bytes	0 - 46 bytes	4 bytes
Trama Ethernet II (DIX)	Preámbulo	Destino	Origen	Tipo	Datos	Relleno	FCS	
	8 bytes	6 bytes	6 bytes	2 bytes	0 - 1500 bytes	0 - 46 bytes	2 o 4 bytes	

Preámbulo

Un campo de 7 bytes (56 bits) con una secuencia de bits usada para sincronizar y estabilizar el medio físico antes de iniciar la transmisión de datos. El patrón del preámbulo es:

10101010 10101010 10101010 10101010 10101010 10101010 10101010

Estos bits se transmiten en orden, de izquierda a derecha y en la codificación Manchester representan una forma de onda periódica.

SOF (Start Of Frame) Inicio de Trama

Campo de 1 byte (8 bits) con un patrón de 1s y 0s alternados y que termina con dos 1s consecutivos. El patrón del SOF es: 10101011. Indica que el siguiente bit será el bit más significativo del campo de dirección MAC de destino.

Aunque se detecte una colisión durante la emisión del preámbulo o del SOF, el emisor debe continuar enviando todos los bits de ambos hasta el fin del SOF.

Dirección de destino

Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo EUI-48 hacia la que se envía la trama. Esta dirección de destino puede ser de una estación, de un grupo *multicast* o la dirección de *broadcast* de la red. Cada estación examina este campo para determinar si debe aceptar la trama (si es la estación destinataria).

Dirección de origen

Campo de 6 bytes (48 bits) que especifica la dirección MAC de tipo EUI-48 desde la que se envía la trama. La estación que deba aceptar la trama conoce por este campo la dirección de la estación origen con la cual intercambiará datos.

Tipo

Campo de 2 bytes (16 bits) que identifica el protocolo de red de alto nivel asociado con la trama o, en su defecto, la longitud del campo de datos. La capa de enlace de datos interpreta este campo. (En la IEEE 802.3 es el campo longitud y debe ser menor o igual a 1526 bytes.)

Datos

Campo de 0 a 1500 Bytes de longitud. Cada Byte contiene una secuencia arbitraria de valores. El campo de datos es la información recibida del nivel de red (la carga útil). Este campo, también incluye los H3 y H4 (cabeceras de los niveles 3 y 4), provenientes de niveles superiores.

Relleno

Campo de 0 a 46 bytes que se utiliza cuando la trama Ethernet no alcanza los 64 bytes mínimos para que no se presenten problemas de detección de colisiones cuando la trama es muy corta.

FCS (Frame Check Sequence - Secuencia de Verificación de Trama)

Campo de 32 bits (4 bytes) que contiene un valor de verificación CRC (Control de redundancia cíclica). El emisor calcula el CRC de toda la trama, desde el campo destino al campo CRC suponiendo que vale 0. El receptor lo recalcula, si el valor calculado es 0 la trama es válida.

802.1Q

Los sub-campos del TAG son:

Identificador de protocolo de etiquetas (TPID): Tiene 16 bits y se establece en 0x8100 para identificar frames con etiqueta 802.1Q.

Punto de código de prioridad (PCP): Tiene 3 bits y refiere el nivel de prioridad del frame entre 0 (el más bajo) y 7 (el más alto).

Indicador de formato canónico (CFI): Tiene 1 bit y se establece en 0 si la dirección MAC está en formato canónico o 1 si está en formato no canónico.

Identificador de VLAN (VID): Tiene 12 bits y especifica a qué vlan pertenece el frame. Esto permite tener 4094 vlans diferentes. 0x0 y 0xFFF no se usan como identificadores de vlan.

REDES IP

Un datagrama IP consta de los siguientes campos:

	Bits 0 -3	4 - 7	8 - 15	16 - 18	19 - 31
0	Versión	Longitud de cabecera	Servicios Diferenciados	Longitud Total	
32	Identificación			Banderas	Offset
64	Tiempo de vida		Protocolo	Checksum de cabecera	
96	Dirección de origen				
128	Dirección destino				
160	Opciones				
160 o 192+	Data				

Versión

Versión del protocolo. Tiene un valor igual a 4.

Longitud de cabecera

Indica el número de bytes en la cabecera. El valor mínimo es 5 (RFC 791), que equivale a una longitud de $5 \times 32 = 160$ bits. Su máximo valor es 15 (480 bits).

Servicios diferenciados (DiffServ)

Se definió originalmente como el campo de tipo de servicio (TOS). La RFC 2474 lo redefinió como servicios diferenciados. Permite definir valores de prioridad para el tratamiento del datagrama

Longitud total.

Campo de 16 bits que define el tamaño del datagrama en bytes, incluyendo la cabecera y la data. La longitud mínima es 20 bytes y la máxima 65535.

Identificación

Campo de 8 bits usado para identificar fragmentos de un datagrama.

Banderas

Campo de 3 bits usado para controlar fragmentos:

- Reservado: debe ser 0
- No fragmentar: Don't Fragment (DF)
- Más fragmentos: More Fragments (MF)

Offset de fragmento

Campo de 13 bits que especifica el offset de un fragmento en particular relativo a el inicio del datagrama original sin fragmentar. Se mide en bloques de 8 bytes, por ejemplo, un valor igual a 0000000000001 equivale a 8 bytes = 64 bits.

Tiempo de vida: Time To Live (TTL)

Campo de 8 bits que previene que los datagramas circulen infinitamente en una red. Se decrementa en 1 cada vez que un ruteador procesa el datagrama; esto permite que dicho datagrama pueda “expirar”.

Protocolo

Este campo define el protocolo usado en los bits de data. La IANA (Internet Assigned Numbers Authority) detalla una lista de protocolos y sus números.

Checksum de cabecera

Campo de 16 bits usado para la detección de errores en la cabecera.

Dirección origen

Es un campo de 32 bits agrupado en 4 octetos que identifica el origen del datagrama.

Dirección destino

Campo de 32 bits agrupado en 4 octetos que identifica el destino final del datagrama.

Opciones

Se pueden adicionar campos luego de la dirección destino, pero no se los utiliza frecuentemente. El final se puede terminar con un EOL (end of options list) que tiene un valor igual a 0x00; únicamente se necesita si el final de las opciones no coincide con el final de cabecera como se especificó en el campo de longitud de cabecera.

BIBLIOGRAFÍA

1. Doyle Jeff, Carroll Jennifer, Routing TCP/IP Vol I, Cisco Press, USA, Oct 19 2005, p 7-45
2. Pepelnjak Ivan, Guichard Jim, MPLS and VPN Architectures, Cisco Press, USA, Oct 31 2000, p 120-146
3. Guichard Jim, Le Faucheur Francois, Vasseur Jean-Philippe, Definitive MPLS Network Designs, Cisco Press, USA, Mar 14 2005, p 3-13
4. Bruno Anthony, CCIE Routing and Switching exam certification guide, Cisco Press, USA, Sept 2002, p 110-127