ESCUELA POLITÉCNICA DEL EJÉRCITO

DPTO. DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMATICA

"ESTUDIO DE FACTIBILIDAD PARA LA MIGRACIÓN DE REDES WAN CONVENCIONALES A LA TECNOLOGÍA MPLS"

Previa a la obtención del Título de:

INGENIERO EN SISTEMAS E INFORMÁTICA

POR: JOSÉ LUIS PASQUEL PASQUEL

SANGOLQUÍ, 30 DE AGOSTO DE 2010

CERTIFICACION

Certifico que el presente trabajo fue realizado en su totalidad por el Sr. JOSÉ LUIS PASQUEL PASQUEL como requerimiento parcial a la obtención del título de INGENIERO EN SISTEMAS E INFORMÁTICA

Sangolquí, 30 de Agosto del 2010

_____

ING. CARLOS ROMERO

DEDICATORIA

Dedico mi proyecto de Tesis a mis Padres, ya que sin su esfuerzo y sacrificio no hubiera podido llegar a culminar mi carrera.

A mi tía Ligia, que sé que donde esté, se encuentra feliz por este logro obtenido.

A mis hermanas Paola e Isabel, que siempre han estado presentes apoyándome en todo momento.

José Luis

AGRADECIMIENTO

A mis Padres y Hermanas, por ser la motivación para seguir adelante en mi vida tanto profesional, como personal.

A Gabriela por su constante motivación para terminar esta etapa mi vida profesional.

A mis amigos, especialmente a los Payasos, por haberme brindado el apoyo durante mi vida universitaria.

Y finalmente un sincero agradecimiento a las personas que de manera directa o indirecta colaboraron para la elaboración de esta tesis, especialmente al Ing. Carlos Romero y el Ing. Diego Marcillo.

José Luis

INDICE DE CONTENIDOS

LISTADO DE TABLAS

LISTADO DE FIGURAS

NOMENCLATURA

AS: Autonomous System. Sistema Autónomo.

ATM: Asynchronous Transfer Mode. Modo de Transferencia Asíncrono

BGP: Border Gateway Protocol. Protocolo de puerta de frontera.

CE: Customer Equipment. Equipamiento en lado del Cliente

CEF: Cisco Express Forwarding. Envío expreso de Cisco.

E-BGP: Exterior Border Gateway Protocol. BGP para exteriores.

EIGRP: Enhanced Interior Gateway Routing Protocol. IGRP reforzado

EXP: Campo “Experimental” Usado por MPLS para Calidad Servicio.

FEC: Forwarding Equivalence Class. Clase equivalente de envío.

FTP: File Transfer Protocol. Protocolo de transferencia de archivos.

I-BGP: Interior Border Gateway Protocol. BGP para interiores.

IGRP: Interior Gateway Routing Protocol. Protocolo de enrutamiento de interiores

IOS: Internetworking Operative System. Sistema operativo de internetwork

IP: Internet Protocol. Protocolo de Internet.

IPS: Intrusion Prevention System. Sistema de prevención de intrusos

IPX: Internet Protocol Exchange. Intercambio de Protocolo de Internet

IS: Intersystem: Intersystem. Protocolo de enrutamiento inter -sistemas

ISP: Internet Service Provider. Proveedor de servicios de internet.

LAN: Local Area Network. Red de área local.

IPX: Internet Protocol Exchange. Intercambio de Protocolo de Internet

ISP: Internet Service Provider. Proveedor de servicios de internet.

LAN: Local Area Network. Red de área local.

LDP: Label Distribution Protocol. Protocolo de distribución de etiquetas.

LER: Label Edge Router. Ruteador de frontera de etiquetas

LSP: Label Switched Path. Ruta conmutada de etiquetas.

LSR: Label Switch Router. Ruteador conmutador de etiquetas

MAC: Media Access Control. Control de acceso al medio

MPLS: Multiprotocol Label Switching.

OSPF: Only Shortest Path First. Protocolo de enrutamiento de únicamente la ruta más corta primero.

P: Provider. Ruteador del proveedor.

PDU: Protocol Data Unit. Unidad de datos de protocolo.

PE: Provider Edge. Ruteador del frontera al proveedor.

PPP: Point to Point Protocol. Protocolo de enlace punto a punto

QoS: Quality of Service. Calidad de servicio.

RIP: Routing Information Protocol. Protocolo de información de enrutamiento.

RSVP: Resource Reservation Protocol. Protocolo de reserve de recursos.

TCP/IP: Transport Control Protocol / Internet Protocol. Protocolo de control de transporte / Protocolo de internet.

UDP: User Datagram Protocol. Protocolo de datagrama de usuario.

VPN: Virtual Private Network. Red privada virtual.

VRF: VPN Routing and Forwarding Instances. Instancias de enrutamiento y envío VPN

WAN: Wide Area Network. Red de area extendida.

CAPÍTULO I

INTRODUCCIÓN

1.1 Descripción del Proyecto

Este proyecto es un estudio de factibilidad para la migración de redes WAN convencionales a la tecnología MPLS. La Finalidad de este proyecto es la de mostrar las ventajas técnicas y prácticas de la migración a esta tecnología, mediante el análisis de la situación actual de las redes WAN y la investigación de la tecnología MPLS.

Este proyecto mostrará un estudio de cuan factible puede ser la migración de la tecnología usada en las redes WAN convencionales a tecnología MPLS proveyendo sus características y las especificaciones propias de su protocolo.

Se expondrá la funcionalidad del protocolo MPLS, explorando sus características con la meta de proponer en un futuro el cambio de infraestructura para mejorar la situación actual de las redes WAN, esto permitirá la optimización de sus servicios para así facilitar y mejorar la transmisión de datos (voz y video en tiempo real) con garantía de calidad.

También se estudiará la factibilidad económica y la demanda de esta técnica, así como el diseño de una red WAN con MPLS, los requerimientos necesarios y las recomendaciones para la migración de una red WAN convencional a MPLS

1.2 Antecedentes

Actualmente, las redes convencionales WAN con la creciente necesidad de reducir costos, aumentar la productividad, soportar más aplicaciones y elevar la seguridad nace la alternativa de migrar hacia una nueva tecnología como es MPLS.

La adopción de servicios basados en MPLS casi se duplicó entre el 2004 y el 2006. El porcentaje de empresas que aseguraban utilizar tales servicios o tenían intención de hacerlo pasó de un 24% a un 42% en el 2007. En paralelo a esta tendencia, baja drásticamente el interés que despiertan Frame Relay y ATM.

1.3 Justificación e Importancia

Las necesidades de tener equipos interconectados en una amplia área geográfica, requiere que las empresas, empleados, usuarios y clientes se encuentren y mantengan interconectados según el crecimiento de la empresa, inclusive si se establecen en diferentes áreas geográficas.

Para ello cada día se desarrollan nuevas tecnologías, algunas de las cuales ya están al alcance, para ello se ha propuesto la implementación de la tecnología MPLS debido a su creciente popularidad, lo que no deja indiferentes a las empresas gracias a su capacidad para integrar voz, vídeo y datos en una plataforma común con

garantías de calidad de servicio (QoS), también hay que tomar en cuenta las mejoras del rendimiento y la disponibilidad que se obtienen con esta tecnología, así como su soporte de una gran y escalable cantidad de servicios.

El migrar a esta tecnología permitirá crear redes WAN efectivas en costos, rápidas y altamente escalables.

Es necesario entonces para las empresas, disponer de un estudio que permita mostrar las ventajas de la migración de la tecnología actual usada por las redes WAN a MPLS. El presente proyecto tiene por objetivo dar ese soporte mediante un estudio de factibilidad que muestre detalladamente las ventajas de dicha migración.

1.4 Alcance

Se realizará la investigación de esta tecnología con el fin de proveer de un estudio de factibilidad de la migración de redes WAN convencionales a MPLS, a la cual ubicaremos como referencia geográfica dentro de Ecuador.

Exponer la funcionalidad del protocolo, explorando sus características con la meta de proponer que se invierta en un futuro en su infraestructura de esta magnitud que mejore la situación actual de las redes WAN. Esto permitirá la optimización de los servicios de una WAN y así facilitar y mejorar la transmisión de datos (voz y video en tiempo real) con garantía de calidad. Además mostraremos la efectividad en costos y

demanda de esta técnica, así como también su diseño del y los requerimientos necesarios. Para cumplir con los objetivos se pretende utilizar simuladores que permitan determinar el comportamiento que puede tener la red.

CAPÍTULO II

SITUACIÓN ACTUAL DE LAS REDES WAN EN EL ECUADOR

La demanda de servicios basados en conmutación de etiquetas multiprotocolo experimenta un gran crecimiento en relación a los servicios clásicos basados en líneas dedicadas, ATM y Frame Relay. Los costos reducidos y mayor flexibilidad de MPLS favorecen a una tendencia que se impone cada vez más con el paso del tiempo.

Un estudio publicado por la consultora IDC revela que el nivel de implantación de redes MPLS crece de un 17% a 20% anual solo en Europa. Es decir, cada vez las organizaciones abandonan el modelo tradicional de comunicaciones basadas en líneas dedicadas y tecnologías de Circuitos Virtuales, ATM y Frame Relay, para adoptar un modelo de conexión que responde mejor a las perspectivas de servicio que los usuarios poseen en la actualidad. Ya que MPLS (MultiProtocol Label Switching) o Conmutación de Etiquetas Multiprotocolo, posee similares soluciones de comunicación que los Circuitos Virtuales, pero con la diferencia que no posee los inconvenientes que estos traen, ya que brindan los siguientes beneficios:

- Mínimo costo en equipamiento y acceso
- Posibilidades accesibles de video, tolerancia a fallos, VoIP, etc.
- Convenios de nivel de servicios atractivos, reales y sostenibles a buen precio.

- Monitorización para planificación anticipada de necesidades.
- Implantación de VPN más seguras y eficientes para todo tipo de tráfico.
- Direccionamiento privado en todas las ubicaciones.
- Facilidad de implementación y bajos costos de migración

Debido a estas razones MPLS se encuentra implementándose en empresas que hasta algún tiempo se comunicaban exclusivamente con Frame Relay, ATM, etc.

2.1 Análisis de la situación actual de las redes WAN en el Ecuador para determinar una futura migración.

Debido al gran crecimiento de los volúmenes de información que se manejan en una empresa gracias al avance de la tecnología, la mayoría de organizaciones han hecho de sus redes de información un conjunto de redes híbridas, lo cual acarrea una serie de problemas dentro de dicha organización, como por ejemplo:

- Inconvenientes con la disponibilidad de la información.
- Problemas de conectividad.
- Problemas de velocidad de transferencia.

Por lo cual, actualmente, para estar dentro de la competencia del mercado global, una organización no puede prescindir ni un instante de la información vital para realizar su trabajo, siendo el uso de la tecnología una necesidad real, haciendo a esta, parte importante de la misma organización y de su modelo de negocio.

Para lo cual surgen nuevas necesidades tecnológicas para una organización, las cuales son:

- Mejorar el desempeño en la manipulación de la información y la seguridad de la misma.
- Asegurar la confidencialidad, integridad y disponibilidad de la información.
- Optimizar la administración de la información.

Dichos puntos pueden ser logrados con la aplicación de una tecnología que sea confiable y segura como lo es MPLS dentro de organizaciones que busquen el mejoramiento tecnológico como necesidad para desarrollar un mejor desempeño y por consiguiente una mejor productividad.

En el Ecuador, actualmente cada vez son más las empresas que se encuentran incorporando MPLS dentro de su organización, poniendo de lado tecnologías antiguas como ATM, Frame Relay, etc., que en la actualidad, aunque válidas y vigentes no aportan nuevas ventajas, ni solucionan problemas que se presentan en la situación actual de las tecnologías de la información, ni permiten aprovechar nuevos recursos tecnológicos.

Algunas empresas que ya migraron y usan MPLS en el Ecuador son:

- Global Crossing Ecuador que usa MPLS para transporte de Internet y Datos.
- Telconet S.A. Ecuador utiliza MPLS en su CORE para transporte de Datos e Internet.
- Porta - Conecel Ecuador actualmente también utiliza MPLS en su CORE para transmisión de Datos e Internet.
- Telefónica Ecuador que utiliza MPLS en su CORE para transporte de Datos e Internet.

- Andinatel – Actual CNT usa MPLS en su CORE para transportar Internet y Datos.

Debido a la importancia de esta migración tecnológica surge la necesidad de realizar un análisis de factibilidad con la finalidad de tener un conocimiento real de los costos técnicos y económicos, así como las ventajas operacionales de migrar de tecnologías WAN actuales a una futura red sobre MPLS.

Con ello, la organización aumentará la efectividad de su red de información, mejorando su eficiencia y productividad.

Pero la migración tecnológica también trae como consecuencia problemas dentro de la organización, tales como:

- Resistencia al cambio de tecnología y errores en el uso de la misma.
- Mala definición de los requerimientos necesarios para la migración por falta de comunicación, coordinación o de compromiso de los involucrados en el análisis.
- Restricciones físicas a lugares necesarios para la configuración o cambio de equipos
- Problemas de colaboración de empleados de la organización.

Obstáculos que pueden ser superados dentro de la implementación tecnológica con una migración transparente para que el impacto hacia el usuario final sea mínimo así como también detallar el uso adecuado de la nueva tecnología, sus ventajas y limitaciones.

Al analizar la situación en la que actualmente funcionan las redes WAN, surgen también problemas técnicos que se deben tomar de en cuenta para el diseño y posterior implementación de una WAN de manera eficaz. Estos son:

- **Latencia:** Considerar si las demoras pueden representar un problema para el tráfico en tiempo real.
- **Infraestructura:** Analizar qué tipo de infraestructura: pública o privada se debe usar, según las funciones de la organización.
- **Confiabilidad:** Ya que la organización y sus sucursales especialmente dependen de la WAN, la confiabilidad de esta es fundamental.
- **Seguridad:** Se debe tomar en cuenta la protección contra las posibles amenazas de seguridad que surjan a través de la WAN.
- **Confidencialidad:** Es fundamental la confidencialidad, debido a la importancia de la información de la organización que viaja a través de la WAN.
- **Calidad de servicio:** Hay que tomar en cuenta que la calidad de servicio de extremo a extremo puede ser difícil de obtener, y más aún si se la hace a través de internet.

2.2 Estudio de la demanda de servicio.

Debido al progresivo aumento de demanda de conectividad y comunicación, por causa del aparecimiento de nuevas aplicaciones, que necesitan cada vez mayores anchos de banda para trabajar y la mayor exigencia respecto a la calidad de servicio, ha obligado a que las empresas portadoras busquen migrar sus redes tradicionales a tecnologías de nueva generación que puedan flexibilizar las comunicaciones.

La mayoría de estas empresas portadoras ya se encuentran operativas con nuevas tecnologías, especialmente a MPLS, prestando actualmente servicios adicionales (VoIP, VPN, etc.).

La demanda de servicios combinados que se dan por internet aún es muy baja, respecto a los servicios tradicionales, pero está en una tasa de crecimiento muy alta. Por ejemplo podemos observar en la figura 2.1 que actualmente los servicios de Internet y Telefonía fija duplican a los abonados que poseen únicamente televisión por cable, algo que hace unos pocos años parecía no tan realista.

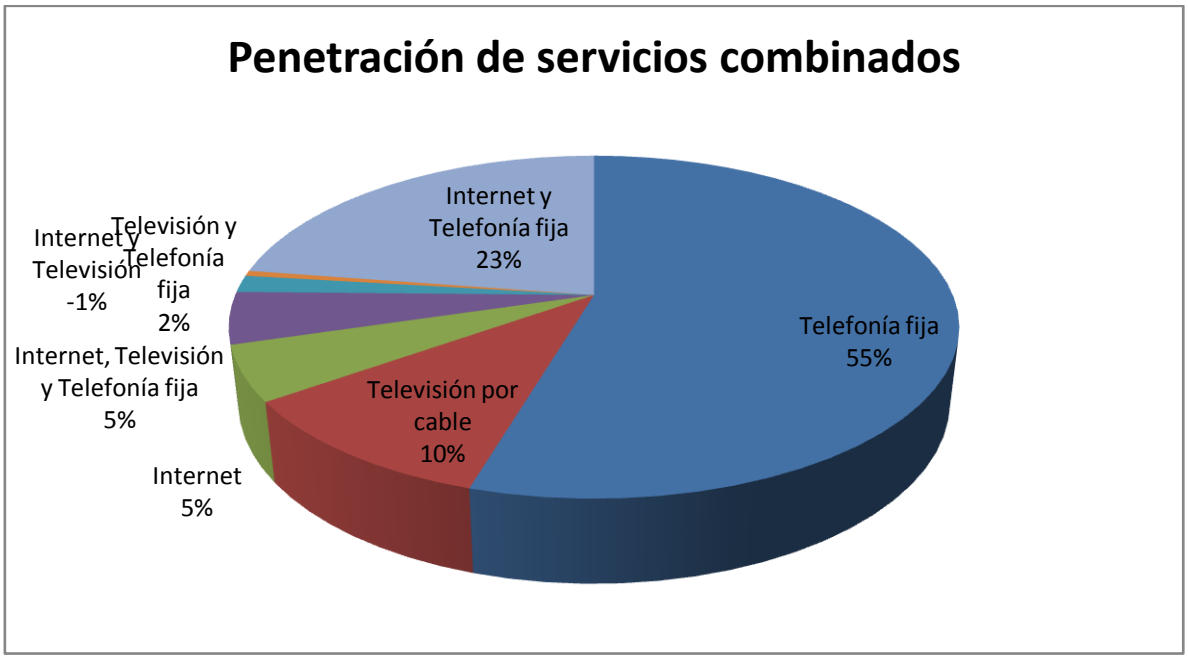


Figura 2. 1: Penetración de servicios combinados

Así mismo, ha aumentado la demanda de redes privadas, como muestra la figura 2.2 de los Permisos otorgaros a redes privadas por la Senatel y Conatel, solo en el mes de enero del 2009 se supera a los permisos concedidos en todo el año 2008, sumando de enero a mayo del 2009 un total de 802 permisos concedidos para redes privadas

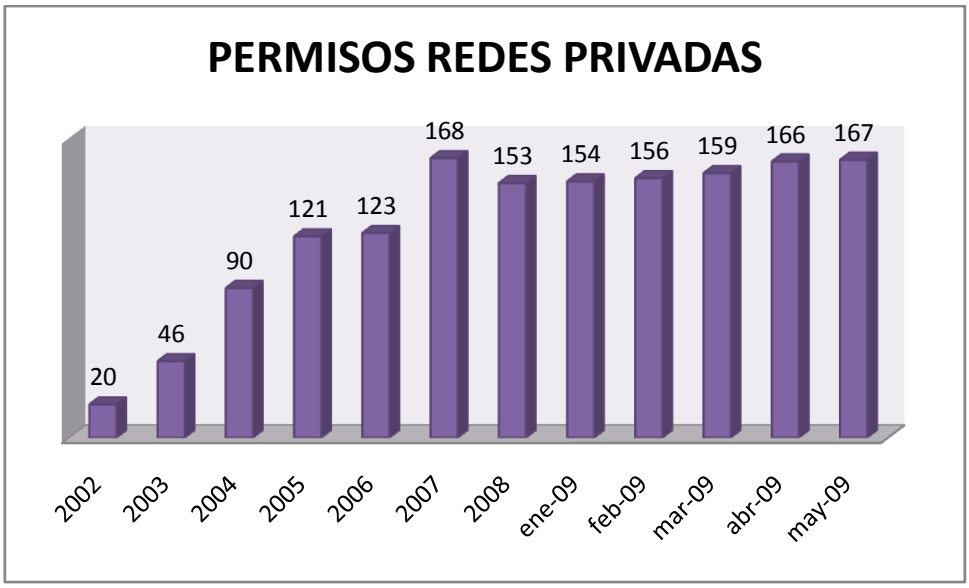


Figura 2. 2: Permisos de Redes Privadas

Tan solo en el año 2009 los usuarios de Banda Ancha aumentaron en una relación de más de 10 a 1 desde diciembre del 2008 hasta diciembre del 2009. Este crecimiento de usuarios obliga a las empresas proveedoras a aumentar su canal de ancho de banda para poder brindar un servicio satisfactorio al creciente número de usuarios, para lo cual se adopta implementar tecnologías de nueva generación como lo es MPLS.

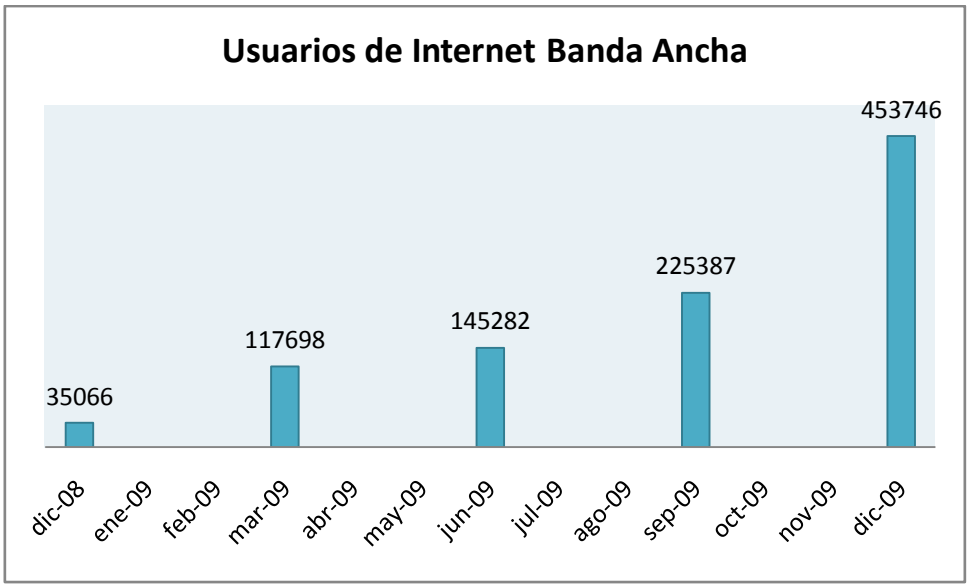


Figura 2. 3: Usuarios de Internet Banda Ancha

Las empresas que operan actualmente como portadoras a nivel nacional según la SENATEL Y CONATEL son:

1. Global Crossing Comunicaciones Ecuador S.A.
2. Suramericana de Telecomunicaciones Suratel
3. Conecel S.A.
4. Quicksat S.A.
5. Megadatos
6. Corporación Nacional de Telecomunicaciones CNT S.A.
7. Telconet S.A.
8. Otecel S.A.
9. Grupo Bravco Cía. Ltda.
10. Negocios y Telefonía Nedetel S.A.
11. Servicios de Telecomunicaciones Setel S.A.

12. Ecuadortelecom S.A.
13. Gilauco S.A.
14. Transnexa S.A.
15. Transelectric S.A.
16. Etapatelecom S.A.
17. Teleholding S.A.
18. Puntonet S.A.
19. Telecsa S.A.
20. Importadora El Rosado Cía. Ltda.
21. Zenix S.A. Servicios de Telecomunicaciones Satelital
22. Empresa Eléctrica Regional Centro Sur C.A.

Según la información recolectada en la presente investigación, actualmente más del 59% de las portadoras se encuentran operando con al menos un dominio MPLS, un 14% más se encuentra superando la etapa de proyecto o prueba, el 23% implementará en un futuro no tan distante MPLS como solución a su red, mientras que el 4% prefiere aun seguir investigando antes de tomar una decisión al respecto.

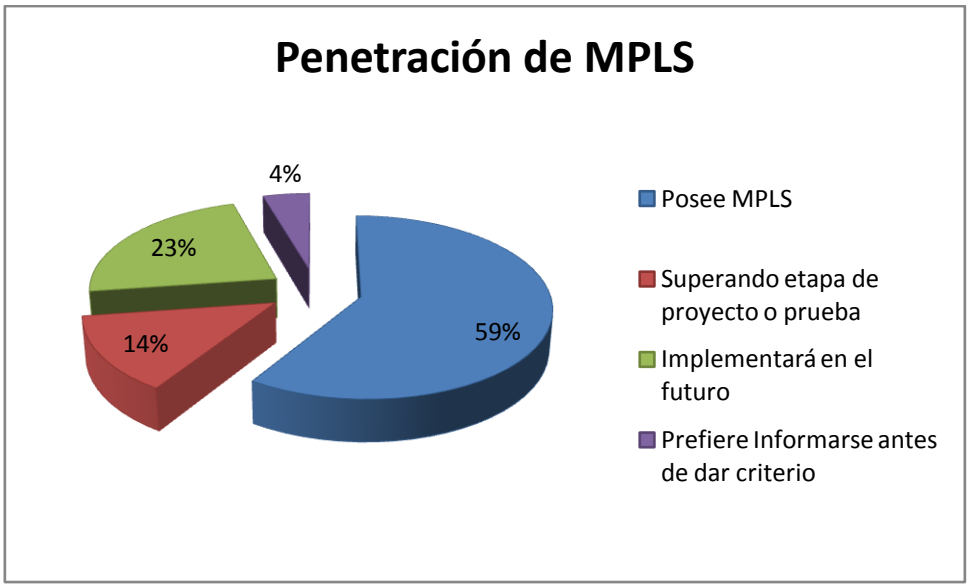


Figura 2. 4: Penetración de MPLS

La información completa respecto a la penetración de mercado de MPLS no está presente en la SENATEL ni en el CONATEL, debido a que las estadísticas se manejan de manera muy generalizada, además que se me indicó que en dichas instituciones la publicación de la información se realiza de manera lenta e incompleta, debido a que la mayoría de operadores entregan los datos de manera incompleta y retrasada, y por esta razón no hay información disponible que corresponde a las tecnologías que están implementadas en los enlaces de los portadores actualmente, ni de la penetración oficial de MPLS en el Ecuador, por lo que se optó por consultar a las empresas que operan actualmente como portadoras a nivel nacional registradas en la Senatel y en el Conatel, de las cuales se ha obtenido el material y la información necesaria para realizar el presente estudio de factibilidad.

2.3 Establecimiento de los requerimientos para una técnica de encaminamiento segura y eficiente.

Una técnica de encaminamiento de datos es casi tan importante como la estructura física de la red, debido a que las comunicaciones deben funcionar de la manera más eficiente, aprovechando todos los recursos disponibles para brindar un servicio de calidad a la organización.

Para ello, se han desarrollado varias técnicas de encaminamiento (OSPF, RIP, Frame Relay, ATM, etc.) que se analizarán detalladamente más adelante, las cuales se encargan de transportar los datos a lo largo de una red WAN, usando diferentes métodos para elegir la ruta a usarse mediante las diferentes métricas que cada técnica usa para este fin.

Al escoger la mejor técnica de comunicación para usarse hay que, a más de tomar en cuenta los aspectos anteriores, analizar el tráfico y las condiciones del flujo de tráfico que existe en una WAN.

La siguiente tabla muestra los tipos de tráfico y los diferentes requerimientos de ancho de banda, latencia y fluctuación que se transportan en una WAN.

Tipo de tráfico	Latencia	Fluctuación de fase	Ancho de banda
Voz	Bajo	Bajo	Medio
Datos de transacción	Medio	Medio	Medio
Mensajería (email)	Alto	Alto	Alto
Transferencia de archivos	Alto	Alto	Alto
Datos en lote	Alto	Alto	Alto
Administración de red	Alto	Alto	Bajo
Videoconferencia	Bajo	Bajo	Alto

Tabla 2. 1: Tabla de Consideraciones sobre el tráfico de WAN

Se debe también considerar las características del tráfico específicas para cada LAN conectada a la WAN con el fin de establecer las condiciones del flujo de tráfico y la temporización de un enlace WAN. Para lo cual se debe evaluar las necesidades de los usuarios de la red.

Para ello consideramos las siguientes características de tráfico y las acciones a tomarse:

- **Conectividad y flujos de volumen:** Se debe tomar en cuenta, hacia donde fluye el tráfico y la cantidad del mismo.
- **Datos de cliente/servidor:** Determinar la clase de tráfico que fluye entre el cliente y el servidor.
- **Tolerancia a la latencia, incluyendo la longitud y la variabilidad:** Establecer si los usuarios pueden tolerar retrasos, la cantidad y frecuencia de los mismos.

- **Tolerancia a la disponibilidad de la red:** Establecer la importancia de la red para los usuarios de las redes LAN, y si pueden tolerar interrupciones de WAN o si detendrían su trabajo por completo.
- **Tolerancia al porcentaje de errores:** Analizar si el tráfico presenta mucho ruido.
- **Prioridad:** Determinar la prioridad que posee determinado tráfico frente a otro.
- **Tipo de protocolo:** Reconocer los tipos de protocolos que están operando al interior de la red.
- **Longitud promedio de los paquetes:** Examinar el tamaño promedio de los paquetes que se transmiten por la red.

Debido a esto, se propone usar la tecnología MPLS como una solución segura y eficiente de encaminamiento respecto a otras soluciones WAN usadas actualmente por las ventajas que esta tecnología presta, tal como se conocerá más delante en este Estudio de Factibilidad.

Se propone a MPLS como una tecnología eficaz y segura debido a que está diseñado con las ventajas que presentan las anteriores tecnologías

Para ello, comparamos brevemente MPLS con tecnologías como IP y ATM.

	IP	ATM	MPLS
Operación (Modelo OSI)	Capa 3	Capa 2	Capa 2 y 3
Interoperabilidad con otras tecnologías	No	No	Si (ATM, Frame Relay, IP, Otros)

Redes Virtuales Privadas VPN	No	Si	SI
Topología Virtual	Multipunto	Punto a Punto	Punto a Punto y Multipunto
Interfaces	Ethernet / IP	SDH / ATM	Ethernet/IP y SDH/ATM
Soporte	Si	No	Si
Orientado a la conexión	No	Si	Si
Calidad de Servicio QoS	No	Si	Si
Ingeniería de Tráfico	No	No	Si
Escalabilidad	Si	No	Si

Tabla 2. 2: Tabla comparativa entre MPLS, IP y ATM

Como se ve en la tabla anterior, se muestra memorablemente las ventajas que ejerce esta tecnología de encaminamiento frente a otras, las cuales se detallarán más adelante en este documento.

CAPÍTULO III

MARCO TEÓRICO

3.1 Definiciones Básicas de Redes

3.1.1 Comunicación e Intercambio de mensajes

Para poder comunicarse en forma confiable a diversos lugares actualmente en el mundo se usan todos los días un sin número de redes interconectadas, las cuales varían en tamaño y capacidad, pero todas constan de los mismos elementos básicos q son:

- Las reglas y acuerdos para regularizar cómo se envían, re direccionan, reciben e interpretan los mensajes,
- Los mensajes o unidades de información que viajan de un dispositivo a otro,
- La forma de interconectar esos dispositivos, es decir, un medio que puede transportar los mensajes de un dispositivo a otro
- Los dispositivos de la red que intercambian mensajes entre sí.

La estandarización permite que dispositivos fabricados por diferentes marcas funcionen de manera transparente y sin problemas.

3.1.2 Elementos de una red

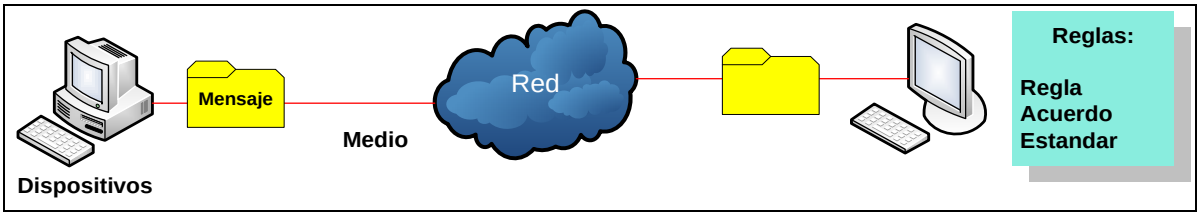


Figura 3. 1: Elementos básicos de una red

Los elementos de una red se conforman de: dispositivos de red, mensajes, medios, y reglas.

- Los mensajes son los datos a intercambiarse, como datagramas, páginas Web, llamadas, entre otros tipos de comunicaciones.

- Los medios son la forma de interconexión entre los dispositivos, la cual puede ser alambicas que transmiten impulsos eléctricos (cable UTP, cable coaxial, etc.) o impulsos de luz (Fibra óptica), o inalámbricas en las cuales el medio es la atmósfera de la tierra o el espacio y las señales son microondas. Por consiguiente un mensaje para llegar de extremo a extremo puede atravesar diferentes medios en su trayecto.

- Las reglas son los protocolos que se usan en los dispositivos de red para comunicarse entre sí, con los cuales se especifican los mecanismos de direccionamiento, enrutamiento y formateo para garantizar que los mensajes sean entregados al receptor correctamente, como por ejemplo TCP/IP.

- Los dispositivos finales son donde por lo general se originan y terminan los mensajes, estos dispositivos pueden ser computadores, servidores, teléfonos IP, cámaras de seguridad, dispositivos móviles, etc. Estos dispositivos constituyen la interfaz entre la red humana y la red de comunicación subyacente.

- Los dispositivos intermedios proporcionan la conectividad y garantizan que los datos fluyan a través de la red. Estos conectan los hosts individuales a la red y pueden conectar redes individuales entre sí para formar una internetwork. Estos dispositivos pueden ser: dispositivos de internetworking (Routers), servidores de comunicación y módems, y dispositivos de seguridad (firewalls).

3.1.3 Tipos de Redes:

Las infraestructuras de red pueden variar en gran medida en términos del tamaño del área cubierta, la cantidad de usuarios conectados, y la cantidad y tipos de servicios disponibles. Estas redes pueden ser: Locales (LAN), Metropolitanas (MAN) y de Área Extendida (WAN).

3.1.3.1 LAN: (Local Area Network) Es una red individual que cubre una única área geográfica y proporciona servicios y aplicaciones a personas dentro de una estructura organizacional común, como una empresa, un campus o una región. Por lo general está administrada por una única organización. En este nivel de red se implementa el control administrativo que rige las políticas de seguridad y el control de acceso.

3.1.3.2 MAN: (Metropolitan Area Network), es una red optimizada para un área más grande que una LAN y menor que una WAN. Por ejemplo, distintos campus.

3.1.3.3 WAN: (Wide Area Network), son redes que cubren una amplia área geográfica, como una región o provincia, incluso entre países. Las WAN utilizan dispositivos de red diseñados específicamente para realizar las interconexiones entre las LAN. Dada la importancia de estos dispositivos para la red, la configuración, instalación y mantenimiento de éstos son aptitudes complementarias de la función de una red de la organización.

3.1.4 Topologías

Las redes están diseñadas con diferentes topologías o rutas físicas conectando los equipos terminales. Tres topologías han sido las más usadas:

3.1.4.1 Bus: Los elementos que constituyen la red se disponen linealmente, es decir, en serie y conectados por medio de un cable que es el bus.

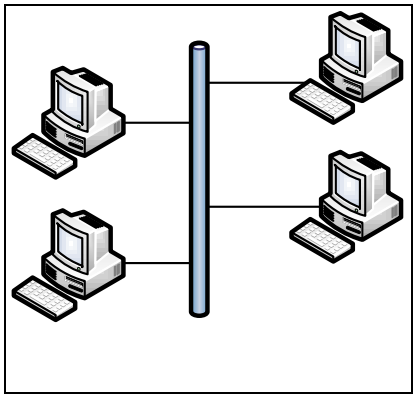


Figura 3. 2: Topología de bus

3.1.4.2 Anillo: Los equipos de la red se disponen en un anillo cerrado, conectados a él mediante enlaces punto a punto. La información describe una trayectoria circular en una única dirección y el equipo principal es quien

gestiona conflictos entre equipos al evitar la colisión de tramas de información.

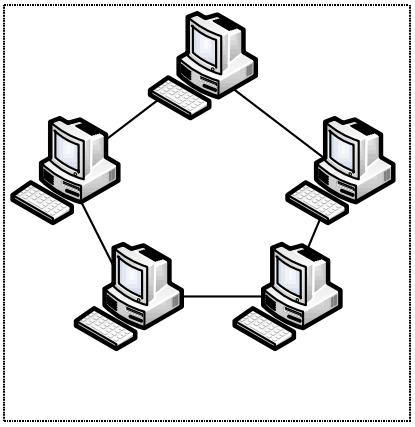


Figura 3. 3: Topología anillo

3.1.4.3 Estrella: Todos los elementos de la red se encuentran conectados directamente mediante un enlace punto a punto al equipo central de la red (concentrador), quien se encarga de gestionar las transmisiones de información por toda la estrella.

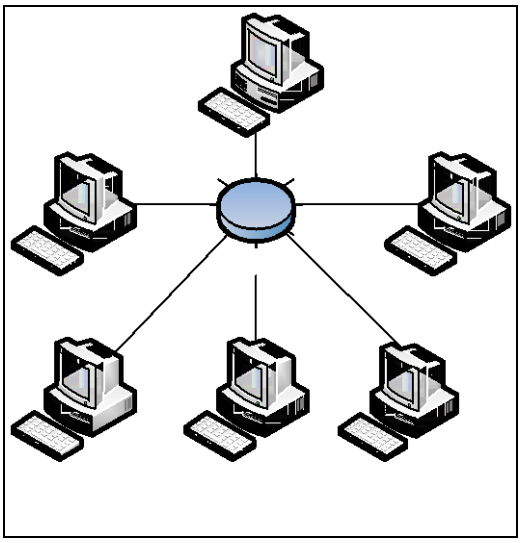


Figura 3. 4: Topología estrella

3.1.5 Dirección MAC

Es una dirección individual, cada dispositivo tiene su propia dirección MAC determinada ya por el fabricante. Para acceder al medio es necesario contar con una manera de identificar al emisor de la información. La dirección MAC es un identificador de 48 bits (6 bytes) que corresponde de forma única a una tarjeta o interfaz de red. Según el estándar IEEE 802 se presenta como seis grupos de dos dígitos hexadecimales, separados por dos puntos (:) o guiones (-), por ejemplo: 01:23:45:67:89:ab ó 01-23-45-67-89-ab

Los primeros tres bytes de la dirección MAC indican el fabricante del producto.

3.1.6 Dirección IP

Una dirección de protocolo de Internet (IP), es un identificador numérico lógico, el cual es asignado a dispositivos que conforman una red de computadores que usan el protocolo de Internet para comunicarse ente nodos.

El esquema de direccionamiento IP se basa en el uso de cuatro octetos separados por un punto. Se usa números binarios desplegados en formato decimal para un mejor manejo. Por ejemplo: 192.168.1.20 (IP v4) ó 2001:db3:0:1231:0:234:1:1 (IP v6)

En IP v4 se usa direcciones de 32 bits, dividida en 4 bytes, con un espacio posible de direcciones de 2^{32}. Existen direcciones reservadas para propósitos especiales, tales como redes privadas o de multicast.

IP v6 surge ante la saturación de direccionamiento IP, ya que empieza a haber más demanda de direcciones IP v4 en dispositivos móviles, celulares, automóviles, etc. Una dirección IP v6 está compuesta por 8 segmentos de 2 bytes cada uno, sumando un total de 128 bits, el equivalente a unos 3.4x1038 hosts direccionables. Su

representación suele ser hexadecimal y para la separación de cada par de octetos se emplean dos puntos ":". Un bloque abarca desde 0000 hasta FFFF.

3.1.7 Descripción Modelo OSI

El modelo de referencia de Interconexión de Sistemas Abiertos (OSI, Open System Interconnection) lanzado en 1984 fue el modelo de red descriptivo creado por ISO (International Organization for Standardization); esto es, un marco de referencia para la definición de arquitecturas de interconexión de sistemas de comunicaciones. Nace para proporcionar una referencia abstracta sobre el cual crear una suite de protocolos de sistemas abiertos. La visión era que este conjunto de protocolos se utilizara para desarrollar una red internacional que no dependiera de sistemas propietarios, usada como modelo de comunicaciones en capas para la definición de arquitecturas de interconexión de sistemas de comunicaciones, por lo que este modelo está compuesto de siete capas o niveles:

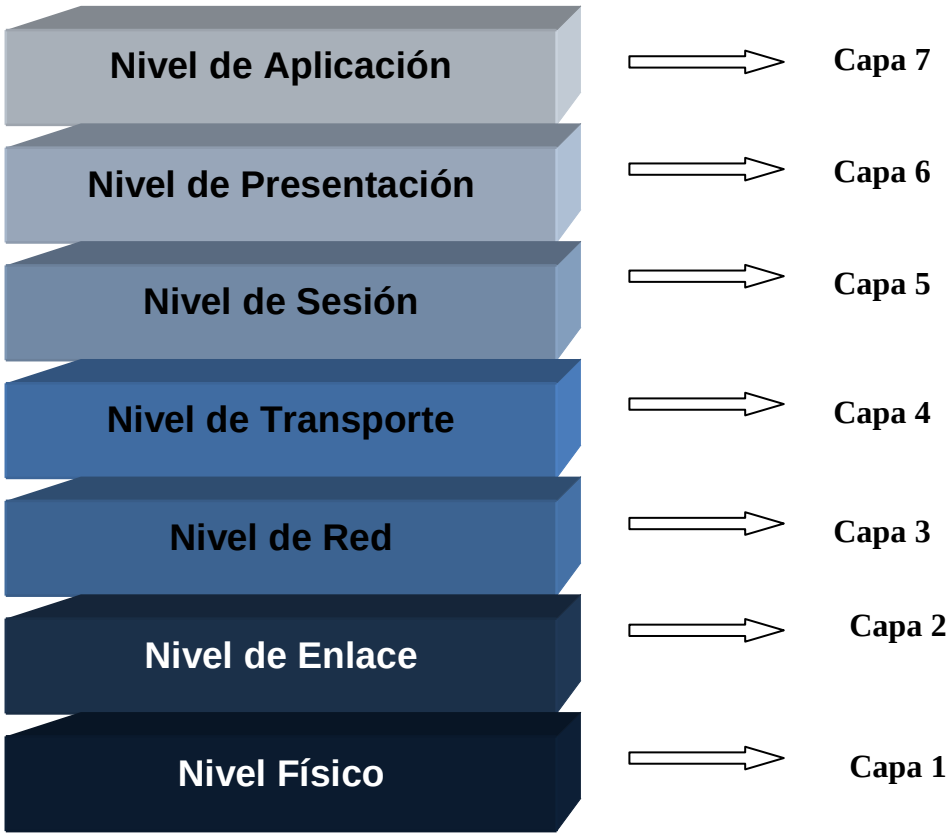


Figura 3. 5: Modelo OSI

3.1.8 Nivel de Aplicación (capa 7): Permite a las aplicaciones acceder a los servicios de las demás capas, define los protocolos que utilizan las aplicaciones para intercambiar datos como correo electrónico (POP y SMTP), gestores de bases de datos y servidor de ficheros (FTP).

3.1.9 Nivel de Presentación (capa 6): Se encarga de la representación de la información de manera reconocible, también permite cifrar los datos y comprimirlos. En otras palabras es un traductor.

3.1.10 Nivel de Sesión (capa 5): Establece, gestiona y finaliza las conexiones entre usuarios finales. También ofrece servicios cruciales para la comunicación como: Control de la sesión, Control de la concurrencia de las comunicaciones, y Mantenimiento de puntos de verificación (Checkpoints). En conclusión esta capa es la que se encarga de mantener el enlace entre los dos computadores que estén trasmitiendo datos cualesquiera.

3.1.11 Nivel de Transporte (capa 4): Acepta los datos enviados por las capas superiores y los pasa a la capa de red, además segmenta los datos de ser necesario. Es la capa encargada de efectuar el transporte de los datos (que se encuentran dentro del paquete) de la máquina origen a la de destino, independizándolo del tipo de red física que se esté utilizando. La PDU (Protocol Data Units) de la capa 4 se llama Segmento.

3.1.12 Nivel de Red (capa 3): Provee los medios para transferir secuencias de datos entre una fuente a un destino a través de una o más redes. La capa Red, se utiliza casi universalmente para analizar y documentar el rango de los procesos que se producen en todas las redes de datos para direccionar y enrutar mensajes a través de una internetwork. El protocolo de capa de Red más significativo en esta capa es el Protocolo de Internet (IP). El enrutamiento de IP de Capa 3 no garantiza una entrega confiable ni establece una conexión antes de transmitir los datos. Esta comunicación no es confiable sin conexión, es rápida y flexible, pero las capas superiores deben proveer mecanismos para garantizar la entrega de datos si se necesita. La función de la capa de

Red es llevar datos desde un host a otro sin tener en cuenta el tipo de datos. Los datos están encapsulados en un paquete. El encabezado del paquete tiene campos que incluyen la dirección de destino del paquete.

3.1.13 Nivel de Enlace de Datos (capa 2): Se encarga de la transmisión de datos entre entidades de red y detección de posibles errores. La capa de enlace de datos se ocupa del direccionamiento físico, de la topología de la red, del acceso a la red, de la notificación de errores, de la distribución ordenada de tramas y del control del flujo.

En esta capa realizan su función los Switches. La capa de enlace de datos OSI prepara los paquetes de capa de red para ser colocados en el medio físico que transporta los datos. El amplio intervalo de medios de comunicación requiere, un amplio intervalo de protocolos de enlace de datos para controlar el acceso a los datos de estos medios. La topología lógica y el medio físico ayudan a determinar el método de acceso al medio. La capa de enlace de datos prepara los datos para ser colocados en el medio encapsulando el paquete de la Capa 3 en una trama. Una trama tiene un encabezado y una información final que incluye las direcciones del enlace de datos de origen y de destino, calidad de servicio, tipo de protocolo y valores de secuencia de verificación de tramas.

3.1.14 Nivel Físico (capa 1): Es la capa responsable de la interconexión física de los dispositivos. Los estándares de esta capa definen las características de la

representación en frecuencias eléctricas, ópticas y radiofrecuencias de los bits que componen las tramas de la capa de Enlace de datos que se transmiten. Los valores de bit pueden representarse mediante impulsos electrónicos, impulsos de luz o cambios en las ondas de radio. Los protocolos de la capa física codifican los bits para la transmisión y los decodifican en el destino. Los estándares de esta capa también son responsables de describir las características físicas, mecánicas y eléctricas de los conectores y medios físicos que interconectan los dispositivos de red. Los diversos protocolos de la capa física y los medios poseen distintas capacidades para transportar datos. El ancho de banda de datos sin procesar es el límite máximo teórico de transmisión de bits. El rendimiento y la capacidad de transferencia útil son diferentes medidas de una transferencia de datos observada durante un período de tiempo determinado.

3.2 Enrutamiento

El enrutamiento o encaminamiento es la función de buscar el mejor camino de todos los disponibles en una red de paquetes en las que sus topologías posean una gran conectividad.

Debe entenderse como “Mejor Ruta” a aquella ruta que presenta menor retardo medio de tránsito, ofrece altas cadencias efectivas independientemente del retardo medio de tránsito, mantiene acotado el retardo entre pares de nodos de la red y permite ofrecer el menor costo.

Elegir el camino más corto es el mejor criterio, es decir, escoger una ruta que pase por el menor número de nodos.

El protocolo de enrutamiento tiene como meta vital determinar las mejores rutas para llegar a una red remota determinada. Dicho protocolo genera una métrica para cada ruta, algunos de los protocolos se pueden basar en varias métricas combinadas en un solo valor métrico.

3.2.1 Métrica

La elección de la “Mejor Ruta” involucra la evaluación de varias rutas hacia la misma red de destino y la selección del camino más óptimo o el más corto para llegar a dicha red.

El protocolo de enrutamiento se encarga de determinar la mejor ruta mediante el valor de la métrica para establecer la distancia para llegar a esa red.

La métrica es un valor cuantitativo usado para medir la distancia hacia una determinada ruta, la cual mientras sea la más baja es la mejor métrica.

Las métricas usadas en enrutamiento IP contienen:

- Ancho de Banda: Mientras mayor sea la banda tendrá más preferencia.
- Conteo de Saltos: cuenta la cantidad de Routers que tiene que cruzar un paquete.
- Retardo: Es el tiempo que le toma cruzar un camino a un paquete
- Carga: Es la utilización en del tráfico en un enlace.
- Costo: El sistema o el administrador califica una ruta, ya sea en base a una métrica, una combinación de métricas o en base a políticas.

- Confiabilidad: Es la evaluación de la probabilidad de que un enlace falle en base al conteo de errores

3.2.2 Encaminamiento en redes de circuitos virtuales y de datagramas

La función de encaminamiento establece una ruta que no cambia mientras el tiempo de vida de un circuito virtual funcione en una red de conmutación de paquetes, dicho encaminamiento se decide por sesión. Mientras que, cuando una red que no tiene el compromiso de garantizar ordenadamente la entrega de paquetes, es decir, cuando funciona en modo datagrama, cambian el criterio de encaminamiento descubriendo una nueva “Mejor Ruta”

3.2.2.1 Clasificación de los Métodos de Encaminamiento

Existen dos criterios para clasificar los métodos de encaminamiento:

3.2.2.1.1 En función de **donde** se decide encaminar:

3.2.2.1.1.1 Fijado en el origen: Los que fijan la ruta que van a seguir cada paquete son los sistemas finales, para eso cada paquete tiene un campo RI (Routing Information) para determinar la ruta y los nodos en cambio se dedican a reenviar los paquetes por las rutas que ya son especificadas sin tener que consultar tablas de encaminamiento en nodos intermedios, solo en los sistemas finales.

3.2.2.1.1.2 Salto a salto: Los nodos conocen solo el siguiente salto a realizar una vez que conocen el destino.

3.2.2.1.2 En función de la **adaptabilidad**:

3.2.2.1.2.1 Estáticos o No Adaptables: En los nodos, las tablas de enrutamiento se configuran manualmente, permaneciendo inalterables hasta que no se vuelva a modificarlas, por lo que no toman en cuenta el estado de la red para encaminar, lógicamente, por este motivo carece de adaptabilidad. Son rápidos, de diseño simple, rígidos, pero los peores al momento de tomar decisiones. Es óptimo para topologías que solo tienen una posibilidad de encaminamiento, por ejemplo la topología en estrella.

3.2.2.1.2.2 Dinámicos o Adaptables: Estos algoritmos no son rígidos, son de diseño complejo, las decisiones tomadas son mucho mejores que las tomadas por los métodos estáticos, pero consumen muchos recursos, por lo que la convergencia es muy alta. Toleran cambios en las redes como fallas en la topología, variaciones de tráfico o aumento del retardo. Este se clasifica en tres clases:

3.2.2.1.2.3 Centralizado: Todos los nodos son iguales salvo un nodo central, el cual recibe la información de control y los nodos acerca de sus vecinos para armar calculando la tabla de encaminamiento, la desventaja de este es que consume muchos recursos, y además, se necesitan rutas

alternativas para comunicarse con el nodo central, más aún si este se cae.

3.2.2.1.2.4 **Aislado**: Cuando un nodo recibe un paquete, lo reenvía a otros nodos por todos sus enlaces, con excepción por el que llegó. Este método se adapta muy sencillamente al cambio de la red, no toma en cuenta la información de otros nodos al momento de encaminar. Son útiles para enviar información de emergencia.

3.2.2.1.2.5 **Distribuido**: En este todos los nodos son iguales, así que todos calculan su tabla de encaminamiento a partir de la información de control que reciben, ya que todos los nodos ejecutan el mismo algoritmo de encaminamiento. Son los más usados ya que cuando ocurren cambios en la red, su adaptación es óptima. Hay dos procedimientos distribuidos que son estado enlace y vector distancia.

3.2.2.1.2.5.1 **Vector distancia**: Las rutas se publican como vectores de dirección y distancia. La primera se define como el vecino más próximo, y la distancia como el conteo de los saltos. Usan el algoritmo BellmanFord al calcular la “Mejor Ruta”. Al enviar un nodo la información de su tabla, los otros nodos comparan y actualizan la información de sus tablas de encaminamiento. Funcionan mejor cuando la red es simple y plana. Por ejemplo los algoritmos RIP v1 y v2, IGRP e EIGRP.

3.2.2.1.2.5.1.1 RIP (Routing Information Protocol): Es un protocolo de Vector Distancia, utiliza como métrica para seleccionar la mejor ruta el conteo de saltos, el cual no puede ser mayor a 15, si llega a 16 no proporciona una ruta para esa red, cada 30 segundos envía actualizaciones.

3.2.2.1.2.5.1.2 IGRP (Interior Gateway Routing Protocol): Desarrollado por CISCO, crea una métrica compuesta por el ancho de banda, la carga, el retardo y la confiabilidad, para calcular la mejor ruta; actualiza cada 90 segundos las tablas de enrutamiento. A este protocolo se lo considera obsoleto, ya que es antecesor de EIGRP.

3.2.2.1.2.5.1.3 EIGRP (Enhanced IGRP): También fue planteado por CISCO, realizan balanceo de carga con distinto costo para calcular la mejor ruta al usar el algoritmo DUAL (algoritmo de actualización por difusión), las actualizaciones solo se envían cuando existe un cambio en la topología.

3.3.2.1.5.2 Estado Enlace: Crean una vista completa de la topología de la red reuniendo la información publicada por los nodos aledaños, por lo que dichos nodos crean un “mapa” de la red para determinar la mejor ruta

aplicando el algoritmo de coste mínimo o algoritmo de Dijkstra. Por ejemplo los protocolos de estado de enlace OSPF e IS-IS.

3.3.2.1.5.2.1 OSPF(Open Shortest Path First): Determina la mejor ruta aplicando el algoritmo de coste mínimo o algoritmo de Dijkstra, opera con encriptación MD5 para autentificar a sus puntos antes de actualizar las rutas, descompone una red mayor en redes más pequeñas, partiendo desde un área central especial o backbone, conectando las otras a esta área.

3.3.2.1.5.2.2 IS-IS (Intermediate System to Intermediate System): Encuentra el camino más corto mediante el algoritmo SPF (Shortest Path First), es un protocolo OSI, pero puede encaminar paquetes IP y CLNP (ConnectionLess Network Protocol), no encapsula los paquetes, permite interconectar redes con protocolos de encaminamiento distintos, permite la comunicación entre sistemas intermedios.

3.3 Redes WAN

3.3.1 Concepto de red WAN

Una WAN es una red de comunicación de datos que puede operar mucho más lejos que el alcance geográfico de una red LAN.

Una WAN hace posible la transmisión de datos a través de distancias geográficas mayores. Para conectar los sitios de una organización entre sí con sitios de otras organizaciones, con usuarios remotos y servicios externos, se utilizan infraestructura

suministrada por un proveedor de servicios, o también llamado portadora, los cuales pueden ser empresas proveedoras de servicios de cable o de telefonía, sistemas satelitales y proveedores de red. También se usan conexiones seriales de distinto tipo para dar acceso al ancho de banda.

Una WAN se usa con frecuencia para compartir datos con una sede central y comunicarse con sus sucursales y oficinas regionales entre sí. Es decir, se las usa para compartir información con otros lugares que se encuentran a amplias distancias.

3.3.2 Opciones de conexión WAN

3.3.2.1 Privada:

Son estructuras de red de uso exclusivo, por lo general se debe pagar para poder usarlas.

3.3.2.1.1 **Dedicada**:

Por lo general se utilizan líneas punto a punto que poseen diversas capacidades, teniendo solamente las limitaciones que dan las instalaciones físicas y los costos dispuestos a pagar por los usuarios. Un enlace punto a punto brinda rutas de comunicación WAN previamente establecidas desde el cliente, a través de la red del proveedor hasta el destino remoto, estas líneas también son llamadas líneas arrendadas.

3.3.2.1.1.1 Líneas Arrendadas:

Se usan enlaces punto a punto cuando se necesitan conexiones dedicadas permanentes, por lo general se alquilan a una operadora.

Los precios en los cuales se alquilan estas líneas dependen de la distancia entre los dos puntos conectados, así como del ancho de banda necesitado.

Estas líneas brindan una capacidad dedicada permanente y se usan frecuentemente en la construcción de redes WAN. Tienen como desventaja el desperdicio de la capacidad, ya que el tráfico WAN es variable, además, cada punto final necesita de una interfaz independiente en el router, lo que hace que los costos de estas soluciones aumenten. Pero los beneficios brindados por estas líneas superan a los costos de las mismas.

3.3.2.1.2 Enlaces de Comunicación Conmutados:

Los enlaces de comunicación conmutados pueden ser por conmutación de circuitos o conmutación de paquetes:

3.3.2.1.2.1 Conmutado por circuitos: Establece una conexión virtual dedicada para datos o voz dinámicamente entre el emisor y el receptor. Antes de la conmutación, se establece la conexión por medio de la red del proveedor de servicios. Algunos enlaces de conmutación de circuitos son el acceso telefónico analógico (PSTN) e ISDN.

3.3.2.1.2.1.1 ISDN: (Red Digital de Servicios Integrado) Permite al bucle local de una PSTN transportar señales digitales, y por ende, aumentando la capacidad de las conexiones conmutadas. Permite la integración de

multitud de servicios en un único acceso, independientemente de la naturaleza de la información a transmitir y del equipo terminal que la genere. La ISDN cambia las conexiones internas de la PSTN de señales portadoras analógicas a señales digitales de multiplexación por división temporal (TDM). Dicho cambio hace que se lleve señales digitales, aumentando la capacidad de la conexión. La conexión usa canales de portadora de 64 Kbps para transportar voz y datos y una señal para la configuración de llamadas. La ISDN también se utiliza como respaldo si la línea arrendada falla

Existen dos tipos de interfaces ISDN:

- La ISDN de interfaz de acceso básico (BRI, Basic Rate Interface) provee dos canales de 64kbps y un canal de 16kbps. Está destinada para uso domestico y de pequeñas empresas. Algunos proveedores permiten que se transmitan a una velocidad baja como las conexiones X.25 a 9.6kbps.
- La ISDN de interfaz de acceso principal (PRI, Primary Rate Interface) brinda 23 canales de 64kbps y un canal de 64hbps (Estandar U.S.A). También está disponible para instalaciones más grandes. En América del Norte, PRI corresponde a una conexión T1. La velocidad de PRI internacional corresponde a una conexión E1.

3.3.2.1.2.1.2 PSTN o Conexión telefónica analógica: Brinda una conexión digital de extremo a extremo por medio de un canal analógico (línea telefónica de voz), traducido mediante un modem en cada extremo. Esta conexión es ideal cuando se necesitan transferencias e intercambios de datos de bajo volumen e intermitentes, ya que las líneas telefónicas ofrecen conexiones conmutadas dedicadas y de baja capacidad. Debido a las características físicas del bucle local y su conexión con la PSTN limitan la velocidad de la señal a menos de 56kbps. Las ventajas de esta tecnología es la simplicidad, la disponibilidad y el bajo costo de implementación. Las desventajas son el tiempo de conexión muy largo, así como la baja velocidad de transmisión de datos.

3.3.2.1.2.2 Conmutado por paquetes: En las redes de conmutación de paquetes los datos se transmiten en tramas, celdas o paquetes rotulados. Incluye tecnologías como X.25, Frame Relay, ATM y Metro Ethernet.

3.3.2.1.2.2.1 X.25: Es un protocolo de capa de red heredado que da una dirección de red a los suscriptores. Establece mecanismos de direccionamiento entre usuarios, negociación de características de comunicación, técnicas de recuperación de errores. Los servicios públicos de conmutación de paquetes admiten numerosos tipos de estaciones de distintos fabricantes. Por lo tanto, es de la mayor

importancia definir la interfaz entre el equipo del usuario final y la red. Se establecen circuitos virtuales a través de la red con paquetes de petición de llamadas a la dirección destino. Un número de canal identifica la SVC resultante. Los paquetes que llevan el número de canal envían la dirección correspondiente. Las velocidades de los enlaces alternan de 2400 bps a 2 Mbps. Sin embargo, las redes públicas poseen velocidades que no superan los 64kbps. Actualmente esta tecnología está en decadencia y es reemplazada por más recientes como ATM, ADSL o Frame Relay.

3.3.2.1.2.2.2 ATM: Se denomina ATM (Asynchronous Transfer Mode) al modo de transferencia asíncrona, la cual es idónea para transferir voz, video y datos a través de redes públicas y privadas.

Se fundamenta en una arquitectura basada en celdas en vez de tramas. Estas celdas con longitud fija de 53 bytes contienen un encabezado de 5 bytes seguido de una longitud fija de 48 bytes para el contenido. Son adecuadas para la transmisión de tráfico de video y voz las celdas pequeñas de longitud fija, ya que este tipo de tráfico no tolera demoras y no tiene que esperar a que se transmita un paquete más grande de datos.

Las celdas ATM son mucho más grandes que las celdas y paquetes de Frame Relay y X.25, lo cual lo vuelven menos eficientes. ATM

usa aproximadamente un 20 por ciento de ancho de banda más que Frame Relay para datos en capa de red.

ATM multiplexa muchas celdas de circuitos virtuales en una ruta (path) virtual colocándolas en particiones (slots), sin embargo, ATM llena cada slot con celdas de un circuito virtual a la primera oportunidad, similar a la operación de una red conmutada de paquetes.

El despliegue de la tecnología ATM no ha sido el esperado. Las velocidades para las que estaba pensada (T1/E1 hasta 622 Mbps) han sido rápidamente superadas. ATM no es la opción más adecuada para las redes actuales y futuras de velocidades del tipo gigabit. ATM es utilizado donde se necesita dar soporte a velocidades moderadas, como en ADSL, aunque se está sustituyendo esta tecnología por otras como Ethernet que la cual está basada en tramas de datos.

3.3.2.1.2.2.3 Frame Relay: Es una técnica de comunicación que funciona mediante la retransmisión de tramas o “frames” de diferentes tamaños, permitiendo la interconexión de redes de área local separadas geográficamente a un costo menor.

Este es un protocolo muy sencillo, debido a que trabaja a nivel de la capa de enlace de datos, por lo que Frame Relay no realiza ningún tipo de control de flujo o de errores. Esto produce una administración

simplificada de las tramas para reducir la latencia. En esta tecnología se ofrecen velocidades de hasta 4 Mbps, e incluso superiores a esta. Frame Relay está orientado a la conexión, ya que suministra conexiones entre usuarios a través de una red pública, igual a una red privada punto – punto. Las conexiones pueden ser del tipo permanente o PVC, o conmutadas o SVC, siendo las permanentes las más usadas ya que se pueden reemplazar las líneas privadas por un solo enlace a la red. Para esto los circuitos virtuales de Frame Relay usan un identificador único llamado DLCI para garantizar una comunicación bidireccional.

Frame Relay ofrece una gran reducción de costos, ya que el Router de la LAN solo necesita una sola interfaz sin importar que existan varios Circuitos Virtuales, por lo cual es óptimo usar esta tecnología para conectar las LAN de una empresa, asimismo, ofrece una conectividad de ancho de banda mediano, compartido y de conectividad permanente.

3.3.2.2 Pública:

Son conexiones que usan la infraestructura global de Internet. Debido a la falta de seguridad y de garantías de rendimiento necesarias para una conexión de extremo a extremo, internet no era uno opción factible como sistema de redes de las empresas. Pese a esto, con el desarrollo de tecnologías como VPN, Internet se volvió una solución segura y económica para la conexión entre trabajadores y oficinas remotas.

La conexión WAN a través de Internet se establecen por medio de servicios de banda ancha (DSL, modem, cable, inalámbrico, etc.).

3.4.2.1.1.1 Internet: Internet es un conjunto descentralizado de redes de comunicación interconectadas, que usa la familia de protocolos TCP/IP, garantizando que las redes físicas heterogéneas que la componen funcionen como una red lógica única, de alcance mundial, lo cual permite que se use esta estructura pública para conexiones WAN.

3.4.2.1.1.1.1 Banda Ancha: Es una tecnología de módems que permite que el tráfico de datos se realice a una velocidad extraordinaria a través de una línea convencional ya sea de teléfono o de TV por cable.

3.4.2.1.1.1.1.1 Cable: El cable coaxial se usa para distribuir las señales de televisión. El acceso a la red está disponible desde algunas redes de televisión por cable, lo cual permite que se disponga de un mayor ancho de banda que con la red telefónica.

Al extremo del usuario se encuentra un modem que traduce las señales digitales a las frecuencias en las que se transmite la televisión por cable, y en el extremo final del

cable (la oficina de TV por cable local) cuenta con el sistema informático y los componentes necesarios para la tener el acceso a internet, en este extremo se encuentra el sistema de terminación de módems de cable (CMTS, cable modem termination system) que envía y recibe señales digitales de módem por cable a través de una red de cables y es necesario para proporcionar los servicios de Internet a los suscriptores del servicio de cable. Todos los suscriptores locales comparten el mismo ancho de banda del cable.

3.4.2.1.1.1.1.2 **DSL:** (Digital Subscriber Line) o Línea de Abonado Digital es una tecnología de conexión permanente que usa las líneas telefónicas de par trenzado existentes para transportar datos de alto ancho de banda y dar servicios IP a los suscriptores. El modem DSL convierte una señal Ethernet en una señal DSL que se transmite a la oficina central. Las líneas del suscriptor DSL múltiples se pueden multiplexar a un único enlace de alta capacidad con un multiplexor de acceso DSL (DSLAM) en el sitio del proveedor.

3.4 Otras Técnicas de Comunicación WAN

3.4.1 VPN

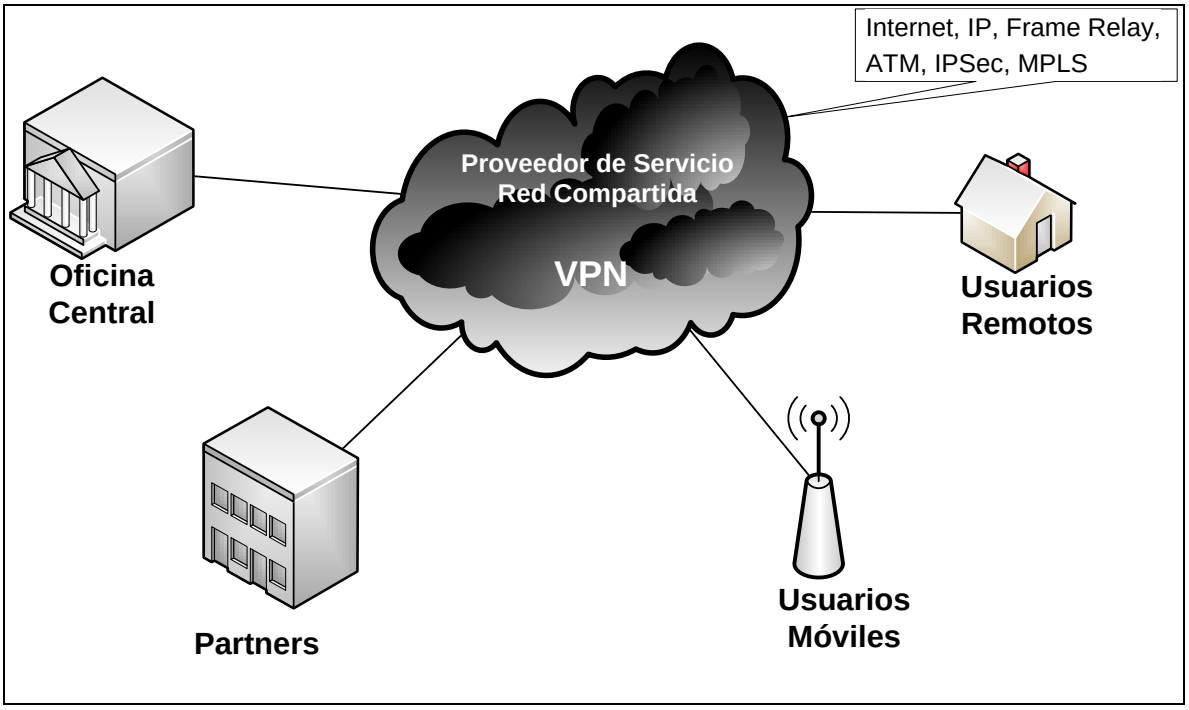


Figura 3. 6: Comunicación VPN

VPN surgió como una alternativa a las conexiones dedicadas punto a punto, porque las conexiones VPN ofrecen los mismos beneficios que una conexión dedicada punto a punto, pero sin los altos costos. Los primeras VPN se pusieron a disposición para Frame Relay y X.25. Mediante el establecimiento de los Circuitos Virtuales (VC) entre los dispositivos cliente, el proveedor de servicios es capaz de emular una conexión dedicada punto a punto, mientras se comparte una infraestructura común del proveedor de servicios y, por tanto, se reducen los costos.

En sí, una VPN no es más que una estructura de red corporativa implantada sobre una red de recursos de carácter público, pero que usa el mismo sistema de gestión y las mismas políticas de acceso que se usan en las redes privadas, finalmente VPN

no es más que la creación en una red pública de un entorno de carácter confidencial y privado que permitirá trabajar al usuario como si estuviera en su misma red local.

En la mayoría de los casos la red pública es Internet, pero también puede ser una red ATM o Frame Relay

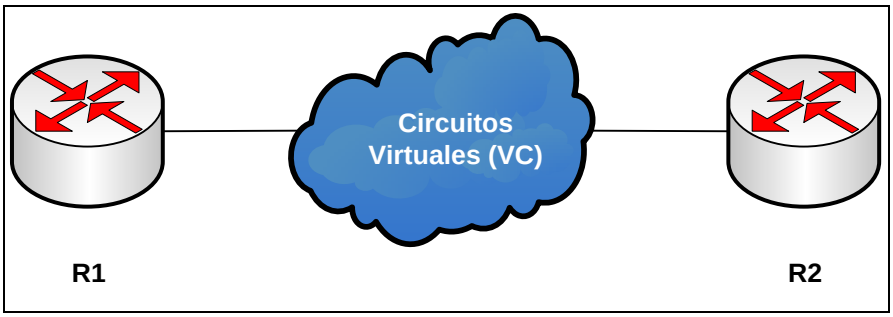


Figura 3. 7: Comunicación por circuitos virtuales

En la figura, los Routers cliente se muestran conectados a través de la red del proveedor de servicios con Circuitos Virtuales.

En el traslado a través de Internet, los paquetes viajan encriptados, por este motivo, las técnicas de autenticación son fundamentales para el correcto funcionamiento de las VPN, ya que se aseguran a emisor y receptor que están intercambiando información con el usuario o dispositivo correcto.

La autenticación en redes virtuales es similar al sistema de inicio de sesión mediante usuario y contraseña, pero se tiene necesidades mayores de aseguramiento de validación de identidades. La mayoría de los sistemas de autenticación usados en VPN están basados en sistema de claves compartidas.

La autenticación se realiza normalmente al inicio de una sesión, y luego, aleatoriamente, durante el transcurso de la sesión, para asegurar que no haya algún tercer participante que se haya podido entrometer en la conversación.

Todas las VPN usan algún tipo de tecnología de encriptación, que empaqueta los datos en un paquete seguro para su envío por la red pública. La encriptación hay que considerarla tan esencial como la autenticación, porque permite proteger los datos transportados de poder ser vistos y entendidos al trasladarse de un extremo a otro de la conexión.

3.4.2 Conexiones Punto-Punto

También conocidas como líneas arrendadas, estas no son VPN, sino que son enlaces privados dedicados a través de una red de proveedor de servicios. Las conexiones punto a punto ofrecen garantía de ancho de banda y privacidad a través de una red de un proveedor de servicio, pero esto posee un precio. El mismo que se cobra, se use o no.

Las conexiones punto a punto son caras debido a que el proveedor de servicios no puede usar multiplexación estadística. La cual está basada en el principio de que no todo el mundo necesita utilizar todo el ancho de banda que están pagando en un momento dado. Ya que no todo el mundo usará todo el ancho de banda todo el tiempo, el servidor de servicios puede vender más ancho de banda que el que realmente está presente en la red.

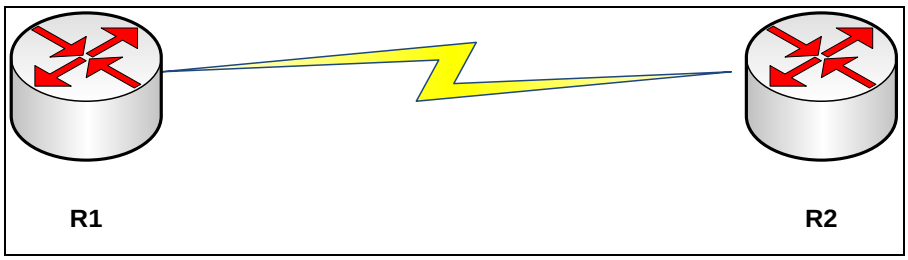


Figura 3. 8: Conexión punto a punto entre dos Routers

Como se ve en la figura, los Routers R1 y R2 son totalmente inconscientes de la infraestructura detrás de su conexión dedicada punto a punto. Es importante recordar que este tipo de conexiones son privadas, seguras y muy caras en precio.

3.4.3 IPsec

IPsec es la abreviatura de Internet Protocol Security, es un conjunto de protocolos que tienen por función el asegurar las comunicaciones sobre el protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para establecer claves de cifrado.

Este protocolo actúa en capa 3 del modelo OSI, es decir en la capa de Red. Otros protocolos de seguridad para Internet de uso extendido, como SSL, SSH y TLS operan desde la capa 4 del modelo OSI (Transporte) hasta la 7. Por lo cual IPsec se vuelve mucho más flexible, ya que se puede usar para proteger protocolos de capa 4, incluyéndose en estos TCP y UDP, teniendo ventaja sobre SSL y otros de capas superiores. Para que una aplicación pueda usar IPsec no hay que hacer ningún cambio, mientras que para usar SSL y otros protocolos de niveles superiores, las aplicaciones tienen que modificar su código.

IPsec se diseñó para proporcionar seguridad en modo transporte (extremo a extremo) del tráfico de paquetes, en el que los PC de los extremos finales realizan el procesado de seguridad, o en modo túnel (puerta a puerta) en el que la seguridad del tráfico de paquetes es proporcionada a varias máquinas (incluso a toda la red LAN)

por un único nodo. IPsec se puede utilizar para crear VPN en estos dos modos, siendo este el uso principal de IPsec.

3.5 MPLS

3.5.1 Protocolo MPLS

El multiprotocolo de conmutación de etiquetas o MPLS (Multi Protocol Label Switching) surge como una solución para cumplir con las necesidades del management de ancho de banda, ingeniería de tráfico, escalabilidad y requerimientos de calidad de servicio, en las redes cuyos backbones son basados en IP. Pero aparte de esto, provee un estándar para la interoperabilidad ente diferentes redes como ATM, Frame Relay e IP. MPLS reduce significantemente el procesamiento de paquetes, lo cual mejora el desempeño de los dispositivos de la red. MPLS es un método para reenviar paquetes a través de una red usando información contenida en etiquetas añadidas a los paquetes.

3.5.1.1 Características MPLS

MPLS es una especificación del IETF, para proveer una designación, ruteo, reenvío y conmutación eficiente de los flujos de datos sobre la red.

Al ser independiente de los protocolos de capa 2 y 3 se dice que MPLS es un protocolo de capa 2.5.

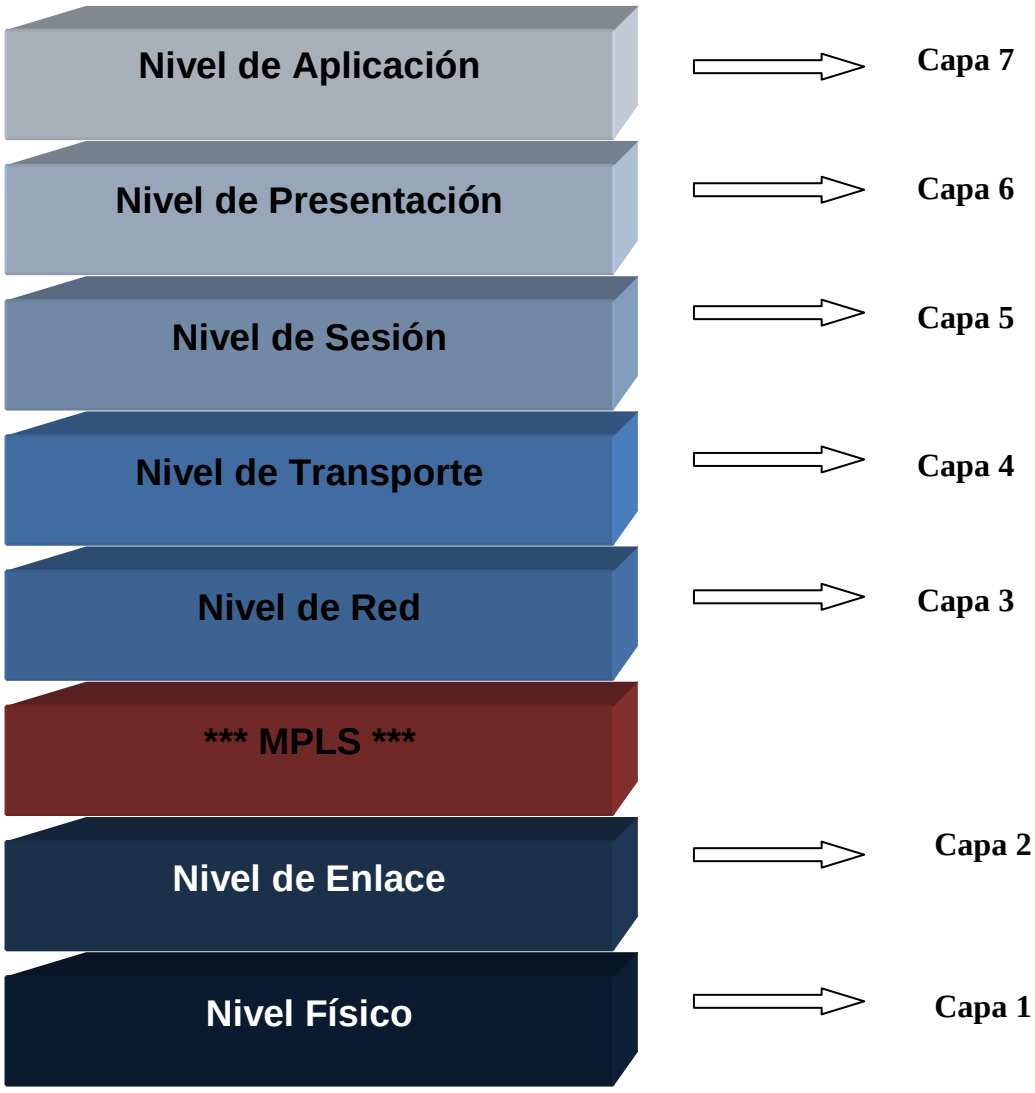


Figura 3. 9: MPLS en el modelo OSI

MPLS suministra una forma de mapear direcciones IP a etiquetas simples, de largo fijo usadas por distintas tecnologías de conmutación de paquetes o reenvío de paquetes. Sirve de interface con protocolos de ruteo como RSVP u OSPF.

El principal objetivo de MPLS es crear redes flexibles y escalables con un incremento en el desempeño y la estabilidad. Esto incluye soporte multiprotocolo, Ingeniería de

Tráfico y soporte de VPNs, el cual ofrece Calidad de Servicio (QoS) con múltiples clases de servicio (CoS).

3.5.1.1.1 QoS (Quality of Service)

QoS o Calidad de servicio, permite a los administradores de redes el uso eficiente de los recursos de la red con la ventaja de garantizar que se asignaran más recursos solo a las aplicaciones que lo necesiten, sin exponer el desempeño de las demás aplicaciones. En si el uso de QoS le da al administrador un mayor control sobre la red, lo que significa menores costos y mayor satisfacción del cliente o usuario final. La Calidad de servicio aparece como solución ante el problema de transmitir más información en menor tiempo, ya que el aumento del ancho de banda en algunas ocasiones no es posible y es limitado. Para esto QoS asigna valores de prioridad a cierto tipo de tráfico.

3.5.1.1.2 Ingeniería de Tráfico

Es la habilidad de definir rutas dinámicamente y planear la asignación de recursos en base en la demanda, así como la optimización del uso de la red. Para el balanceo de carga MPLS facilita la asignación de recursos en las redes dependiendo de la demanda de tráfico de los usuarios, además brinda diferentes niveles de soporte. A diferencia que en OSPF, en MPLS se ven flujos de paquetes con su QoS respectivo y demanda tráfico predecible. Con MPLS es posible predecir rutas en base a flujos individuales, consiguiendo diferentes flujos entre canales similares pero dirigiéndose a diferentes enrutadores. Si llegase a amenazar congestión en la red, las rutas MPLS

pueden ser re-ruteadas inteligentemente, cambiando las rutas de flujo de paquetes dinámicamente conforme a las demandas de tráfico de cada flujo.

Con MPLS el flujo de paquetes viaja a través de un túnel de datos en el eje troncal creado por el Protocolo de Reserva de Recursos (RSVP), la ruta del túnel se da por los requisitos de recursos del túnel y de la red (constraint-based routing). El Protocolo de Enrutamiento Interno (IGP) rutea el tráfico a dichos túneles.

3.5.1.1.3 Soporte de Redes Virtuales Privadas (VPN)

MPLS provee un mecanismo eficiente para el manejo de redes privadas virtuales. De esta manera el tráfico de una red privada atraviesa la red pública (Internet) eficazmente y de manera transparente para el usuario, eliminando cualquier tráfico externo y protegiendo la información. Las VPN sobre MPLS son más flexibles en cualquier red, principalmente IP, además que son de mayor expansión.

MPLS reenvía los paquetes a través de túneles privados usando etiquetas, las cuales actúan como códigos postales. Estas etiquetas tienen in identificador que aísla a esa VPN de las demás.

3.5.1.1.4 Soporte Multiprotocolo

MPLS se puede usar con diversas tecnologías, por lo que por ejemplo, Routers y switches MPLS pueden trabajar sin ningún problema con otros que sean IP. Lo que facilita la escalabilidad en la red, ya que esta tecnología está diseñada para trabajar con redes Frame Relay y ATM. Esto da la ventaja de tener redes mixtas añadiendo QoS para optimizar los recursos y expandirlos.

3.5.2 Funcionamiento MPLS

En MPLS la transmisión de datos sucede sobre el *LSP (Label Switching Paths)*. Cada LSP es una cadena de etiquetas, una por cada nodo, desde el origen al destino. Hay dos formas en las que se establecen los LSP, una es antes de la transmisión y es generada manualmente o por los protocolos de control como BGP, y en la otra los LSP se crean a conforme se detectan los flujos de datos en los nodos. Estos dos procesos reciben la denominación de *Control Driven* y *Data Driven* respectivamente. La conmutación de alta velocidad de los paquetes es posible debido a que las etiquetas son de largo fijo y están insertadas en la cabecera de los paquetes, de modo que no hay que desarmarlos para acceder a ellas, esto permite la conmutación de los paquetes a nivel de hardware.

Una red MPLS es de un conjunto de Enrutadores de Conmutación de Etiquetas *(LSR - Label Switching Router)* que tienen la capacidad de conmutar y rutear paquetes en base a la etiqueta que se ha añadido a cada paquete. Cada etiqueta define un flujo de paquetes entre dos puntos finales. Cada flujo es diferente y es llamado Clase de Equivalencia de Reenvío (*FEC - Forwarding Equivalence Class*), así como también cada flujo tiene un camino específico a través de los LSR de la red, es por eso que se dice que la tecnología MPLS es “orientada a conexión”.

Cada FEC aparte de la ruta de los paquetes contiene varios caracteres que definen los requerimientos de Calidad de Servicio del flujo. Los Routers de la red MPLS no necesitan examinar ni procesar el encabezado IP, solo se necesita reenviar cada paquete dependiendo el valor de su etiqueta. Esta es una de las ventajas que tienen

los Routers MPLS sobre los Routers IP, en donde el reenvío de paquetes es más complicado.

En un Router IP cada vez que se recibe un paquete se analiza su encabezado IP para compararlo con la tabla de enrutamiento y ver cuál es el siguiente salto o el destino más próximo. El hecho de examinar estos paquetes en cada uno de los puntos de tránsito que deberán recorrer para llegar a su destino final significa un mayor tiempo de procesamiento en cada nodo y por lo tanto, una mayor duración en el recorrido, lo cual hace que el tiempo de procesamiento en un Router MPLS sea menor.

3.5.2.1 Flujo MPLS

Según la figura, el flujo de paquetes MPLS se establece de la siguiente forma:

1. Se establece un Camino de Conmutación de Etiquetas (LSP - Label Switched Path) entre los Routers que van a transmitir los FEC. Estos LSP sirven como túneles de transporte entre los componentes de la red MPLS incluyendo los parámetros de Calidad de Servicio específicos del flujo. Dichos parámetros determinan la cantidad de recursos para reservar al LSP y las políticas de desechado y la cola de procesos en cada LSR. Para ello se usan dos protocolos para intercambiar la información entre los Routers de la red.

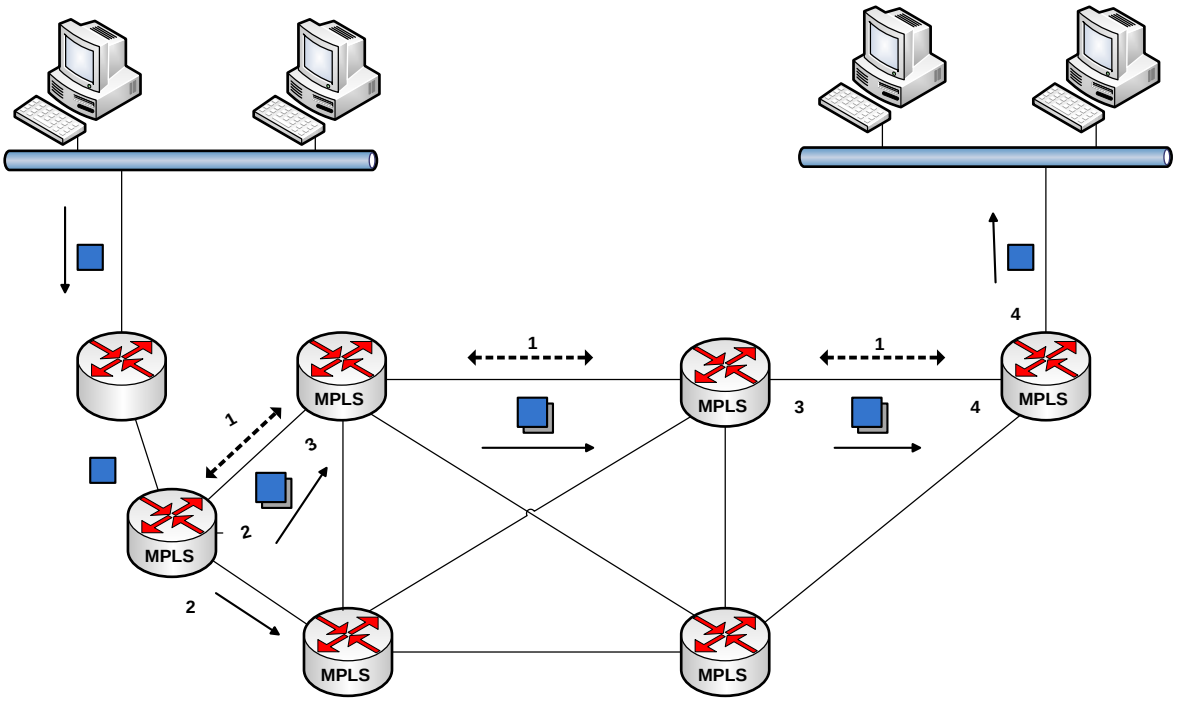
   A cada flujo FEC particular se le asignan etiquetas para evitar el uso de etiquetas globales y así evitar complicaciones en el manejo y cantidad de las mismas. Por esto las etiquetas se referencian al flujo específico. La asignación

de rutas y nombres se pueden realizar manualmente o usando el Protocolo de Distribución de Etiquetas o LDP.

2. El paquete entra al dominio MPLS gracias al LSR de Frontera, el cual determina que servicios de red requiere definiendo la Calidad de Servicio. Al terminar la asignación, el LSR asigna un paquete FEC y a un LSP particular, dándole una etiqueta y lo envía. Si no existe un LSP, el LSR de frontera trabaja junto a los demás LSRs para concretarlo.

3. El paquete se encuentra dentro del dominio MPLS, cuando los Routers adyacentes al LSR reciben el paquete se desecha la etiqueta de entrada y se le añade la nueva etiqueta de salida al paquete y se envía el paquete al siguiente LSR dentro del LSP.

4. El LSR de salida abre la etiqueta y lee el encabezado IP.



Terminología MPLS:
LSP: Label Switched Path
LSR: Label Switching Router
LER: Label Edge Router
FEC: Forwarding Equivalence Class
LDP: Label Distribution Protocol

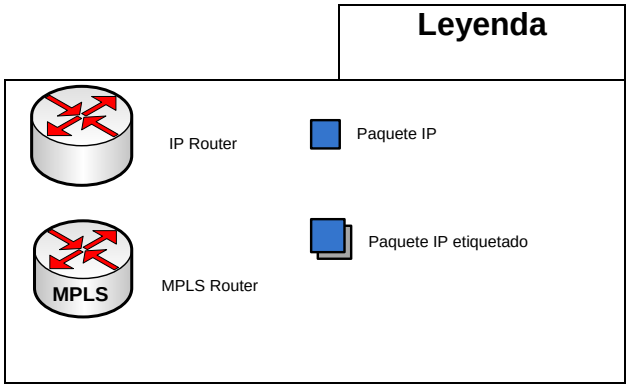


Figura 3. 10: Diagrama de flujo de paquetes de MPLS

3.5.2.2 Label Stacking (Apilamiento de Etiquetas)

MPLS maneja el apilamiento de etiquetas, por lo cual, un paquete etiquetado puede contener varias etiquetas organizadas en modo L.I.F.O (Último en Entrar, Primero en Salir). Por este motivo el procesado de etiquetas MPLS siempre se basa en la

etiqueta superior, por lo que en cualquier LSR se puede añadir o remover una etiqueta.

La ventaja del apilamiento de etiquetas es que permite agregar rutas parciales dentro de la red a un LSP ya existente, creando de esta manera túneles.

Al inicio de cada túnel los LSR fijan la misma etiqueta a los paquetes entrantes, al final de cada túnel pasa lo contrario, el LSR de salida remueve la etiqueta superior q se agregó al inicio del túnel, con el fin de conservar la etiqueta original y así el paquete siga con su trayectoria. Es decir, se puede decir que se crean varios túneles dentro de un LSP original, como en ATM, a diferencia que ATM solo maneja apilamiento de un nivel.

3.5.2.3 Formato de etiquetas MPLS

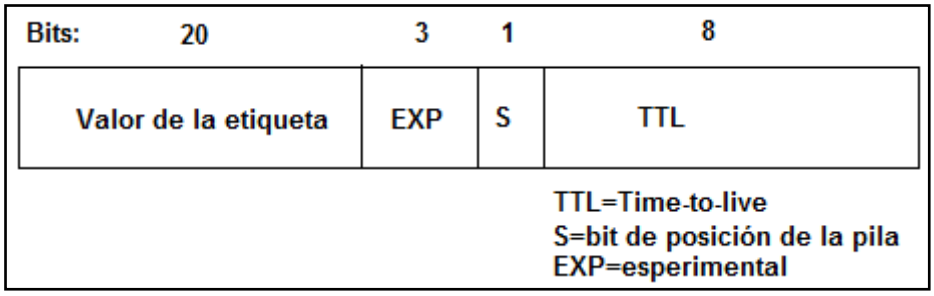


Figura 3. 11: Etiqueta MPLS

Una etiqueta MPLS, como se muestra en la figura, está conformada por 32 bits, divididos en 4 campos con diferentes tamaños y funciones, los cuales son:

Etiqueta: Tiene valor local, y su tamaño es de 20 bits, por lo cual puede generarse más de un millón de etiquetas.

EXP o Experimental: Como su nombre lo indica es un campo experimental, tiene una longitud de 3 bits, y se usa para mapear los paquetes IP estándar ToS (Tipo de Servicio) en el campo experimental para MPLS CoS (Clase de Servicio).

S o Stack Bit: Las etiquetas MPLS pueden apilarse una sobre otra, cuando tiene el valor de 1 indica que es la entrada más antigua de la pila o la parte inferior de la pila, cuando es 0 indica que es cualquier otra entrada.

TTL o tiempo de vida: se usa para codificar el valor de conteo de saltos (IPv6) o de tiempo de vida (IPv4). Este campo se decrementa en 1 y luego se copia dentro de la etiqueta MPLS en el campo TTL. Al salir de la red MPLS, el campo TTL de la etiqueta MPLS es copiado de nuevo dentro del campo TTL de IP. Si ese campo llega a tener un valor igual a 0, el paquete será descartado. El campo TTL tiene un tamaño de 8 bits.

3.5.2.4 Ubicación de la Etiqueta MPLS

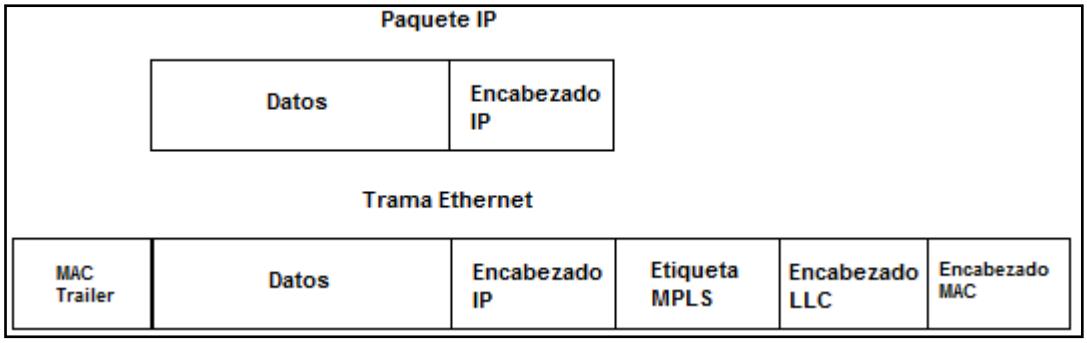


Figura 3. 12: Ubicación de la etiqueta MPLS

Como se muestra en la figura, la etiqueta MPLS se encuentra montada entre la cabecera de Capa 2 y la cabecera de Capa 3. Asimismo se muestra la colocación de

la etiqueta MPLS encapsulada en la trama Ethernet, donde la ubicación de la etiqueta MPLS sigue siendo la misma.

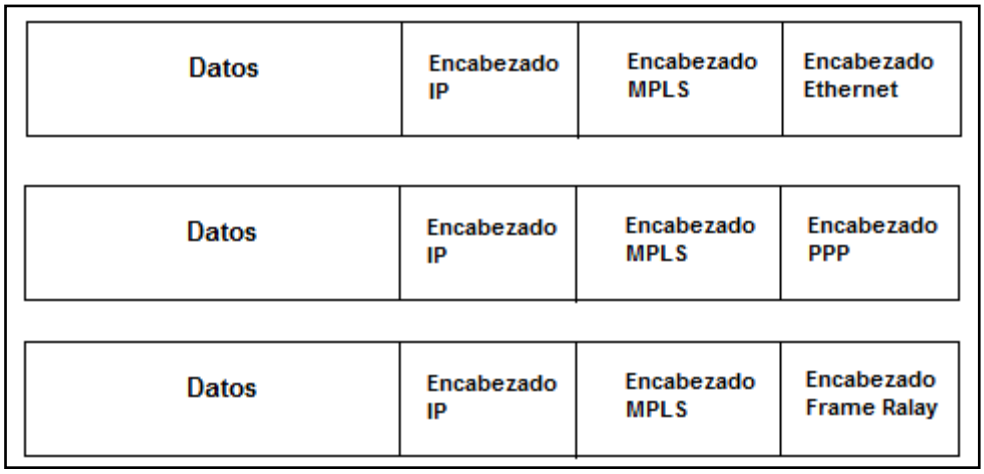


Figura 3. 13: Encabezado MPLS entre cabecera Capa 2 y Capa 3

Independientemente del método que se use para la encapsulación de los datos, la colocación de la etiqueta MPLS no cambia. La cabecera de Capa 3 contiene el campo de destino que se usa para el enrutamiento de capa 3 (forwarding). Debido a que la etiqueta MPLS se presenta antes que la cabecera de Capa 3, el Router la ve primero, entonces el Router puede reenviar paquetes basados en la etiqueta MPLS, en lugar de la cabecera de Capa 3. En MPLS se dice que el tráfico es Switchado, en lugar que Ruteado.

En sí, las etiquetas están vinculadas a las rutas en la tabla de enrutamiento.

3.5.2.5 Manejo de Etiquetas:

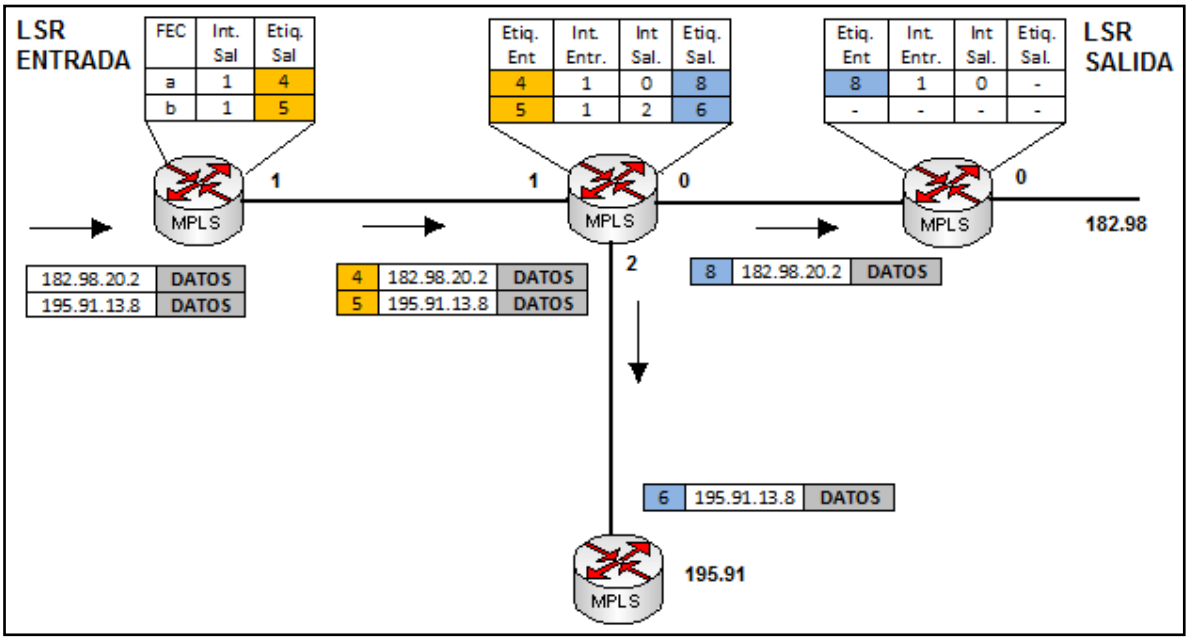


Figura 3. 14: Flujo de etiquetas

Cada LSR posee una tabla de reenvío para cada LSP que pasa por sus interfaces, estas tablas manejan diferentes tipos de datos, la tabla del LSR de entrada maneja la interfaz y etiqueta de salida, y la FEC. Los LSR siguientes en cambio, manejan tanto las etiquetas e interfaces de entrada y salida. En el gráfico se muestra como llegan los datos (a y b) sin etiquetar al LSR de entrada, el mismo que les asigna una etiqueta de salida y lo envía al siguiente LSR. El LSR siguiente deshecha las etiquetas de entrada y les añade nuevas etiquetas y las envía a los LSR correspondientes, en esta parte se muestra la escalabilidad de la tecnología, ya que las etiquetas solo tienen significado local.

Aparte, una función de del LSR de entrada es asignarle una FEC a cada paquete sin etiquetar que entra, y en base a esto se asigna un LSP particular a cada paquete. En el gráfico se muestra los dos FEC (a y b) con su particular LSP.

3.5.3 Dominio de MPLS

Un dominio MPLS es un conjunto de Routers continuos y contiguos habilitados con MPLS. Es un continuo conjunto de nodos, los cuales operan con enrutamiento y envío MPLS. El tráfico puede entrar por un punto final que se encuentre físicamente conectado a la red, o por otro Router que no sea MPLS y que esté conectado a una red sin conexión directa a la nube MPLS.

En enrutamiento tradicional los paquetes son reenviados de un enrutador a otro, cada enrutador hace una decisión de reenvío independiente por cada paquete y se realiza una clasificación dentro de una FEC (Forwarding Equivalency Class).

Para determinar el FEC se pueden usar varios parámetros que define el administrador de red y son: la dirección IP origen o destino y/o las direcciones IP de la red, Usar el Id del protocolo IP, Etiqueta de flujo IPv6, el número de puerto del origen o del destino o elegir el punto de código de los servicios diferenciados.

En MPLS tan pronto un paquete es asignado a un FEC, el análisis del encabezado ya no es hecho por los enrutadores subsecuentes. Todo el reenvío se realiza basado en etiquetas

El reenvío de la información se realiza mediante una búsqueda simple en una tabla predefinida que enlaza los valores de las etiquetas con las direcciones del siguiente salto. Se escoge un next-hop (Siguiente salto) basado en el análisis del encabezado de los paquetes y el resultado del algoritmo de enrutamiento.

Se puede especificar un comportamiento por salto diferente en cada Router de la FEC. Esto define la prioridad en la cola y las políticas de desechado de los paquetes.

Se pueden generar diferentes flujos de datos en la misma red, ya que los paquetes que se envían por los mismos puntos finales pueden tener un diferente FEC, por lo

que las etiquetas serán diferentes y tendrán un comportamiento de salto distinto en cada LSR.

3.5.4 MPLS VPNs

Una de las características fundamentales de MPLS es que permite la creación de Redes Privadas Virtuales (VPN), las cuales se prestan para crear servicios de eje troncal VPN IPv4 de capa 3. Una VPN IP es la plataforma para crear y administrar servicios de valor agregado, como servicios de telefonía y transmisión de datos.

3.5.4.1 Funcionamiento de VPN en MPLS

Cada VPN se asocia con una o más instancias de Ruteo/Reenvío Virtual (VRF). Una VRF determina la membrecía del cliente conectado al Router de frontera del proveedor del servicio (Router PE). Cada VRF se compone de una tabla de ruteo IP, una tabla de reenvío express propietaria de Cisco (CEF), un grupo de interfaces que usan dicha tabla, y un conjunto de reglas y parámetros del protocolo de ruteo que controlan la información que se incluye en la tabla de ruteo.

Las VRF contienen las rutas disponibles en la VPN que pueden ser accesadas por los sitios de los clientes, cada uno de estos sitios puede estar suscritos a varias VPN, pero únicamente a un solo VRF. Cada VRF tiene almacenada información de reenvío de paquetes en las tablas IP y CEF para evitar que no salga ni que entre tráfico fuera de las VPN.

CAPÍTULO IV

DISEÑO DE LA RED

4.1 Establecer parámetros básicos para la configuración de una red segura y estable

Para establecer los parámetros básicos para la configuración de una red estable y segura, antes de todo, debemos tomar en cuenta, que un proveedor de comunicaciones, es dueño de los enlaces de datos que componen una WAN, salvo que una organización posea los recursos para levantar su propio enlace WAN, caso contrario, se puede alquilar los enlaces a un proveedor de comunicaciones.

El ancho de banda de una WAN es mucho menor que el ancho de banda de una LAN. Los costos de suministro de enlace son el elemento más caro, por lo que, la implementación de WAN tiene que buscar proveer un máximo de velocidad de transmisión a un costo por demás tolerable.

El establecer la configuración óptima de una WAN no es una tarea fácil debido sobre todo a la presión por parte de los administradores de contener los costos, y también de los usuarios para alcanzar mayores velocidades de acceso al servicio.

Debido a que a través de una WAN puede viajar un tráfico de video, datos y voz; el diseño que se determine para una WAN debe ofrecer una capacidad adecuada y tiempos de tráfico que cumplan con las necesidades de la organización.

Entre las especificaciones que se debe tomar en cuenta dentro del diseño: la topología de las conexiones entre varias ubicaciones, la naturaleza de esas conexiones y la capacidad de ancho de banda.

Antiguamente, las WAN consistían en su mayoría de enlaces de datos directamente conectados a computadoras centrales remotas, actualmente, las WAN enlazan las LAN que están geográficamente alejadas.

La tecnología WAN funciona en las tres capas inferiores del modelo OSI, las estaciones de los usuarios finales, servidores y Routers se comunican a través de las LAN y los enlaces de datos de la WAN acaban en los Routers locales.

Los Routers determinan la ruta más adecuada hacia el destino de los datos a partir de los encabezados de la capa de red y transfieren los paquetes a la conexión de enlace de datos indicada para su envío en la conexión física.

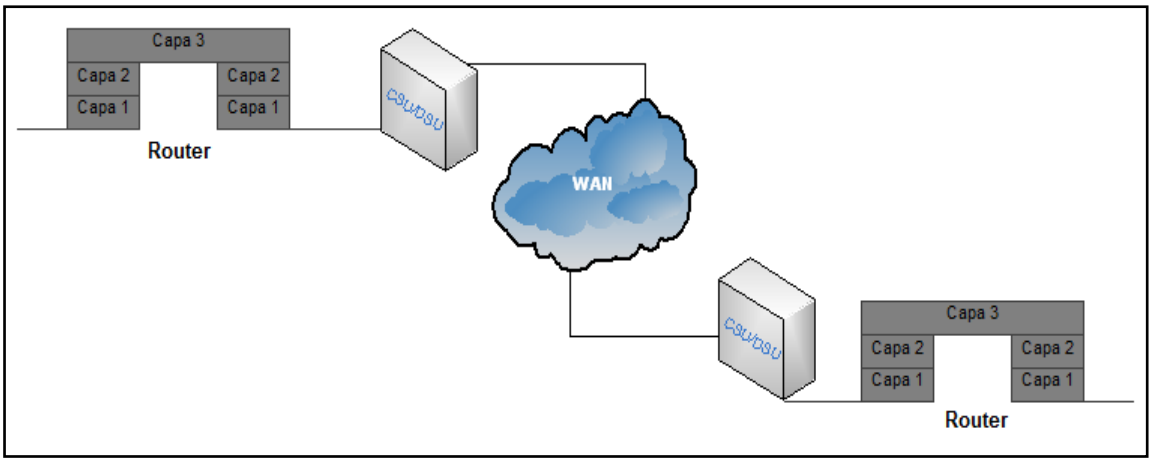


Figura 4. 1: Comunicación de una WAN

Se implementa WAN principalmente para integrar el traspaso de datos entre sucursales externas dentro de una organización, y debido a esta importancia y a los elevados costos de su implementación, nos obliga a diseñar una WAN de manera sistemática.

4.1.1 Pasos para el diseño de una WAN

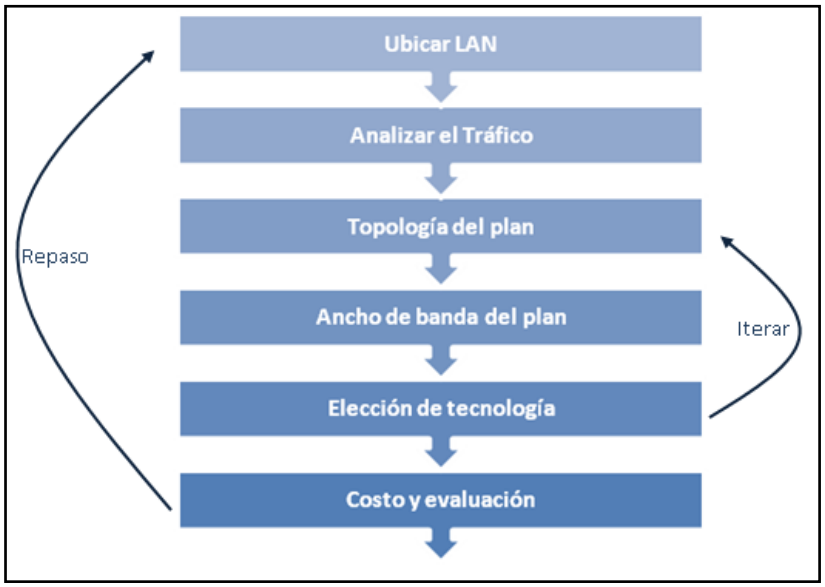


Figura 4. 2: Pasos para el diseño de una WAN

Los pasos que se recomienda para realizar el diseño sistemático de una WAN o para la modificación de una WAN ya existente son los siguientes:

1. **Ubicar las LAN:** Establecer los puntos finales de origen y destino que se enlazarán a través de la WAN.

2. **Analizar el tráfico:** Estudiar el tipo de tráfico de datos a transportarse, su origen y su destino. Las WAN transportan varios tipos de tráfico con requerimientos variables de ancho de banda, fluctuación de fase y latencia. Es necesaria información sobre las diferentes características del tráfico por cada par de puntos finales (origen y destino) y por cada tipo de tráfico.

3. **Planificar la topología:** Tomar en cuenta que tendrán influencia en la topología las cuestiones geográficas y los requerimientos como la disponibilidad. Un alto requisito de disponibilidad demanda enlaces adicionales que brinden rutas de datos alternativas y balanceo de carga adecuado.

4. **Calcular el ancho de banda necesario:** Hay que tener en cuenta, que el tráfico en los enlaces puede tener diferentes requisitos de fluctuación y latencia, además se necesita incluir la demanda de ancho de banda por parte de los usuarios.

5. **Seleccionar la tecnología de WAN:** Se deben seleccionar las tecnologías de enlace apropiadas, analizando detenidamente que tecnología de encaminamiento es la más adaptable a nuestro modelo.

6. **Evaluar los costos:** Una vez que todos los requerimientos se hayan establecido, se pueden determinar y comparar los costos de instalación y operación de la WAN con la necesidad comercial que llevó a la implementación de WAN.

Se debe considerar que estos pasos no son un proceso lineal para diseñar o para hacer una modificación a una WAN existente, es necesario repetir algunos pasos varias veces antes de presentar el diseño final de la WAN a ser implementado. No obstante, gracias a la evolución en el tiempo de muchas WAN, quizá no necesiten tomar en cuenta algunos pasos de los presentados para su diseño.

4.1.2 Robustecimiento de la infraestructura de red

El robustecimiento de una red, no es una tarea, sino un proceso. Por lo cual se debe tener constante vigilancia sobre las amenazas continuas a la red y poder realizar acciones correctivas a tiempo. El robustecimiento, se basa en configuraciones óptimas de hardware y software en la red.

Las principales actividades que se deben hacer en una red para hacerla más robusta y segura y que nos servirá como base para el diseño son:

- **Revisar el diseño de red:** Se trata de comprender cómo está diseñada la red, saber cómo los dispositivos están conectados entre sí y como se comportan los flujos de datos.

- **Implementar un firewall:** Es de vital importancia implementar un firewall, ya que es la tarea de mayor impacto dentro del robustecimiento de una red, puesto que permite definir un perímetro.

- **Implementar listas de control de acceso (ACLs):** Se debe controlar y limitar todo el tráfico que sale y entra de la red desde el mundo exterior. Asimismo, se debe limitar el tráfico entre segmentos de red internos, dependiendo de las necesidades de los departamentos y usuarios dentro de la organización. Las ACLs deben implementarse no solo en los firewalls y Routers externos, sino también en los internos.

- **Apagar características y servicios innecesarios:** Si no se tiene alguna razón para que determinados servicios y características se encuentren activos, se deben apagar ya que consumen ancho de banda y recursos de procesamiento dentro de los dispositivos de red.

- **Aplicar protección contra virus:** Una vez levantada la red, es imprescindible que todos los sistemas de escritorio hasta los servidores se encuentren ejecutando alguna protección antivirus, especialmente como en los STMP Gateways para evitar los virus basados en correo electrónico y también gusanos, ya que a pesar de que casi la totalidad de los virus están dirigidos a las aplicaciones, causan a menudo ataques distribuidos de negación de servicio (DDoS) contra Routers y switches por la forma en la que estos se replican.

- **Asegurar las conexiones inalámbricas:** Se debe tomar en cuenta en el diseño de red que tan necesaria es el uso de un dispositivo inalámbrico, ya que una conexión inalámbrica, al no poseer un medio físico para su propagación es más propensa a que usuarios no autorizados puedan usarla para conectarse a la red. De ser el caso que sea necesaria la conexión inalámbrica, se debe usar el cifrado y la autenticación para evitar que usuarios no autorizados intercepten la comunicación inalámbrica, y si no es necesaria la conexión, lo recomendable es apagarla.

4.1.2.1 Fortaleciendo la seguridad de Routers y switches

Los Routers y Switches forman el núcleo de la infraestructura de red. De hecho son en sí la misma infraestructura de red. Por consiguiente, si se necesita que la infraestructura de red pueda ser tan segura como sea posible, se debe fortalecer la seguridad de los Routers y switches.

4.1.2.1.1 Endurecimiento del Acceso a la Administración

Aunque se va a trabajar con un IOS Cisco, los conceptos y recomendaciones de este estudio son válidas para todos los dispositivos de las diferentes marcas, además que la mayoría de los comandos citados son válidos para cualquier dispositivo basado en IOS con interfaz de línea de comandos (CLI), así mismo, los comandos sirven tanto para Routers o switches.

Antes de implementar un dispositivo de red y esperar ser capaz de utilizarlo para asegurar la red, primero se debe configurar el dispositivo para acceder a la administración de seguridad. Hay cuatro métodos principales de acceso a la gestión interactiva:

- **Acceso a la consola:** Requiere conectividad de consola física al dispositivo
- **Acceso VTY:** Utiliza la red para establecer una consola virtual como acceso a través del uso de protocolos como Telnet y SSH
- **GUI basada en Web:** Usa una interfaz gráfica de usuario basada en web a través de HTTP o HTTPS para administrar el dispositivo
- **Acceso auxiliar:** Utiliza una conexión de módem de fuera de banda de acceso a la consola.

Para hacer más seguras estas conexiones se puede aplicar el servicio de cifrado de la contraseña en el dispositivo

Router(config)# service password-encryption

También se debe configurar el tiempo de espera, para que la gestión administrativa del dispositivo finalice automáticamente después de un periodo de inactividad, esto asegura que si alguien se olvida de cerrar la sesión del sistema, la sesión no queda

abierta, para lo cual ingresamos la siguiente línea de comando dependiendo de qué tipo de conexión vamos a asegurar:

Router(config-line)#exec-timeout 5 0

Esto configura el tiempo de espera exec para cerrar la sesión en cualquier sesión inactiva después de cinco minutos y cero segundos. Hay que ejecutar este comando para cada tipo de línea, la consola, auxiliar y VTY.

4.1.2.1.1.1 Asegurar acceso a la consola

Primero se necesita restringir al acceso físico al dispositivo, ya que el acceso a la consola requiere que alguien sea capaz de conectarse físicamente al puerto de consola en el dispositivo, por lo general mediante una conexión serial del PC. Por lo cual el primer paso de obtener acceso a la consola es cuidar la seguridad física del dispositivo. El dispositivo debe ser colocado en un área cerrada y asegurada para restringir el acceso a ella.

El siguiente paso es configurar el dispositivo para requerir autenticación de cualquier consola de conexiones a través de la utilización de contraseñas de consola. Esto se realiza ejecutando los siguientes comandos desde el modo de configuración global de ejecución:

Router(config) # line con 0

Router(config-line) # login

Router(config-line) # password <enterpassword>

4.1.2.1.1.2 Proteger el acceso VTY

El acceso VTY es el acceso tradicional de gestión de red que utiliza Telnet o SSH. Se debe asegurar la autenticación y el control de acceso a la administración del dispositivo por este medio. Para ello, se hace lo mismo que para asegurar la consola, solamente con la diferencia que se debe permitir la conexión antes de definir una contraseña de autenticación.

Router(config) # line vty 0 4

Router(config-line) # login

Router(config-line) # password <enter password>

Posteriormente a esto, podemos controlar el acceso VTY a través del uso de ACLs (listas de acceso) para permitir o negar el acceso VTY a determinadas direcciones IP dependiendo de su autorización de acceso al dispositivo.

4.1.2.1.1.3 Asegurar el acceso a la administración basada en Web

Por razones de su entorno amigable para el usuario, la administración basada en Web es a la que muchos de los dispositivos están dirigidos, pero traen muchos problemas de seguridad, por lo cual es recomendable deshabilitar este tipo de administración ingresando los siguientes comandos:

Router(config)#no ip http server

Router(config)#no ip http secure-server

4.1.2.1.1.4 Asegurar el Acceso Auxiliar

El puerto auxiliar es el de más alto reforzamiento del dispositivo, debido a que no solo sirve para realizar gestión remota a través de un modem, también se puede usar

como un puerto de consola secundario, por lo cual si no se lo toma en cuenta, puede significar un punto libre de entrada para ataques. Para lo cual se recomienda deshabilitar dicho puerto, a menos que sea de vital importancia, para lo cual realizamos:

```
Router(config)#line aux 0
Router (config-line)#transport input none
Router (config-line)#login local
Router (config-line)#exec-timeout 0 1
Router (config-line)#no exec
```

Si se va a usar el puerto auxiliar para gestión fuera de banda, debe ser asegurado en la misma manera que sus líneas VTY.

4.1.2.1.1.5 Proteger el acceso a modo privilegiado

El modo de acceso privilegiado es el modo de acceso que permite a los usuarios empezar a hacer cambios, por lo cual se necesita asegurar este acceso por medio de una contraseña. Para ello hay dos métodos, el primero es usando el comando **enable password** pero es un método obsoleto sin casi ninguna protección, ya que se puede ver la contraseña haciendo un show run. El método recomendado ya que posee cifrado MD5 es mediante el comando **enable secret**, el cual se configura con el siguiente comando en el modo de configuración global:

```
Router(config)#enable secret <enterpassword>
```

4.1.2.1.2 Fortalecimiento de Servicios y Características

Así como fortalecemos los servicios que se ejecutan en la red, también debemos deshabilitar servicios innecesarios en sus servidores y estaciones de trabajo, así como también hay que deshabilitar servicios innecesarios en los Routers y Switches. Para lo cual se deben revisar los siguientes servicios y características:

4.1.2.1.2.1 Cisco Protocolo de descubrimiento (CDP)

Es un protocolo propietario de Cisco para gestión administrativa, propaga la información de las características de otros dispositivos de marca Cisco adyacentes. Por lo cual, si bien es útil, si se ejecuta permanentemente, aparte de dar problemas de uso de banda innecesariamente, brinda información útil a un atacante, para lo cual deshabilitamos de las siguientes formas:

Router (config)#no cdp run

Dentro de una interfaz:

Router(config)#interface fastethernet 0

Router(config-if)#no cdp run

4.1.2.1.2.2 TCP y UDP Small Servers

TCP y UDP Small Servers ejecutan una serie de servidores que proporcionan información de diagnostico entre otras, pero en si es información sin valor, hasta pueden ser usadas para ataques. Para lo cual deshabilitamos con estos dos comandos:

Router(config)#no service tcp-small-servers

Router(config)#no service udp-small-servers

4.1.2.1.2.3 Finger

El Finger Server se usa para obtener información sobre los usuarios conectados en una determinada localización de la red, mostrando lo mismo que se puede visualizar simplemente tecleando el comando **show users**, para lo cual no se necesita levantar un servidor, así que es necesario desactivar este servidor.

Router(config)#no ip finger

Router(config)#no service finger

4.1.2.1.2.4 Tiempo de protocolo de red (NTP)

NTP sincroniza la hora en todo su entorno de red, por lo cual se propagan actualizaciones recurrentes por la red. Para lo cual es necesario deshabilitarlo.

Router(config-if)#ntp disable

4.1.2.1.2.5 Servidor BOOTP

Bootp se usa por los usuarios para cargar su sistema operativo a través de la red, normalmente estaciones de trabajo sin disco. Puede utilizar un Router de Cisco como un servidor bootp para proporcionar el software IOS a otro equipo Cisco, lo cual es una buena estrategia de implementación, pero se pueden usar otras que no

castiguen al ancho de banda de nuestra red, por lo cual se recomienda deshabilitar este servicio.

Router(config)#no ip bootp server

4.1.2.1.2.6 Protocolo de configuración dinámica de host (DHCP)

DHCP se usa para proporcionar direcciones IP a los clientes que las soliciten. Los Routers Cisco pueden actuar como un servidor DHCP. Sin embargo, un servidor local puede proporcionar servicios de DHCP, o el Router puede ser configurado para soportar el reenvío de broadcast DHCP (DHCP Relay agent) a un servidor DHCP centralizado con el comando **ip helper-address**.

Por defecto, el Router no está ejecutando un servidor DHCP, sin embargo, puede asegurarse que no se ejecute con el comando:

Router(config)#no ip dhcp pool <poolname>

4.1.2.1.2.7 Configuración de carga automática

Muchos dispositivos de Cisco son capaces de extraer su configuración desde un dispositivo de red a través de un proceso conocido como la carga automática de configuración. Este es un proceso completamente inseguro ya que puede cargar dichas configuraciones de servidores que posean configuraciones erróneas o inválidas.

Puede desactivar esta funcionalidad en los dispositivos ejecutando los siguientes comandos desde el modo de configuración global:

Router(config)#no boot network

Router(config)#no service config

4.1.2.1.2.8 Resolución de nombres

La resolución de nombres es utilizada por los dispositivos para apoyar la inscripción de nombres de host en lugar de direcciones IP. Se puede desactivar con el comando:

Router(config)#no ip domain-lookup

4.1.2.1.2.9 Proxy ARP

El Proxy ARP se utiliza para permitir que los sistemas en dos subredes diferentes que normalmente no serían capaces de comunicarse unos con otros puedan hacerlo. Proxy ARP es implementado para dial-in de usuarios PPP. Si no se usa PPP es necesario deshabilitar este servicio ejecutando el siguiente comando en el modo de configuración de la interfaz para todas las interfaces en el dispositivo:

Router(config-if)#no ip proxy-arp

4.1.2.1.2.10 Broadcast dirigidos

Permite que un host remoto iniciar un broadcast en una segmento LAN diferente, como resultado de esto, los broadcasts dirigidos se usan generalmente para generar ataques de negación de servicio (DoS), inundando un segmento con tráfico broadcast. Se puede desactivar esta función con el comando:

Router(config-if)#no ip directed-broadcast

4.1.2.1.2.11 IP source routing

Se utiliza para permitir la fuente para definir la ruta que un paquete debe tomar en la red (por lo tanto, el nombre de la fuente de enrutamiento). Se utiliza comúnmente para las redes Token Ring, y puede ser usado para diferentes ataques, se deshabilita ejecutando el siguiente comando en el modo de configuración global de ejecución:

Router(config)#no ip source-route

4.1.2.1.2.12 ICMP Redireccionados, inalcanzables, y respuestas de máscara

Aunque los mensajes ICMP proporcionan una gran cantidad de información para resolver problemas, también puede ser usado por un usuario malicioso para localizar y diagnosticar una red. Tres mensajes ICMP, en particular, son comúnmente utilizados para este propósito: Redirecciones, inalcanzables, y respuestas de máscara. Se desactiva estos protocolos ejecutando los siguientes comandos en el modo de configuración de la interfaz para todas las interfaces en el dispositivo:

Router(config-if)#no ip redirects

Router(config-if)#no ip unreachable

Router(config-if)#no ip mask-reply

4.1.2.1.2.13 Syslog

Se utiliza para proporcionar un repositorio central de datos de registro que se puede utilizar para auditar y para la solución de problemas. Puede configurar syslog para

enviar todos los eventos de un determinado nivel o inferior a un servidor syslog. Debido a que la depuración no es rutinaria en los dispositivos, se recomienda no enviar la depuración de eventos al servidor de syslog por defecto y usar informational como el nivel de severidad por defecto de registro de syslog. Se configura syslog ejecutando los siguientes comandos en el modo de configuración global:

Router(config)#logging trap informational

Router(config)#logging 192.168.173.114

4.1.2.1.2.14 Protocolo simple de administración de Red (SNMP)

SNMP se usa para gestionar sus dispositivos de red, proporcionando mecanismos de configuración, así como la supervisión del funcionamiento y configuración de dispositivos. Es importante analizar que si no se está usando SNMP para gestionar, lo podemos deshabilitar con el comando **no snmp-server**

4.1.2.1.2.15 Implementación de direcciones loopback

Se debe configurar la dirección de loopback del Router para proporcionar un método estable y seguro de manejar el dispositivo porque la interfaz loopback es fija. Además, puede utilizar la interfaz loopback como interfaz de origen para una serie de servicios y protocolos de enrutamiento, lo que le permite configurar la seguridad de otros dispositivos con más fuerza, porque sólo es necesario permitir el acceso de la dirección loopback en lugar de una de las interfaces.

El establecimiento de loopback asegura que todo el tráfico que el Router crea será leído desde la misma IP, lo que facilita una mejor gestión y control. Puede ejecutar

los siguientes comandos desde el modo de configuración global de ejecución para aplicar una dirección loopback:

Router(config)#interface loopback 0

Router(config-if)#ip address 192.168.250.1 255.255.255.255

A continuación, puede hacer referencia a la dirección loopback en toda la configuración del Router. Por ejemplo, puede asignar la dirección de bucle invertido como la fuente de FTP, TFTP, syslog, SNMP, y NTP, sólo para nombrar unos pocos, ejecutando los siguientes comandos en el modo de configuración global:

Router(config)#ip ftp source-interface loopback 0

Router(config)#ip tftp source-interface loopback 0

Router(config)#logging source-interface loopback 0

Router(config)#snmp-server trap-source loopback 0

Router(config)#ntp source loopback 0

4.1.2.1.2.16 Deshabilitar las interfaces no utilizados

Algo esencial debería ser el desactivar las interfaces no utilizados. Puede desactivar las interfaces de los dispositivos ejecutando el siguiente comando en el modo de configuración de la interfaz de todas las interfaces de dispositivos que deben ser desactivados:

Router(config-if)#shutdown

4.1.2.1.2.17 Configurar volcado de memoria

Todos los sistemas tienen la capacidad de volcado de memoria por lo general cuando exceden la capacidad de su memoria RAM. Para ayudar a diagnosticar la causa de las caídas de sistema de los Routers, podemos configurarlos para descargar la memoria principal a un servidor externo. El método más seguro de llevar a cabo esto es mediante el uso del protocolo FTP:

```
Router(config)#ip ftp source-interface loopback 0
Router(config)#ip ftp username routeruser
Router(config)#ip ftp password routerpass
Router(config)#exception protocol ftp
Router(config)#exception dump <IP servidor FTP>
```

4.1.2.2 Fortalecimiento de las Tecnologías de Ruteo

Para fortalecer las tecnologías de ruteo se necesitan realizar cuatro tareas principales:

4.1.2.2.1 Implementación de redundancia

Una de las cosas más importantes que se puede hacer para proporcionar seguridad de la infraestructura es proporcionar redundancia de dispositivos críticos. Esto garantiza que si un dispositivo falla, el dispositivo redundante transparente puede llenar el vacío dejado atrás.

4.1.2.2.2 Endurecimiento de los protocolos de enrutamiento

Por la forma en que los protocolos funcionan, no hay mucho que se pueda hacer sobre la seguridad de los mismos, ya que la mayoría de protocolos de enrutamiento fueron creados para no estar cifrados, asimismo, la mayoría de protocolos de enrutamiento usa tráfico multicast o broadcast para propagar las rutas, lo cual lo hace muy inseguros.

Pero para solucionar estos problemas de seguridad existen varias alternativas:

- Se puede levantar los protocolos de enrutamiento con autenticación.
- Implementar interfaces pasivas que no van a participar en el enrutamiento.
- Filtrado de las actualizaciones de enrutamiento para restringir la información que se comparte entre los dispositivos.
- Usar Agujeros Negros y Null Routing para enrutar todos los paquetes de una red dada a la interfaz nula, impidiendo de manera efectiva cualquier tráfico que vaya a esa red.

4.1.2.2.3 Aplicación de la gestión del tráfico

Las funciones de un Router también incluyen gestión de tráfico, es decir, definen que tráfico será permitido, y cuanto de cualquier tráfico será autorizado.

Para esto los Routers tienen los siguientes mecanismos:

- Verificación RPF (Unicast Reverse-Path Forwarding) permite configurar el Router para realizar una comprobación inversa de la ruta de acceso en todos los paquetes que recibe.

- Listas de Control de Acceso (ACLs) representan el método más funcional de control de la circulación, ya que ofrecen un alto grado de granularidad de configuración.
- Control de acceso basado en Contexto (CBAC) proporciona la funcionalidad adicional de ser capaces de realizar satisfactoriamente inspección dinámica de paquetes, así como ser capaz de profundizar en los datos. Es como ACLs reforzados.
- Gestión de Inundaciones, es la función del Router que se encarga de controlar el flujo de tráfico a través del mismo, para protegerse de los ataques de inundación como los de negación de servicio.

4.1.2.2.4 La implementación de IPsec

La implementación de IPsec es el único método efectivo real de asegurar el tráfico que de otras formas inseguras (SNMP, TFTP, syslog, etc.). Por lo que se puede implementar de dos formas:

Estableciendo IPsec entre dos Routers o entre dos dispositivos para cifrar todo el tráfico que atraviesan la red entre los dos dispositivos, y también, usando IPsec para la gestión remota segura del dispositivo, como por ejemplo, para hacer un túnel Syslog, SNMP, o el tráfico Telnet en IPsec.

4.2 Estudio de la vialidad para la realización de una red WAN basada en MPLS

Actualmente, se está empleando tecnologías de conmutación de etiquetas añadidas a paquetes IP o Label Switching, principalmente debido a los avances en Hardware y a la necesidad de realizar mantenimiento a una red, debido a que estas tecnologías

aportan velocidad, calidad de servicio y facilitan la gestión de los recursos de una red.

Esto rompe toda regla del enrutamiento convencional, ya que, en con las convencionales, los Routers eligen sus caminos previa consulta a su tabla de enrutamiento, la misma que se crea estáticamente o por protocolos dinámicos (OSPF, RIP, IGRP, BGP, etc.). Por lo cual no lo hace tan flexible ni escalable al momento de enviar paquetes.

Es por eso que se necesitan de nuevas técnicas para direccionar y aprovechar la infraestructura de una red con el fin que no existan problemas de flexibilidad ni escalabilidad que se presentan actualmente en soluciones tecnológicas ya antiguas.

El rediseño de una red siempre debe tomar en cuenta los puntos vistos en la sección anterior, ya que conlleva un gran gasto de tiempo y sobre todo de dinero, pero sobre todo, se debe encaminar hacia un fin, el cual es, hacerla lo más útil posible, aprovechando todos los recursos de infraestructura posible, de bajo costo, y sobre todo, totalmente transparente para la migración.

Al momento de elegir la tecnología de encaminamiento a usarse, se debe analizar desde el punto de vista de las tecnologías existentes, estableciendo semejanzas y diferencias fundamentales, así como si podrán satisfacer las tendencias del mañana.

Una solución actual para los problemas de encaminamiento presentes y que se proyecta a los del mañana, es MPLS, que es un conjunto de procedimientos que combinan el desempeño, calidad de servicio y gestión del tráfico, del barrido de

etiquetas de capa de acceso a la red, con la escalabilidad y flexibilidad de funcionalidades del enrutamiento en capa de red.

El funcionamiento de MPLS como hemos visto en el capítulo anterior, se basa en la asignación de etiquetas de longitud corta y fija a paquetes en la frontera a un dominio MPLS, y entonces usa esas etiquetas en lugar de las cabeceras de los paquetes IP para enviar los paquetes a través de los caminos preestablecidos dentro de una red MPLS.

Asimismo, la ruta por la que se envía el paquete a través del dominio MPLS es asignada una sola vez a medida que un paquete ingresa a la red. Los nodos a través de la ruta no toman decisiones de envío para un paquete específico, ya que usan la etiqueta del paquete como índice en una tabla que les define el siguiente salto del paquete, antes de enviar el paquete, el Router cambia la etiqueta a una etiqueta que es usada para enviar datos por el siguiente Router en el camino.

MPLS tiene como concepto arquitectural la separación del plano de control del plano de envío en los elementos de conmutación.

Debido a esto, para que un proveedor pueda usar nuevas tecnologías de transmisión de datos y banda ancha, se tiene que analizar que tan viable es la migración de una red a otra red mucho más actual en el aspecto técnico y operacional.

Como se ha visto, la arquitectura de MPLS necesita de dos elementos de red propios, que son un equipo que tiene como función conmutar las etiquetas, y otro equipo que trabaja en dos entornos de tecnologías diferentes.

Para lo cual se necesita sustituir el software que se usa en los equipos de red para poder tener compatibilidad con el envío MPLS, para lo cual hacemos un Upgrade o actualización del IOS de los Routers de la red que vamos a migrar a MPLS por un IOS que sea compatible con nuestro Hardware del Router y permita realizar MPLS.

Para un equipo de núcleo de red las funcionalidades del equipo únicamente deben basarse en la conmutación y el intercambio de etiquetas. Para un equipo de frontera de red, en cambio, las funcionalidades de red se basan en el envío MPLS y en el envío IP tradicional.

Por lo tanto, debido a que la mayoría de las modificaciones en la red son a nivel de IOS o software operativo de los equipos, aplicar una solución MPLS es técnicamente viable, ya que nos permite usar los mismos dispositivos de la red, incrementando la funcionalidad de los mismos y abaratando considerablemente los costos ahorrando recursos a la organización.

Dentro del control de un equipo de núcleo de red se añaden funcionalidades que le permiten entablar y relacionar conceptos de enrutamiento IP tradicional con la conmutación de etiquetas. Dentro de los equipos de frontera se añaden técnicas que permiten comunicar entre dos entornos diferentes (MPLS e IP tradicional).

Consecuentemente, MPLS nos permite añadir características tanto de control, como de envío a los dispositivos de red para darle funcionalidad y compatibilidad a la nueva tecnología, siendo entonces MPLS una solución operacionalmente viable.

4.3 Realizar el Diseño de la Red, procurando cumplir con todas las expectativas para la elaboración adecuada de una red WAN basada en MPLS

Para aplicar e implementar la tecnología MPLS en una red en la que se pueda mostrar al máximo las ventajas y prestaciones de esta novedosa tecnología, vamos a partir de un nodo de una red usado por un proveedor de comunicaciones que alquila circuitos virtuales por medio de Frame Relay a clientes corporativos.

Dicho proveedor usa una topología WAN de malla completa, la cual posee diez Routers marca Cisco modelo 3640 con software de características básicas IP, pero capaces de levantar Frame Relay y módulos NM-4E y NM 4T para sus conexiones.

Esta red Frame Relay con la actual demanda de ancho de banda y de tiempos de respuesta del nuevo tráfico trae problemas a los clientes de dicho proveedor, ya que experimentan las desventajas evidentes de Frame Relay, ya que no soporta aplicaciones sensibles al tiempo como son el tráfico de voz y video, además que los circuitos de Frame Relay suele perderse si el enlace entre el nodo conmutador de dos redes falla, sumado a esto, Frame Relay no se ha actualizado para solucionar dichos problemas.

Por ello, el proveedor de comunicaciones se ve obligado a buscar una solución a los problemas presentados, la cual debe ser económica, aprovechando al máximo la infraestructura ya instalada de la red, así como, prestando confiabilidad y escalabilidad a la red.

La red Frame Relay tiene la siguiente topología, en la cual los Routers FRSx hacen de Switches Frame Relay.

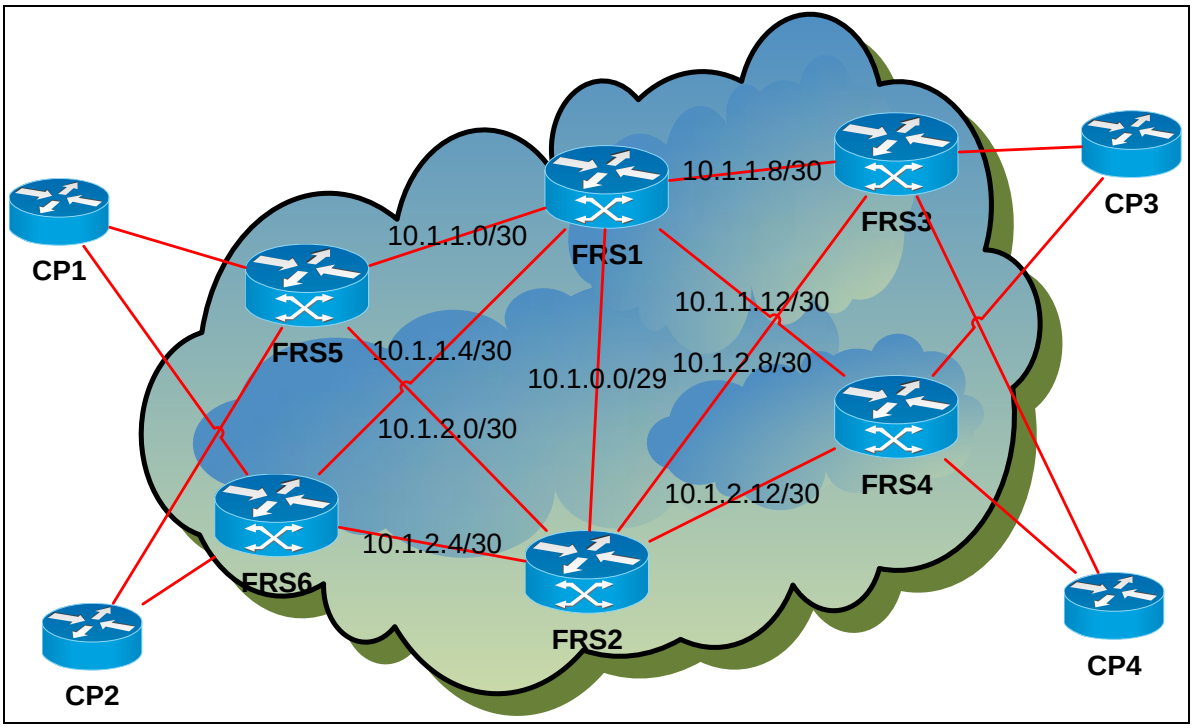


Figura 4. 3: Dominio FRAME RELAY y topología mallada completa

El diagrama de la red ya levantada en el simulador muestra una que posee conexiones seriales en una topología de malla completa, y dos conexiones Ethernet entre FRS1 y FRS2 lo cual nos permite convertir a estos dos Routers en Routers de Core o de núcleo. Posibilitando esto, tener un diseño full-mesh en el núcleo de red del proveedor de comunicaciones, haciendo que este pueda ofrecer garantías de envió de datos y que también cuente con caminos secundarios y redundantes en el caso de que algún nodo en el núcleo de la nube falle.

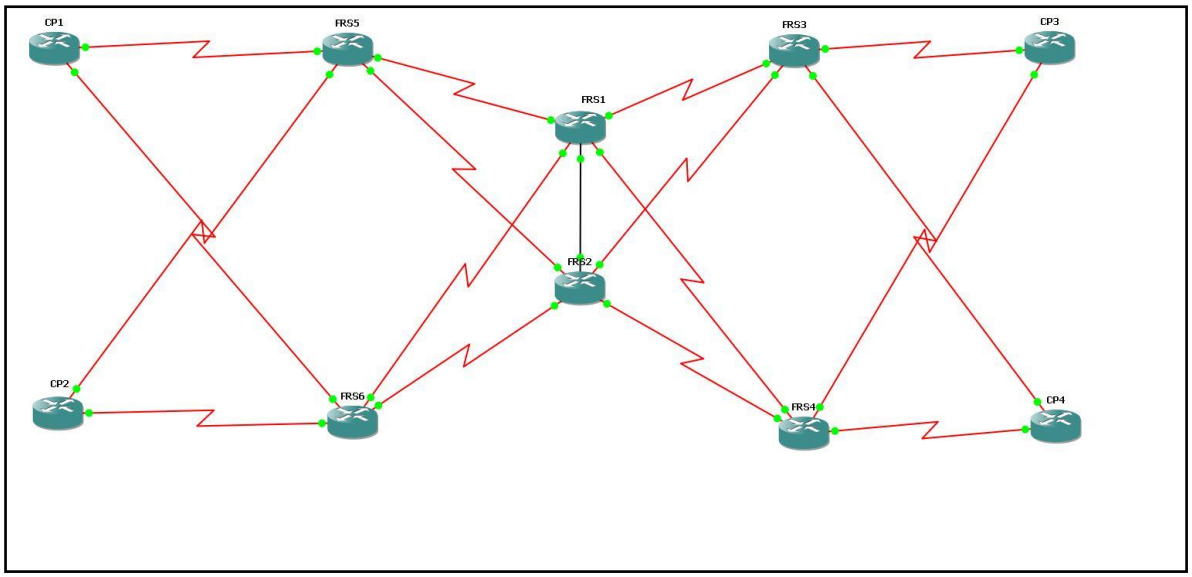


Figura 4. 4: Topología física de la red de la red Frame Relay

Asimismo, gracias a que el diseño de la red Frame Relay fue pensada en un posible crecimiento no es necesario realizar cambios físicos en la topología, para lo cual solo necesitaremos realizar cambios en el software, ahorrándonos elevadísimos costos en hardware.

Ya que no necesitamos realizar cambios en las conexiones físicas de la red, en lo que respecta a los Routers Switches Frame Relay, vamos a usar las mismas direcciones IP para dichos enlaces, ahorrándonos con esto también tiempo en la implementación.

Se debe ofrecer una topología lógica que permita que los usuarios se comuniquen a través del dominio MPLS lo más transparentemente posible, ya que al ser un protocolo de rutas dinámico no tiene un camino ni un tiempo de respuesta definido, pero en cambio, los optimiza.

Para lo cual definimos una red donde dos clientes deban conectarse con sus sucursales remotas a través de un dominio MPLS como lo muestra la figura, para compartir distintos tipos de información, como correo, video, voz, etc.

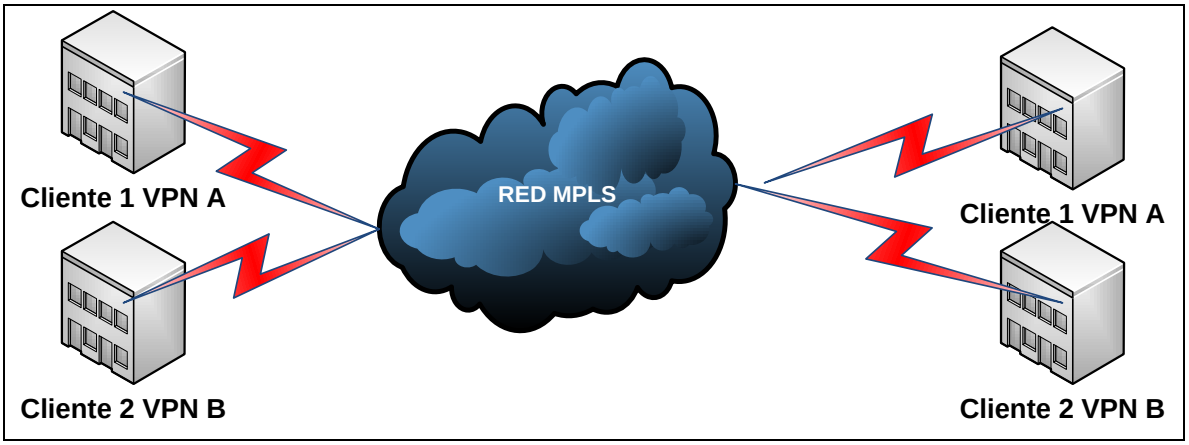


Figura 4. 5: Dominio MPLS

Como se muestra en la figura, los clientes del proveedor de comunicaciones pueden compartir su información a través de un dominio MPLS por medio de VPNs ofrecidas por el proveedor como solución económica a la necesidad de enlaces dedicados.

4.3.1 Implementación de MPLS en la red

Dado que vamos a implementar MPLS en una red que estaba destinada a enlaces Frame Relay, tenemos que renombrar los equipos con nombres propios de una red MPLS para una mejor administración de red.

Para lo cual, FRS1 y FRS2 por sus conexiones redundantes son Routers P1 y P2 por ser los Routers del núcleo.

FRS3, FRS4, FRS5 y FRS6 por sus conexiones cambian a ser Routers de borde de proveedor (PE provider edge) PE1, PE2, PE3 y PE4.

Y, finalmente, los Routers CP1, CP2, CP3, CP4, al ser Routers del borde del cliente (CE customer edge), y por usar VPNs MPLS necesitan identificar con el nombre del VRF (VPN routing and forwarding) usado para las VPN, en este caso serán VRF1-CE1, VRF2-CE1, VRF1-CE2 y VRF2-CE2 respectivamente.

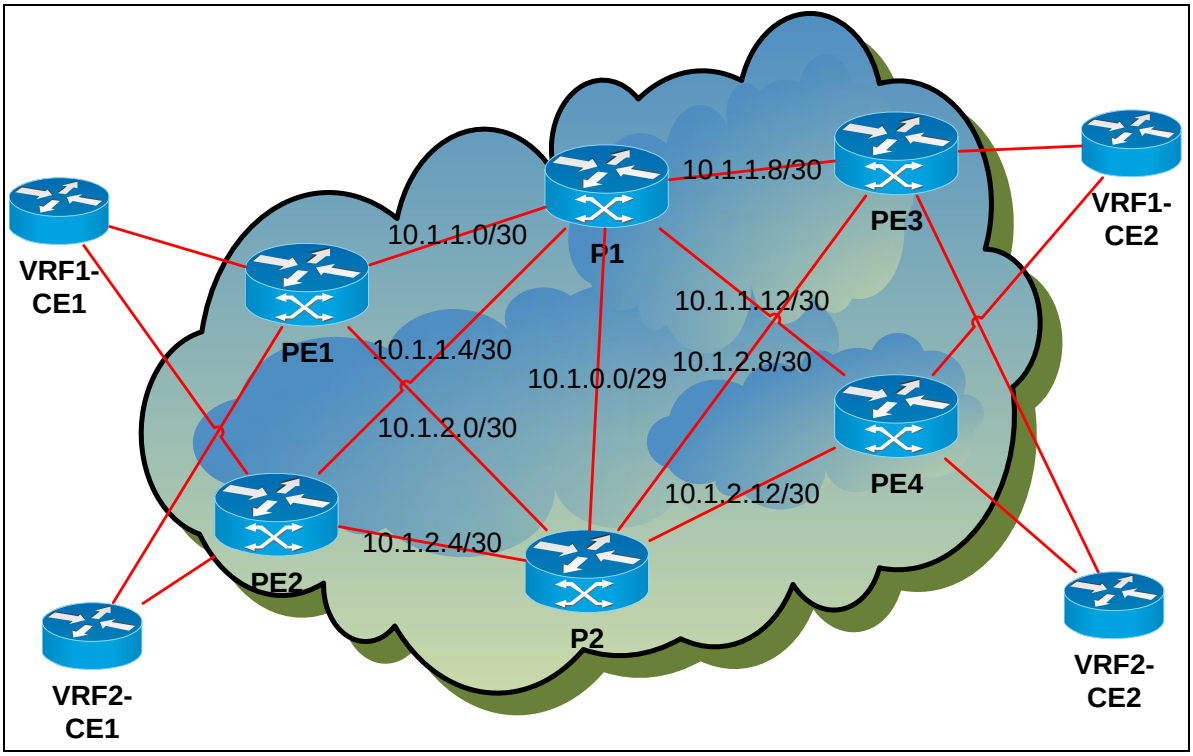


Figura 4. 6: Modelo de implementación de MPLS

Levantando esta topología en el simulador tendríamos el siguiente modelo listo para la implementación de MPLS

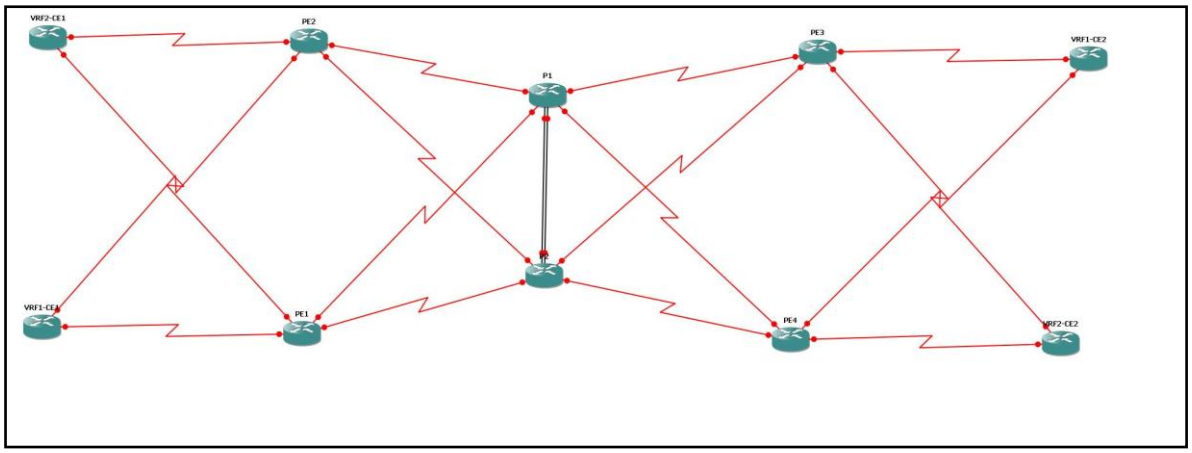


Figura 4. 7: Topología física de la red MPLS

Una vez hechos estos cambios debemos cargar un nuevo IOS que soporte MPLS en el caso de ser necesario.

Para ello debemos tener activa una conexión entre el Router y un PC. En el PC instalamos un software servidor TFTP, debemos considerar también que la imagen no sobrepase la capacidad de la memoria Flash del Router.

Una vez conectado el PC y levantado el TFTP server, desde la consola del Router ingresamos los siguientes comandos:

Router# copy copy tftp flash

Address or name of remote host []? <Ingresar IP del servidor>

Source filename []? <Nombre del IOS en el servidor TFTP>

Destination filename [Nombre del IOS en el servidor TFTP]? <Se puede elegir otro nombre para el IOS>

Reiniciamos el Router

Router# reload

4.3.1.1 Configuración MPLS y BGP de un Router

La configuración que seguiremos será para Routers Cisco, ya que es la marca de Routers de la red que se diseñó anteriormente para trabajar en un dominio MPLS, pero estas configuraciones también sirven para otras marcas.

Se configurará BGP y se establecerá los comandos necesarios para la realización de VPN sobre MPLS.

4.3.1.2 Configurar la interfaz loopback

La interfaz de loopback sirve como identificador del Router. Debemos configurar una interfaz de loopback ya que, esta interfaz se asocia a los procesos OSPF y BGP, asegurando no perder las sesiones OSPF o BGP por un problema físico en la interfaz debido a que las interfaces de loopback son interfaces lógicas. Una interfaz de loopback se crea con estos comandos:

Router# configure terminal

Router(config)# interface loopback<número de la interfaz>

Router (config-if)# ip address <dirección IP> <máscara>

4.3.1.3 Configurar la interfaz

La creación y configuración de subinterfaces se realiza siguiendo los siguientes pasos:

Router# configure terminal

Router(config)# interface fastethernet<nº interfaz>.<nº subinterfaz>

Router(config-subif)# encapsulation dot1Q <VLAN ID>

Router(config-subif)# ip address <dir IP> <máscara>

Router(config-subif)# no shutdown

4.3.1.4 Configuración básica de OSPF:

Se configurará OSPF como protocolo de ruteo dinámico en el futuro backbone MPLS, especialmente para la comunicación redundante de los Routers de núcleo P y los PE. Todos estos se los configurará como enlaces OSPF punto-punto

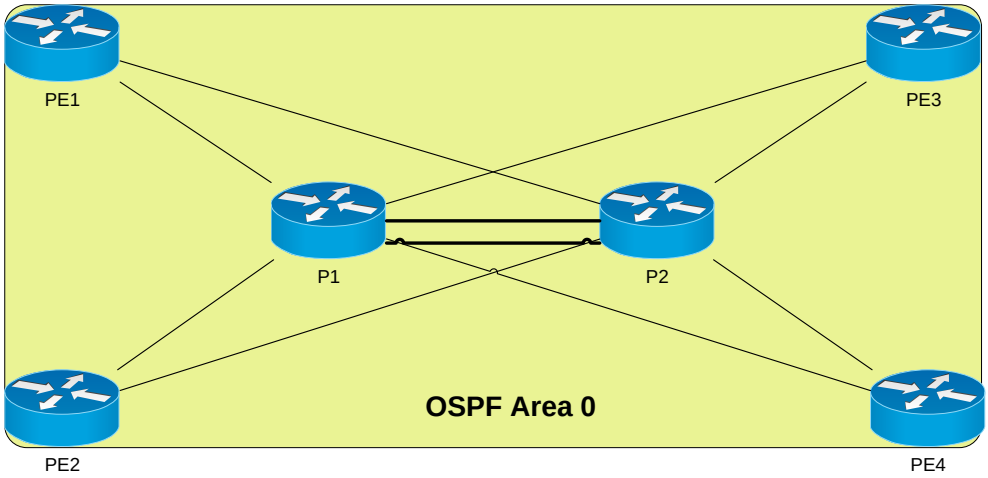


Figura 4. 8: Área de OSPF

Router(config)# interface <tipo_interfaz> <número de la interfaz>

Router (config-if)# ip ospf network point-to-point

Router(config)# router ospf #AS

Router (config-router)# router-id #Id

Router (config-router)# network IP #wildcard area #area

El comando para comprobar las adyacencias OSPF y que permite ver la tabla de rutas del Router es:

Router# show ip route

4.3.1.4.1 Verificar el estado de OSPF

Podremos comprobar el estado de OSPF por interfaz así como los vecinos OSPF con los siguientes comandos:

Router# show ip ospf interface

Router# show ip ospf neighbors

4.3.1.5 Configuración básica de BGP:

Antes de configurar MPLS en la red, es necesario establecer un full-mesh de sesiones BGP en nuestro backbone y así dejar preparada la red para la configuración final de MPLS en los Routers.

Se configura BGP en un dominio MPLS con el fin de dejarlo preparado por si se requiere crear servicios de redes privadas virtuales sobre MPLS (VPN-MPLS) lo cual sí necesita la configuración de un protocolo del tipo de BGP para poder ofrecer servicio. Por lo cual, no es del todo obligatorio el uso de BGP en un dominio MPLS, ya que se puede implementar una red con funcionalidad MPLS sobre OSPF directamente.

La configuración de BGP necesita seguir los siguientes pasos:

- Configurar el proceso de ruteo BGP:

Router# configure terminal

Router(config)# router bgp <número de proceso BGP>

Lo que se configura con el comando Router bgp <numero de proceso BGP> es el sistema autónomo en el que queremos que se “converse” BGP.

El número de proceso BGP que se usa es el 65000 para entorno de pruebas, ya que hay otras numeraciones que están reservadas.

- De cada pareja de Routers, en uno de los Routers definimos al Router vecino y le indicamos que actualice el ruteo a través de la interfaz de loopback configurada anteriormente:

Router(config-router)# neighbor <dir IP de la interfaz del vecino que tiene enfrentada> remote-as <número de proceso BGP >

Router(config-router)# neighbor <dir IP de la interfaz del vecino que tiene enfrentada > update-source loopback<número de la interfaz>

En el caso de que no estén conectados directamente los Routers, la dirección IP que se tiene que indicar es la de la interfaz de loopback configurada en el otro Router para que se instauren relaciones de vecindad.

En el otro Router debemos especificar al Router vecino con la interfaz de loopback con la que le hemos indicado que actualice el encaminamiento:

Router(config-router)# neighbor <dir IP de la interfaz de loopback del vecino> remote-as <número de proceso BGP >

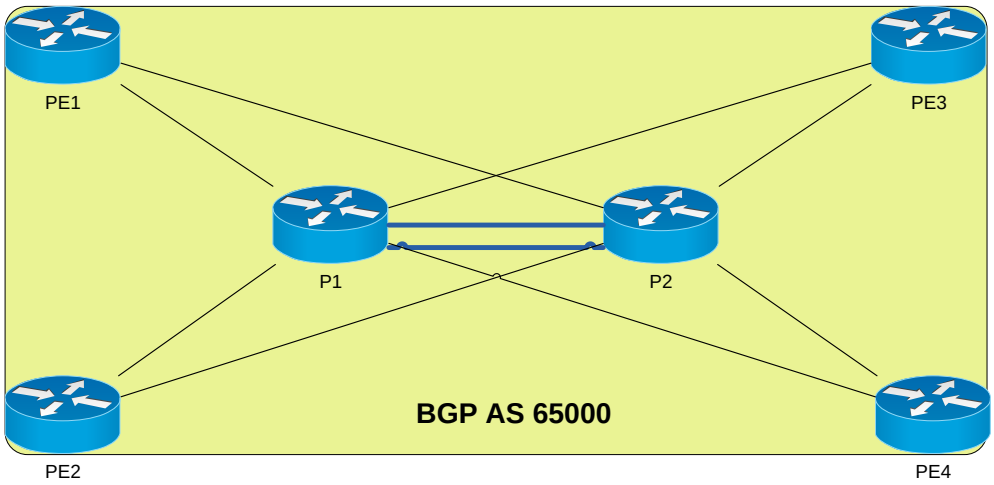


Figura 4. 9: Área de configuración de BGP

Todos los Routers PE reflejan las rutas de los Routers P, los dos Routers P, en cambio, ofrecen grupos de rutas reflejadas. Las líneas negras representan iBGP reflejando rutas (iBGP route-reflector iBGP), las azules son iBGP estándar.

Se recomienda usar BGP Route Reflectors si se tienen un número considerable de Routers haciendo de PE, sobre todo para poder tener una mayor escalabilidad.

4.3.1.5.1 Verificar del estado de BGP

Para verificar el estado de BGP usaremos los siguientes comandos:

Comandos:	
show ip bgp neighbor	Muestra los Routers que mantienen una relación de vecindad con el Router en el que se ejecuta el comando, así como la información relativa a esa relación
show ip bgp summary	Muestra los Routers que mantienen una relación de vecindad con el Router en el que se ejecuta el comando, así como el estado en el que se encuentran
clear ip bgp *	Permite resetear las sesiones BGP establecidas

Tabla 4. 1: Comandos para configurar el estado de BGP

4.3.1.6 Configuración básica de MPLS

Una vez establecidos los protocolos de ruteo, se establecen las funcionalidades MPLS en los Routers. Para ello hay que levantar el protocolo de distribución de etiquetas en las distintas interfaces por las que vamos a comunicar por MPLS.

La configuración de MPLS requiere los siguientes pasos:

- Configurar el CEF (Cisco Express Forwarding) en todos los Routers con funcionalidad "PE" y "P", CEF es el conjunto de funcionalidades que reúnen los equipos Cisco para poder trabajar en un entorno MPLS entre otras funciones.

  Router# configure terminal
  Router(config)# ip cef

  Para comprobar si se ha activado CEF correctamente usamos el comando:
  Router# show ip cef summary

- Activar el protocolo de distribución de etiquetas LDP en cada interfaz por la que se quiere comunicar por MPLS

  Router(config)# interface <nombre de la interfaz>
  Router(config-if # mpls ip
  Router(config-if)# mpls label protocol ldp

4.3.1.6.1 Verificación del funcionamiento de MPLS en la red

Para realizar la verificación del funcionamiento de MPLS, algunos comandos para chequear el funcionamiento de MPLS en la red son los siguientes:

Comandos	
show mpls interfaces	Muestra las interfaces en las que está funcionando MPLS-LDP.
show mpls ldp parameters	Muestra los parámetros que está utilizando el protocolo en el equipo donde se ejecuta el comando.
show mpls ldp neighbor	Muestra los Routers que mantienen una relación de vecindad con el Router en el que se ejecuta el comando.
show mpls ldp binding	Muestra la tabla de etiquetas que está utilizando el Router donde se ejecuta el comando.
show mpls forwarding-table	Muestra la tabla de forwarding del Router donde se ejecuta el comando.

Tabla 4. 2: Comandos para la verificación del funcionamiento de MPLS

4.3.1.7 Configuración de VPNs sobre MPLS

La configuración que se detalla a continuación es para crear VPNs en las que el encaminamiento entre los equipos de cliente (CE) y los equipos del proveedor (PE) se realiza de forma dinámica mediante OSPF y la topología que se generará será totalmente mallada (Full-Mesh).

Hay una configuración distinta según estemos trabajando en un equipo de cliente (CE) o en un equipo de proveedor (PE).

Los Routers con funcionalidad “CE” van a tener configurado el proceso 255 de OSPF en el área 0 en los enlaces que les unen al backbone MPLS, ya que es el proceso

configurado en el backbone. Además, tendrán configurado otro proceso OSPF para las áreas distintas de la cero.

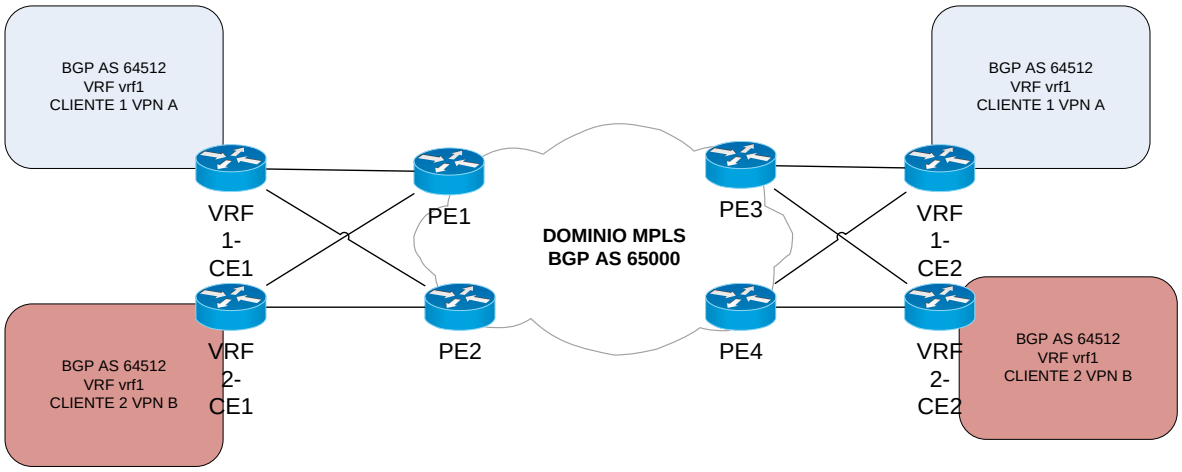


Figura 4. 10: Diagrama de comunicación de las VPNs de los clientes

4.3.1.7.1 Configuración de equipos con funcionalidad PE

La configuración de VPNs sobre MPLS requiere establecer los siguientes pasos en cada uno de los Routers con funcionalidad “PE”:

4.3.1.7.1.1 Configurar la VRF asociada a la VPN a configurar en los Routers con funcionalidad PE

Una VRF (VPN routing and forwarding) incluye las tablas de envío y encaminamiento de los sitios pertenecientes a una VPN.

Los parámetros necesarios para crearla son el Route Distinguisher (RD) que permite identificar unívocamente un prefijo de VPN-IPv4 y el Route-Target (RT) que identifica los Routers que deben recibir la ruta.

Router# configure terminal

Router(config)# ip vrf <nombre de la VRF>

Router(config-vrf)# rd <valor del rd>

Router(config-vrf)# route-target export <valor que tiene que exportar>

Router(config-vrf)# route-target import <valor que tiene que importar>

El siguiente comando agrupa en uno solo los dos últimos comandos, para indicar que el Router donde se ejecuta debe exportar e importar el mismo route-target:

Router(config-vrf)# route-target both <valor que tiene que importar y exportar>

En una topología Hub & Spoke, el sitio que hace de “Hub” debe tener conocimiento de enrutamiento completo de todos los sitios que pertenecen a la misma VPN. Todo el tráfico destinado a la VPN fluirá a través del sitio Hub. Con esta topología, las sedes que hacen de Spoke exportan sus rutas al Hub, por lo que el route-target debe cambiar con respecto a una topología Full-Mesh.

En el sitio que hace de Hub:

Router(config-vrf)# route-target export <valor que tiene que exportar>

Router(config-vrf)# route-target import <valor que tiene que importar>

En el sitio que hace de Spoke:

Router(config-vrf)# route-target export <valor que importa el Hub >

Router(config-vrf)# route-target import <valor que exportar el Hub>

4.3.1.7.1.2 Configuración del “forwarding” en las interfaces de los Routers “PE” que están enfrentadas a los Routers CE

Router# configure terminal

Router(config)# interface <nombre de la interfaz>

Router(config-if)# ip vrf forwarding <nombre de la VRF>

4.3.1.7.1.3 Asignación de la dirección IP a la interfaz donde se configura el “forwarding” dentro de la VPN.

Ya que pierde el direccionamiento de dicha interfaz. Después de ejecutar este último comando se mostrará un mensaje indicando que en la interfaz anterior se le ha quitado la configuración IP, por lo que habrá que volver a configurarla:

Router(config-if)# ip address <dirección IP> <máscara>

4.3.1.7.1.4 Configuración del encaminamiento dinámico en la VRF creada

Se debe levantar un nuevo proceso OSPF dedicado al ruteo dentro de la VRF:

Router# configure terminal

Router(config)# router ospf <identificador del proceso> vrf <nombre VRF>

Definir el área en la que se encuentran las interfaces pertenecientes a la VPN:

Router(config-router)# network <red> <wildcard> area 0

4.3.1.7.1.5 Configuración de iMBGP:

Para que los prefijos aprendidos puedan ser transmitidos a los otros equipos PE, hay que configurar iMBGP siguiendo los siguientes pasos:

Comprobar que los vecinos iBGP siguen activos y operativos. Utilizar el comando Router# show ip bgp summary.

Nos metemos en la configuración de BGP del router:

Router# configure terminal

Router(config)# router bgp <número de proceso BGP que esté configurado>

Entramos a configurar iMBGP para la VPN:

Router(config-router)# address-family vpnv4

Hay que activar los vecinos existentes con la nueva funcionalidad. Según se vayan ejecutando los comandos siguientes se resetearán las sesiones BGP, ya que sus vecinos se encuentran en negociación.

Configurar para cada vecino iBGP mostrado con el comando **show ip bgp summary** lo siguiente:

Router(config-router-af)# neighbor <dir IP del vecino iBGP> activate

Router(config-router-af)# neighbor <dir IP del vecino iBGP> send-community both

4.3.1.7.1.6 Configuración del envío de los prefijos aprendidos al resto de los equipos con funcionalidad PE

Una vez establecidas las sesiones iMBGP con el resto de equipos PE y verificada la conectividad local con los integrantes de la VPN, se deben propagar los prefijos locales al resto de equipos PE para que éstos encaminen los paquetes hacia dichos prefijos. Para esto se debe redistribuir OSPF en el iMBGP:

Router# configure terminal

Router(config)# router bgp <número de proceso BGP que esté configurado>

Router(config-router)# address-family ipv4 vrf <nombre del VRF>

Router(config-router-af)# redistribute ospf <identificador del proceso OSPF> vrf <nombre del VRF>

4.3.1.7.1.7 Configuración del envío de los prefijos aprendidos a los equipos con funcionalidad CE

Router# configure terminal

Router(config)# router ospf <identificador del proceso OSPF> vrf <nombre del VRF>

Router(config-router)# redistribute bgp <número de proceso BGP que esté configurado> subnets metric 20

4.3.1.7.2 Verificación del funcionamiento de la VPN-MPLS

Con los siguientes comandos se verifica que la VPN que hemos configurado está funcionando según lo esperado:

Comandos	
show ip route vrf <nombre VRF>	Comprobamos los prefijos que se han exportado y los que se han importado en la tabla de ruteo de la VRF, así como los prefijos de la VPN.
ping vrf <nombre VRF> <Dirección remota>	Igual que un ping normal, pero se usa dentro del dominio MPLS
traceroute vrf <nombre VRF> <Dirección remota>	Igual que un traceroute normal, pero comprueba el funcionamiento de la VPN, ya que el traceroute deja de funcionar en un dominio MPLS.

Tabla 4. 3: Comandos para la verificación del funcionamiento de la VPN-MPLS

4.3.2 Resultados de la implementación

Una vez establecidos los parámetros para el diseño de la red, así como la implementación de MPLS en las configuraciones de la topología de la red, tenemos como resultado una red MPLS con VPNs estable y totalmente funcional.

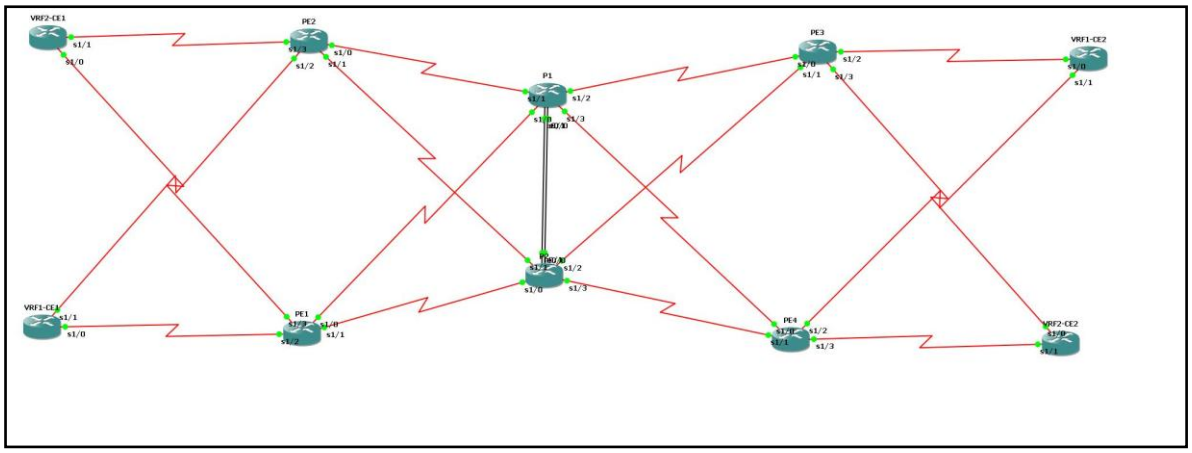


Figura 4. 11: MPLS implementado y funcionando

La información BGP/OSPF en los P Routers indica que el núcleo actualmente está hablando BGP entre sí (Ruteo EGP) y habla OSPF con los PE Routers y con los P Routers (Ruteo IGP).

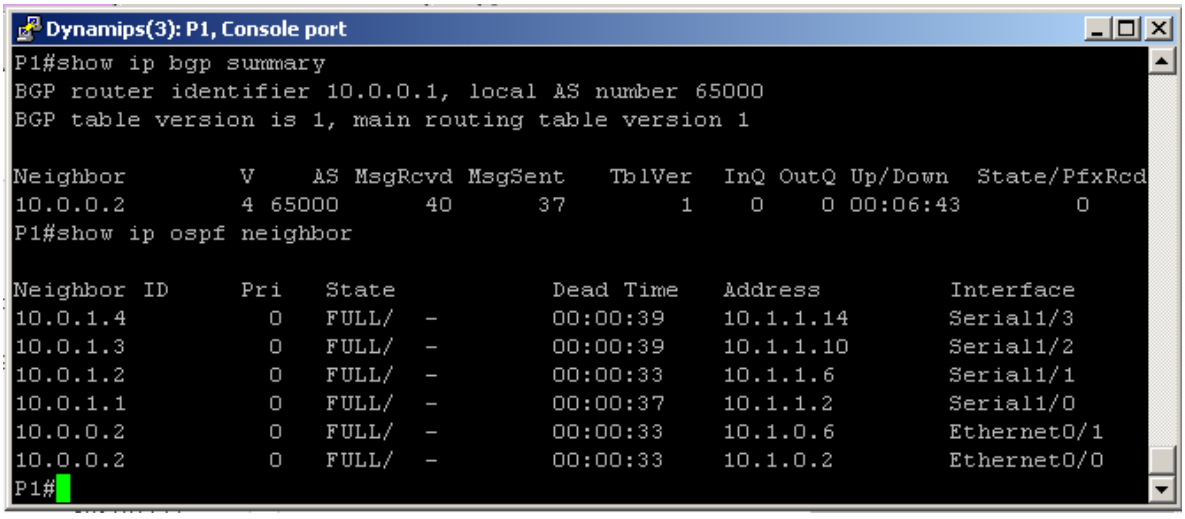


Figura 4. 12: Corrida del ruteo BGP en el Router P1

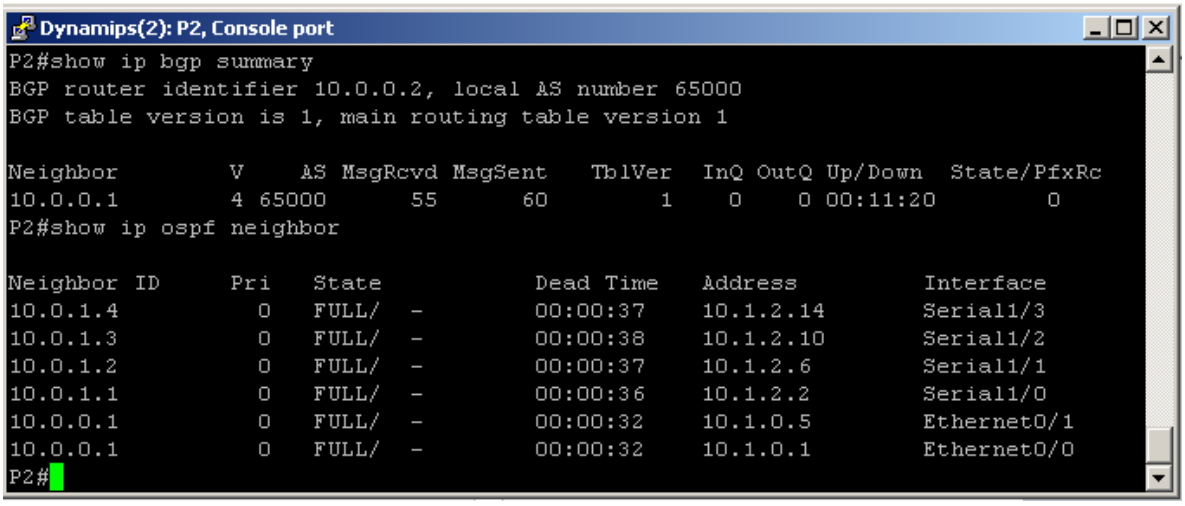


Figura 4. 13: Corrida del ruteo BGP en el Router P2

Verificamos la conectividad entre las VPNs con el comando “show ip verf brief” en los Routers PE para comprobar si la las interfaces están configuradas en el VRF correcto.

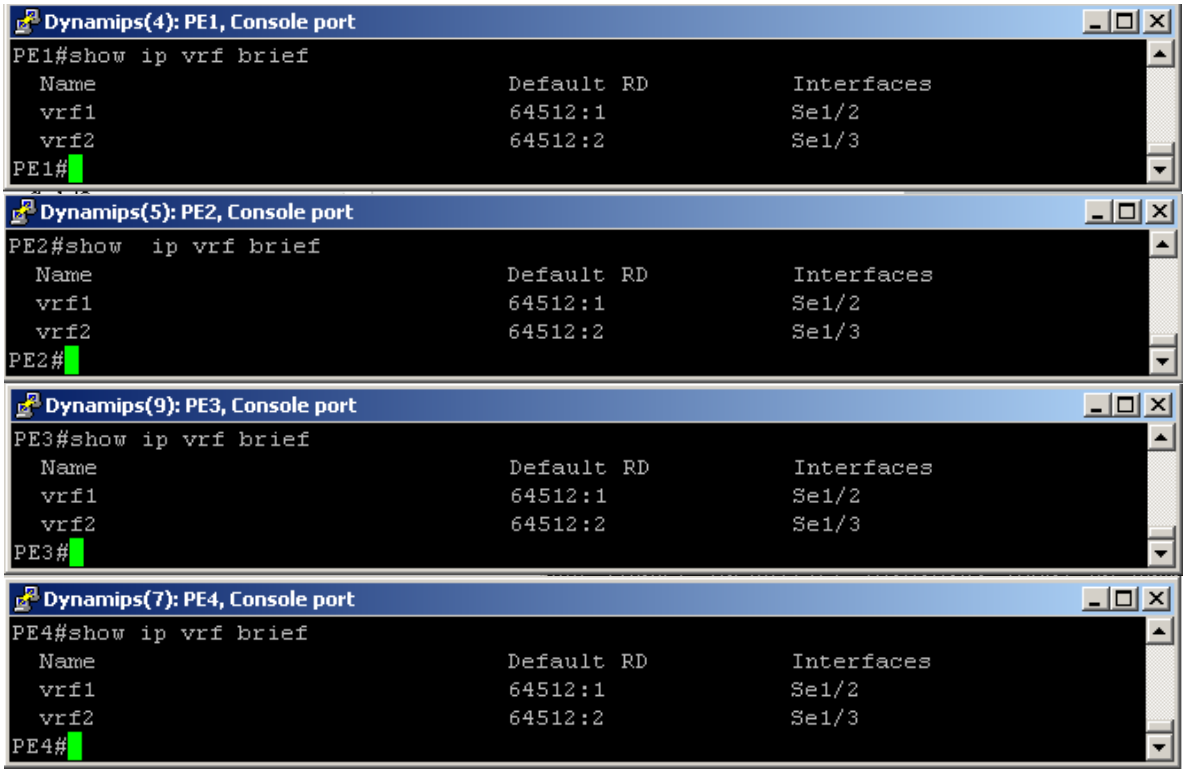
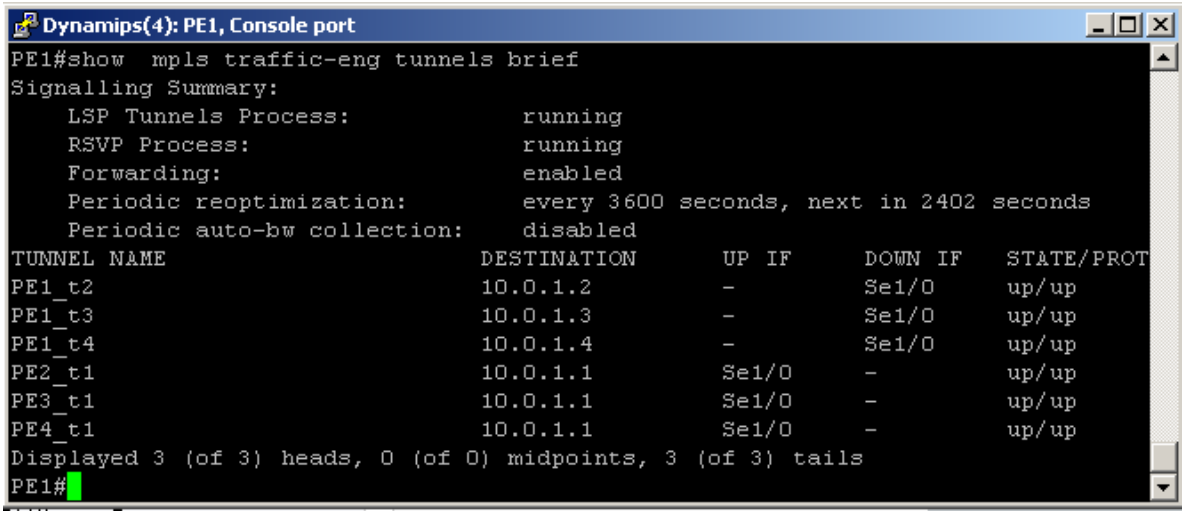
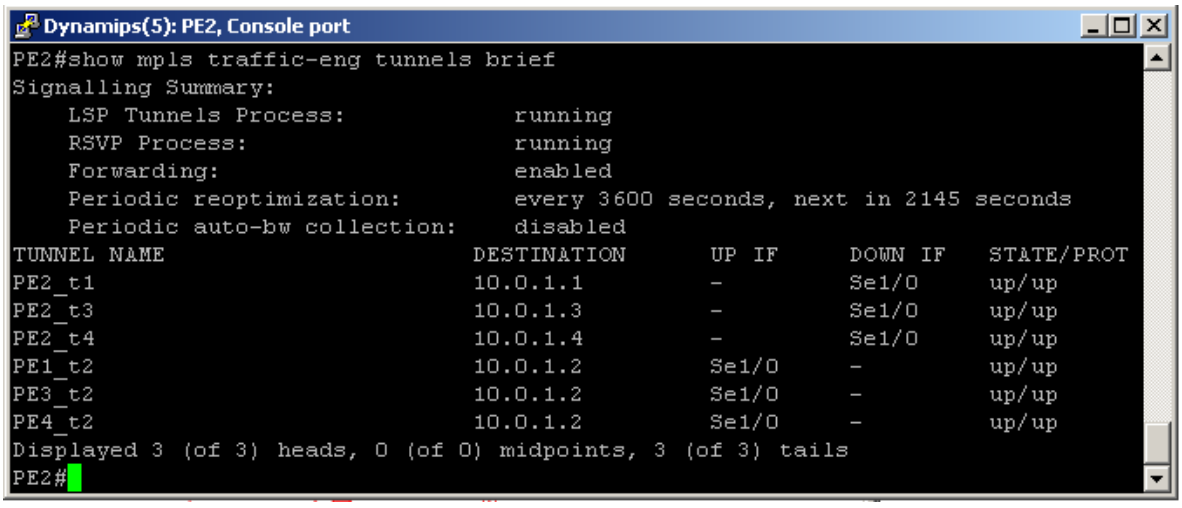


Figura 4. 14: Verificación de las interfaces con VRF

Los Routers PE establecen Ingeniería de tráfico de túneles MPLS para enrutar el tráfico. Se lo usa básicamente para reducir el costo en los enlaces WAN, ya que permite al proveedor de comunicaciones enrutar el tráfico de red de tal manera que pueda ofrecer mejor servicio a los clientes en términos de retrasos, redundancia y rendimiento.

Con el comando “show mpls traffic-eng tunnels brief” en cada uno de los Routers PE comprobamos si los túneles de ingeniería de tráfico son creados en ambos sentidos, de manera adecuada:





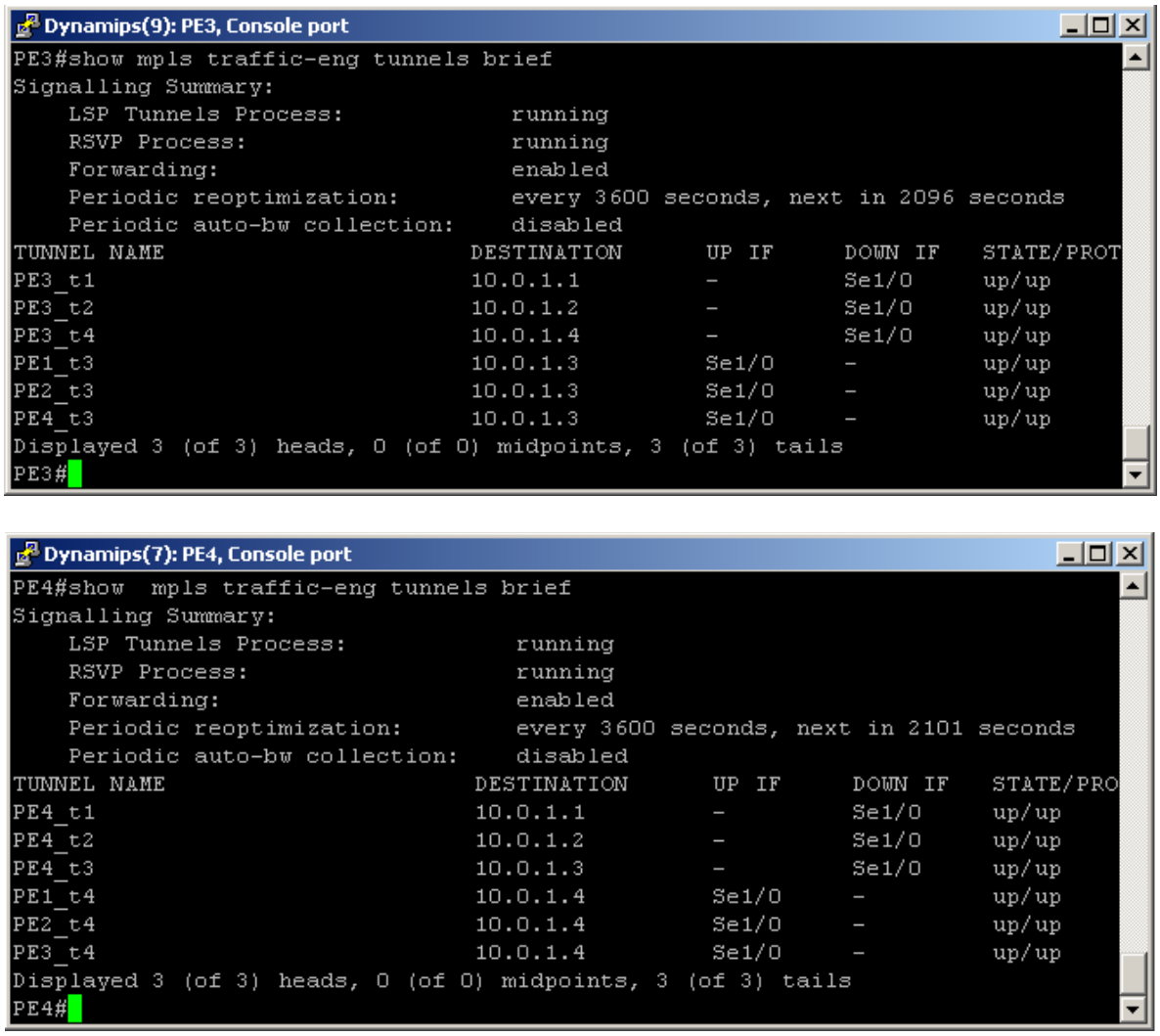
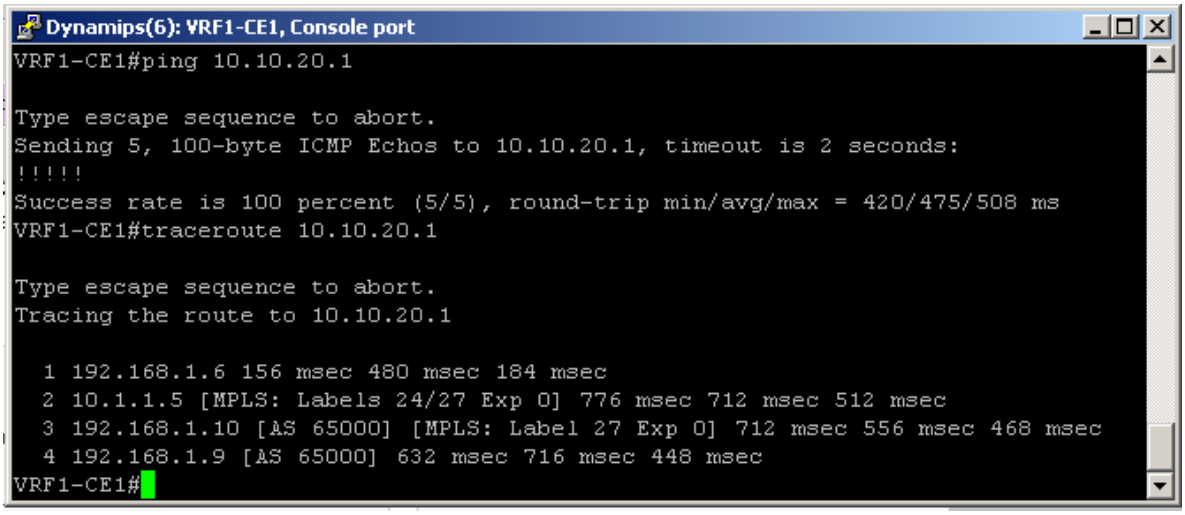
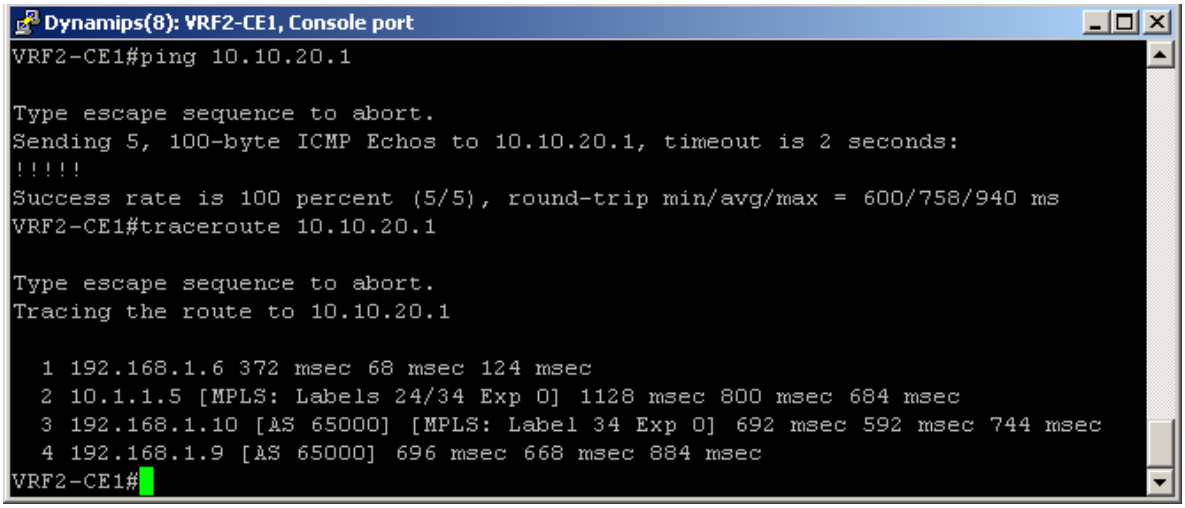
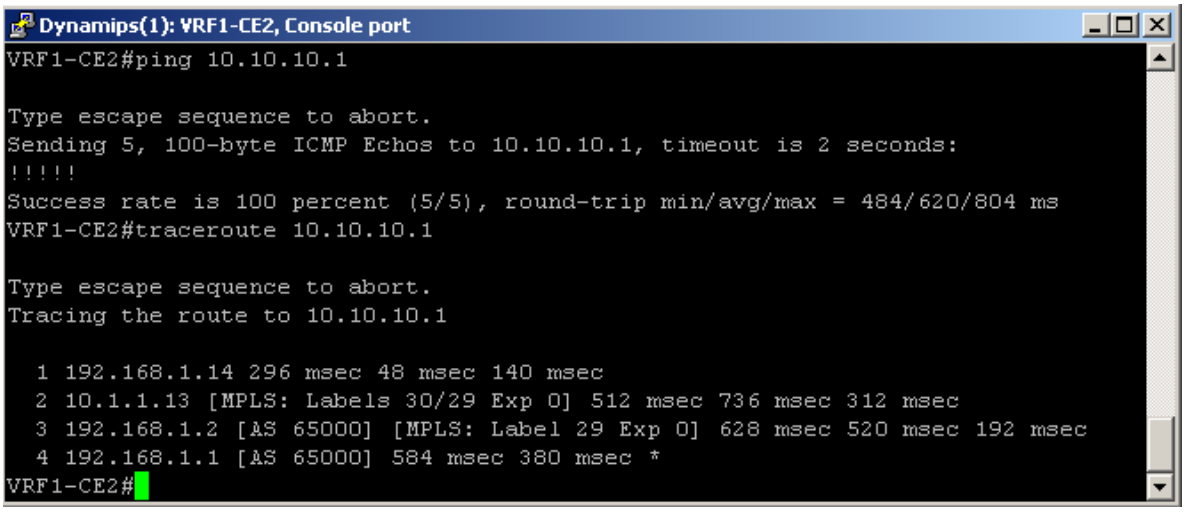


Figura 4. 15: Comprobación de túneles de ingeniería de tráfico en los Routers PE1, PE2, PE3 y PE4

Para comprobar la conexión entre las VPNs hacemos ping y traceroute de la dirección remota en los dos sentidos, donde vemos los pocos saltos que hacen para atravesar la nube MPLS y podemos ver la etiqueta asignada al paquete:


Dynamips(6): VRF1-CE1, Console port
VRF1-CE1#ping 10.10.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 420/475/508 ms
VRF1-CE1#traceroute 10.10.20.1
Type escape sequence to abort.
Tracing the route to 10.10.20.1
1 192.168.1.6 156 msec 480 msec 184 msec
2 10.1.1.5 [MPLS: Labels 24/27 Exp 0] 776 msec 712 msec 512 msec
3 192.168.1.10 [AS 65000] [MPLS: Label 27 Exp 0] 712 msec 556 msec 468 msec
4 192.168.1.9 [AS 65000] 632 msec 716 msec 448 msec
VRF1-CE1#


Dynamips(8): VRF2-CE1, Console port
VRF2-CE1#ping 10.10.20.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.20.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 600/758/940 ms
VRF2-CE1#traceroute 10.10.20.1
Type escape sequence to abort.
Tracing the route to 10.10.20.1
1 192.168.1.6 372 msec 68 msec 124 msec
2 10.1.1.5 [MPLS: Labels 24/34 Exp 0] 1128 msec 800 msec 684 msec
3 192.168.1.10 [AS 65000] [MPLS: Label 34 Exp 0] 692 msec 592 msec 744 msec
4 192.168.1.9 [AS 65000] 696 msec 668 msec 884 msec
VRF2-CE1#


Dynamips(1): VRF1-CE2, Console port
VRF1-CE2#ping 10.10.10.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.10.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 484/620/804 ms
VRF1-CE2#traceroute 10.10.10.1
Type escape sequence to abort.
Tracing the route to 10.10.10.1
1 192.168.1.14 296 msec 48 msec 140 msec
2 10.1.1.13 [MPLS: Labels 30/29 Exp 0] 512 msec 736 msec 312 msec
3 192.168.1.2 [AS 65000] [MPLS: Label 29 Exp 0] 628 msec 520 msec 192 msec
4 192.168.1.1 [AS 65000] 584 msec 380 msec *
VRF1-CE2#

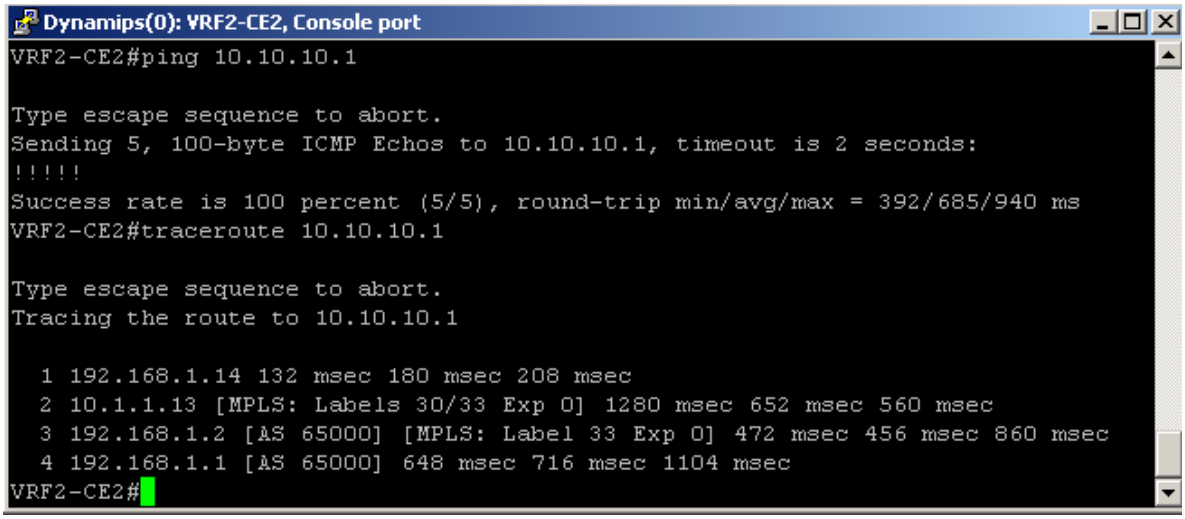
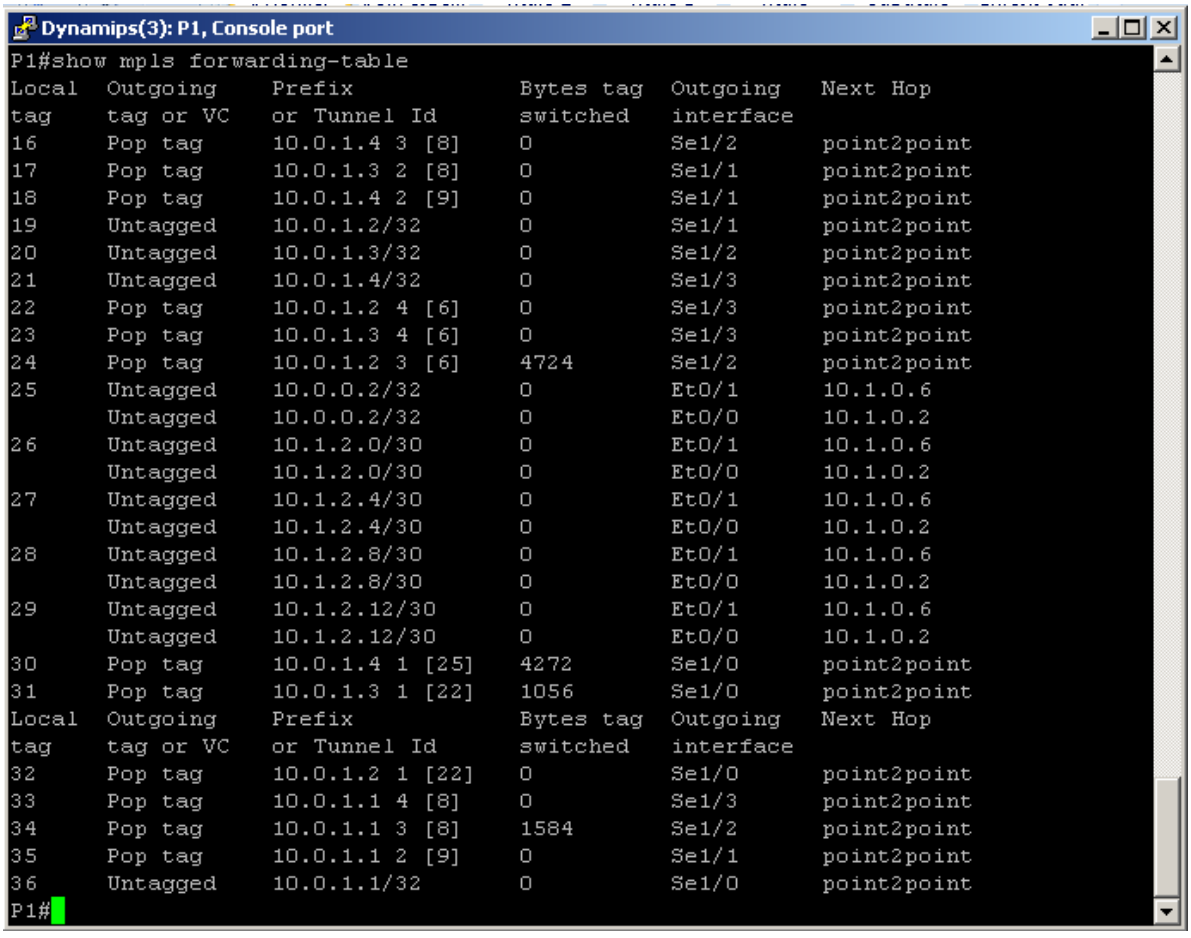


Figura 4. 16: Verificación del estado de conexión

Para mirar la tabla de reenvío MPLS solo necesitamos poner el comando “show mpls forwarding-table”, el cual también muestra las etiquetas asignadas y los next hops.



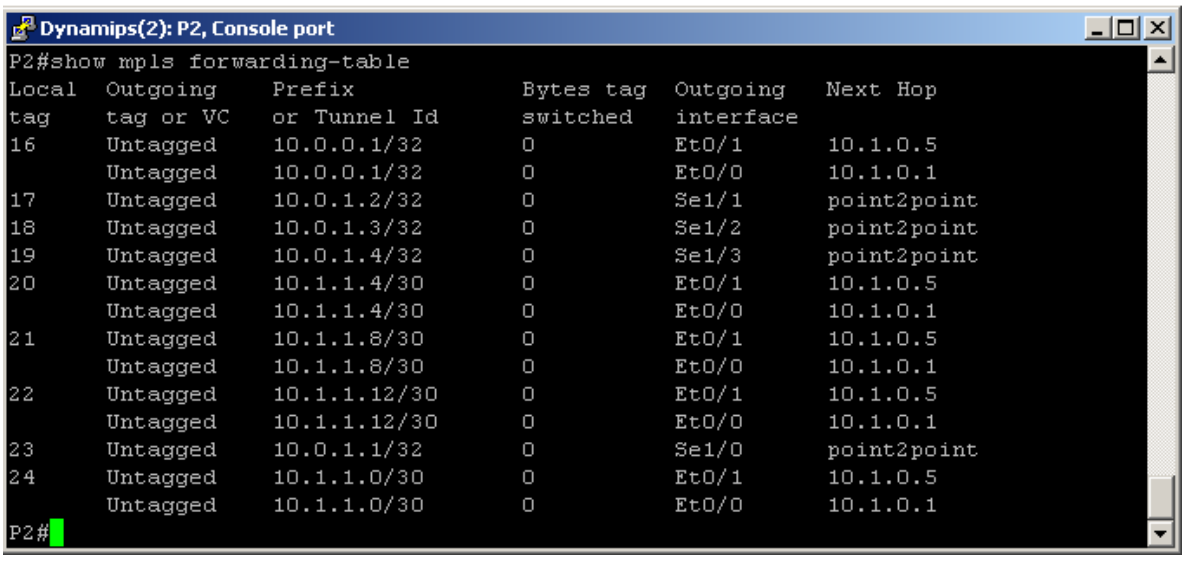


Figura 4. 17: Tabla de reenvío MPLS en los Router P1 y P2

Para poder ver las interfaces que se encuentran operativas con MPLS usamos el comando “show mpls interfaces”.

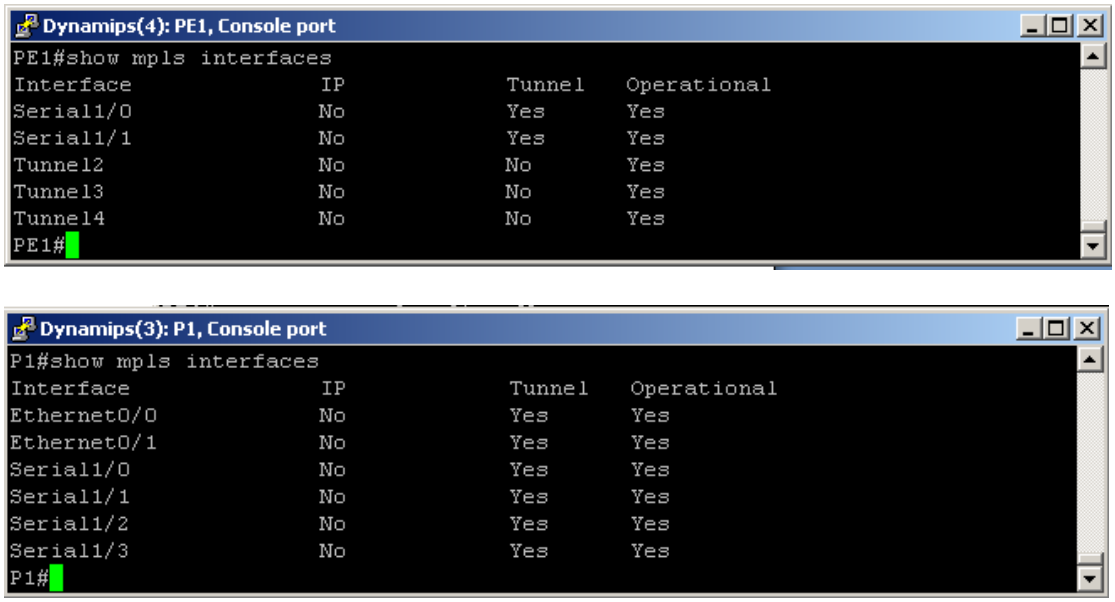


Figura 4. 18: Verificación del estado de las interfaces con MPLS

Para ver la tabla de etiquetas que está usando el Router se ejecuta el comando “show mpls ldp bindings”:

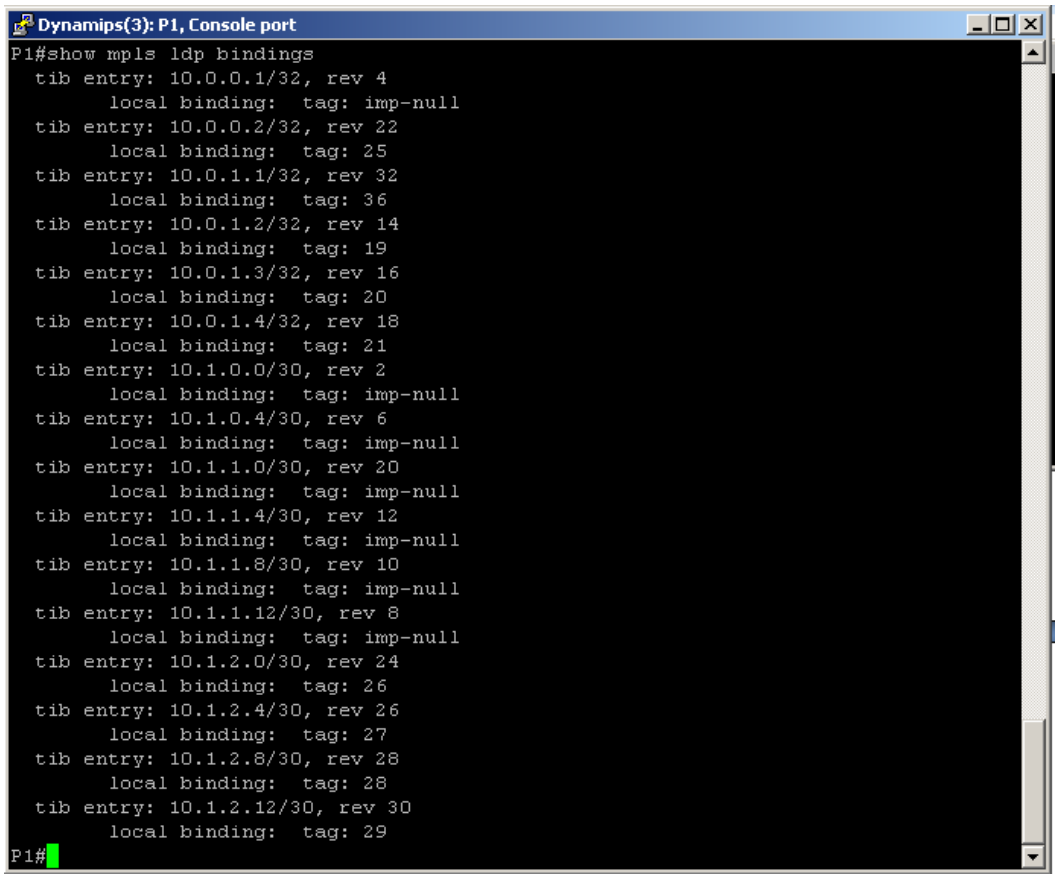


Figura 4. 19: Tabla de etiquetas

Como se ve en las pantallas capturadas de las consolas de los Routers de la red MPLS, se encuentra totalmente funcional, corriendo con VPNs para los clientes. Además tiene funcional redundante, por lo que si se produce alguna falla en un Router o en un enlace dentro de la nube MPLS, el servicio no se pierde y es automáticamente levantada su funcionalidad a través de otro camino o túnel.

4.3.3 Startup-config de los Routers de la implementación MPLS

P1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname P1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$fabT$1ZHprjtAiwxCFT0ald/sl0
!
no aaa new-model
memory-size iomem 5
no ip source-route
!
ip cef
no ip domain lookup
!
no ip bootp server
mpls traffic-eng tunnels
!
```

```
interface Loopback0
ip address 10.0.0.1 255.255.255.255
!
interface Ethernet0/0
description Connected to P2 E0/0
ip address 10.1.0.1 255.255.255.252
ip ospf network point-to-point
half-duplex
mpls traffic-eng tunnels
!
interface Ethernet0/1
description Connected to P2 E0/1
ip address 10.1.0.5 255.255.255.252
ip ospf network point-to-point
half-duplex
mpls traffic-eng tunnels
!
interface Ethernet0/2
no ip address
shutdown
half-duplex
!
interface Ethernet0/3
no ip address
```

```
shutdown
half-duplex
!
interface Serial1/0
description Connected to PE1 S1/0
ip address 10.1.1.1 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/1
description Connected to PE2 S1/0
ip address 10.1.1.5 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/2
description Connected to PE3 S1/0
ip address 10.1.1.9 255.255.255.252
```

```
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/3
description Connected to PE4 S1/0
ip address 10.1.1.13 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
router ospf 65000
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
router-id 10.0.0.1
log-adjacency-changes
network 10.0.0.1 0.0.0.0 area 0
network 10.1.0.0 0.0.0.7 area 0
network 10.1.1.0 0.0.0.15 area 0
!
```

```
router bgp 65000
bgp router-id 10.0.0.1
bgp log-neighbor-changes
timers bgp 12 36
neighbor MPLS peer-group
neighbor MPLS remote-as 65000
neighbor MPLS update-source Loopback0
neighbor 10.0.0.2 remote-as 65000
neighbor 10.0.0.2 update-source Loopback0
neighbor 10.0.1.1 peer-group MPLS
neighbor 10.0.1.2 peer-group MPLS
neighbor 10.0.1.3 peer-group MPLS
neighbor 10.0.1.4 peer-group MPLS
!
address-family ipv4
neighbor 10.0.0.2 activate
neighbor 10.0.0.2 send-community extended
no neighbor 10.0.1.1 activate
no neighbor 10.0.1.2 activate
no neighbor 10.0.1.3 activate
no neighbor 10.0.1.4 activate
no auto-summary
no synchronization
exit-address-family
```

```
!
address-family vpnv4
neighbor MPLS send-community extended
neighbor MPLS route-reflector-client
neighbor 10.0.1.1 activate
neighbor 10.0.1.2 activate
neighbor 10.0.1.3 activate
neighbor 10.0.1.4 activate
exit-address-family
!
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
password 7 02050D480809
logging synchronous
login
line aux 0
```

exec-timeout 0 1

login local

no exec

line vty 0 4

password 7 070C285F4D06

login

!

end

P2

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname P2

!

boot-start-marker

boot-end-marker

!

enable secret 5 $1$6aKP$fWgtlKgDseFwmWhCBt63K.

!

no aaa new-model

memory-size iomem 5

```
no ip source-route
!
ip cef
no ip domain lookup
!
no ip bootp server
mpls traffic-eng tunnels
!
interface Loopback0
ip address 10.0.0.2 255.255.255.255
!
interface Ethernet0/0
description Connected to P1 E0/0
ip address 10.1.0.2 255.255.255.252
ip ospf network point-to-point
half-duplex
mpls traffic-eng tunnels
!
interface Ethernet0/1
description Connected to P1 E0/1
ip address 10.1.0.6 255.255.255.252
ip ospf network point-to-point
half-duplex
mpls traffic-eng tunnels
```

```
!
interface Ethernet0/2
no ip address
shutdown
half-duplex
!
interface Ethernet0/3
no ip address
shutdown
half-duplex
!
interface Serial1/0
description Connected to PE1 S1/1
ip address 10.1.2.1 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/1
description Connected to PE2 S1/1
ip address 10.1.2.5 255.255.255.252
encapsulation ppp
```

```
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/2
description Connected to PE3 S1/1
ip address 10.1.2.9 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/3
description Connected to PE4 S1/1
ip address 10.1.2.13 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
router ospf 65000
```

```
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
router-id 10.0.0.2
log-adjacency-changes
network 10.0.0.2 0.0.0.0 area 0
network 10.1.0.0 0.0.0.7 area 0
network 10.1.2.0 0.0.0.15 area 0
!
router bgp 65000
bgp router-id 10.0.0.2
bgp log-neighbor-changes
timers bgp 12 36
neighbor MPLS peer-group
neighbor MPLS remote-as 65000
neighbor MPLS update-source Loopback0
neighbor 10.0.0.1 remote-as 65000
neighbor 10.0.0.1 update-source Loopback0
neighbor 10.0.1.1 peer-group MPLS
neighbor 10.0.1.2 peer-group MPLS
neighbor 10.0.1.3 peer-group MPLS
neighbor 10.0.1.4 peer-group MPLS
!
address-family ipv4
neighbor 10.0.0.1 activate
```

```
neighbor 10.0.0.1 send-community extended
no neighbor 10.0.1.1 activate
no neighbor 10.0.1.2 activate
no neighbor 10.0.1.3 activate
no neighbor 10.0.1.4 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor MPLS send-community extended
neighbor MPLS route-reflector-client
neighbor 10.0.1.1 activate
neighbor 10.0.1.2 activate
neighbor 10.0.1.3 activate
neighbor 10.0.1.4 activate
exit-address-family
!
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
```

!

line con 0

exec-timeout 5 0

privilege level 15

password 7 110A1016141D

logging synchronous

login

line aux 0

exec-timeout 0 1

login local

no exec

line vty 0 4

password 7 14141B180F0B

login

!

end

PE1

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname PE1

```
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$nu6K$cJ47rd56IrhxH/e6sE6ym.
!
no aaa new-model
memory-size iomem 5
no ip source-route
!
ip cef
no ip domain lookup
!
ip vrf vrf1
rd 64512:1
route-target export 64512:1
route-target import 64512:1
!
ip vrf vrf2
rd 64512:2
route-target export 64512:2
route-target import 64512:2
!
no ip bootp server
```

```
mpls traffic-eng tunnels
!
interface Loopback0
ip address 10.0.1.1 255.255.255.255
!
interface Tunnel2
ip unnumbered Loopback0
tunnel destination 10.0.1.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 2 dynamic
no routing dynamic
!
interface Tunnel3
ip unnumbered Loopback0
tunnel destination 10.0.1.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 3 dynamic
no routing dynamic
!
interface Tunnel4
ip unnumbered Loopback0
tunnel destination 10.0.1.4
```

```
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 4 dynamic
no routing dynamic
!
interface Ethernet0/0
no ip address
shutdown
half-duplex
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Ethernet0/2
no ip address
shutdown
half-duplex
!
interface Ethernet0/3
no ip address
shutdown
half-duplex
```

```
!
interface Serial1/0
description Connected to P1 S1/0
ip address 10.1.1.2 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/1
description Connected to P2 S1/0
ip address 10.1.2.2 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/2
description Connected to VRF1-CE1 S1/0
ip vrf forwarding vrf1
ip address 192.168.1.2 255.255.255.252
encapsulation ppp
```

```
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/3
description Connected to VRF2-CE1 S1/0
ip vrf forwarding vrf2
ip address 192.168.1.2 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
router ospf 65000
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
router-id 10.0.1.1
log-adjacency-changes
network 10.0.1.1 0.0.0.0 area 0
network 10.1.1.2 0.0.0.0 area 0
network 10.1.2.2 0.0.0.0 area 0
!
router bgp 65000
bgp router-id 10.0.1.1
bgp log-neighbor-changes
timers bgp 12 36
```

```
neighbor MPLS peer-group
neighbor MPLS remote-as 65000
neighbor MPLS update-source Loopback0
neighbor 10.0.0.1 peer-group MPLS
neighbor 10.0.0.2 peer-group MPLS
!
address-family ipv4
neighbor MPLS send-community extended
no neighbor 10.0.0.1 activate
no neighbor 10.0.0.2 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor MPLS send-community extended
neighbor 10.0.0.1 activate
neighbor 10.0.0.2 activate
exit-address-family
!
address-family ipv4 vrf vrf2
neighbor 192.168.1.1 remote-as 64512
neighbor 192.168.1.1 activate
neighbor 192.168.1.1 as-override
```

```
maximum-paths 2
no synchronization
exit-address-family
!
address-family ipv4 vrf vrf1
neighbor 192.168.1.1 remote-as 64512
neighbor 192.168.1.1 activate
neighbor 192.168.1.1 as-override
maximum-paths 2
no synchronization
exit-address-family
!
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
password 7 121A0C041104
logging synchronous
```

login

line aux 0

exec-timeout 0 1

login local

no exec

line vty 0 4

password 7 0822455D0A16

login

!

end

PE2

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname PE2

!

boot-start-marker

boot-end-marker

!

enable secret 5 1qGa5$mgi6mdn3pjakk1niKvRNn1

!

```
no aaa new-model
memory-size iomem 5
no ip source-route
!
ip cef
no ip domain lookup
!
ip vrf vrf1
rd 64512:1
route-target export 64512:1
route-target import 64512:1
!
ip vrf vrf2
rd 64512:2
route-target export 64512:2
route-target import 64512:2
!
no ip bootp server
mpls traffic-eng tunnels
!
interface Loopback0
ip address 10.0.1.2 255.255.255.255
!
interface Tunnel1
```

```
ip unnumbered Loopback0
tunnel destination 10.0.1.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 1 dynamic
no routing dynamic
!
interface Tunnel3
ip unnumbered Loopback0
tunnel destination 10.0.1.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 3 dynamic
no routing dynamic
!
interface Tunnel4
ip unnumbered Loopback0
tunnel destination 10.0.1.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 4 dynamic
no routing dynamic
!
interface Ethernet0/0
```

```
no ip address
shutdown
half-duplex
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Ethernet0/2
no ip address
shutdown
half-duplex
!
interface Ethernet0/3
no ip address
shutdown
half-duplex
!
interface Serial1/0
description Connected to P1 S1/1
ip address 10.1.1.6 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
```

```
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/1
description Connected to P2 S1/1
ip address 10.1.2.6 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/2
description Connected to VRF1-CE1 S1/1
ip vrf forwarding vrf1
ip address 192.168.1.6 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/3
description Connected to VRF2-CE1 S1/1
ip vrf forwarding vrf2
```

```
ip address 192.168.1.6 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
router ospf 65000
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
router-id 10.0.1.2
log-adjacency-changes
network 10.0.1.2 0.0.0.0 area 0
network 10.1.1.6 0.0.0.0 area 0
network 10.1.2.6 0.0.0.0 area 0
!
router bgp 65000
bgp router-id 10.0.1.2
bgp log-neighbor-changes
timers bgp 12 36
neighbor MPLS peer-group
neighbor MPLS remote-as 65000
neighbor MPLS update-source Loopback0
neighbor 10.0.0.1 peer-group MPLS
neighbor 10.0.0.2 peer-group MPLS
!
```

```
address-family ipv4
neighbor MPLS send-community extended
no neighbor 10.0.0.1 activate
no neighbor 10.0.0.2 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor MPLS send-community extended
neighbor 10.0.0.1 activate
neighbor 10.0.0.2 activate
exit-address-family
!
address-family ipv4 vrf vrf2
neighbor 192.168.1.5 remote-as 64512
neighbor 192.168.1.5 activate
neighbor 192.168.1.5 as-override
maximum-paths 2
no synchronization
exit-address-family
!
address-family ipv4 vrf vrf1
neighbor 192.168.1.5 remote-as 64512
```

```
neighbor 192.168.1.5 activate
neighbor 192.168.1.5 as-override
maximum-paths 2
no synchronization
exit-address-family
!
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
password 7 045802150C2E
logging synchronous
login
line aux 0
exec-timeout 0 1
login local
no exec
line vty 0 4
```

password 7 110A1016141D

login

!

end

PE3

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname PE3

!

boot-start-marker

boot-end-marker

!

enable secret 5 1LHCF$DGlKckgWtI3y5GssmAVOD1

!

no aaa new-model

memory-size iomem 5

no ip source-route

!

ip cef

no ip domain lookup

```
!
ip vrf vrf1
rd 64512:1
route-target export 64512:1
route-target import 64512:1
!
ip vrf vrf2
rd 64512:2
route-target export 64512:2
route-target import 64512:2
!
no ip bootp server
mpls traffic-eng tunnels
!
interface Loopback0
ip address 10.0.1.3 255.255.255.255
!
interface Tunnel1
ip unnumbered Loopback0
tunnel destination 10.0.1.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 1 dynamic
no routing dynamic
```

```
!
interface Tunnel2
ip unnumbered Loopback0
tunnel destination 10.0.1.2
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 2 dynamic
no routing dynamic
!
interface Tunnel4
ip unnumbered Loopback0
tunnel destination 10.0.1.4
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 4 dynamic
no routing dynamic
!
interface Ethernet0/0
no ip address
shutdown
half-duplex
!
interface Ethernet0/1
no ip address
```

```
shutdown
half-duplex
!
interface Ethernet0/2
no ip address
shutdown
half-duplex
!
interface Ethernet0/3
no ip address
shutdown
half-duplex
!
interface Serial1/0
description Connected to P1 S1/2
ip address 10.1.1.10 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/1
description Connected to P2 S1/2
```

```
ip address 10.1.2.10 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/2
description Connected to VRF1-CE2 S1/0
ip vrf forwarding vrf1
ip address 192.168.1.10 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/3
description Connected to VRF2-CE2 S1/0
ip vrf forwarding vrf2
ip address 192.168.1.10 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
router ospf 65000
```

```
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
router-id 10.0.1.3
log-adjacency-changes
network 10.0.1.3 0.0.0.0 area 0
network 10.1.1.10 0.0.0.0 area 0
network 10.1.2.10 0.0.0.0 area 0
!
router bgp 65000
bgp router-id 10.0.1.3
bgp log-neighbor-changes
timers bgp 12 36
neighbor MPLS peer-group
neighbor MPLS remote-as 65000
neighbor MPLS update-source Loopback0
neighbor 10.0.0.1 peer-group MPLS
neighbor 10.0.0.2 peer-group MPLS
!
address-family ipv4
neighbor MPLS send-community extended
no neighbor 10.0.0.1 activate
no neighbor 10.0.0.2 activate
no auto-summary
no synchronization
```

```
exit-address-family
!
address-family vpnv4
neighbor MPLS send-community extended
neighbor 10.0.0.1 activate
neighbor 10.0.0.2 activate
exit-address-family
!
address-family ipv4 vrf vrf2
neighbor 192.168.1.9 remote-as 64512
neighbor 192.168.1.9 activate
neighbor 192.168.1.9 as-override
maximum-paths 2
no synchronization
exit-address-family
!
address-family ipv4 vrf vrf1
neighbor 192.168.1.9 remote-as 64512
neighbor 192.168.1.9 activate
neighbor 192.168.1.9 as-override
maximum-paths 2
no synchronization
exit-address-family
!
```

```
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
password 7 1511021F0725
logging synchronous
login
line aux 0
exec-timeout 0 1
login local
no exec
line vty 0 4
password 7 094F471A1A0A
login
!
end
```

PE4

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname PE4
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$TMf3$8679kumpGppr8ExFrnpK1/
!
no aaa new-model
memory-size iomem 5
no ip source-route
!
ip cef
no ip domain lookup
!
!
ip vrf vrf1
rd 64512:1
route-target export 64512:1
```

```
route-target import 64512:1
!
ip vrf vrf2
rd 64512:2
route-target export 64512:2
route-target import 64512:2
!
no ip bootp server
mpls traffic-eng tunnels
!
interface Loopback0
ip address 10.0.1.4 255.255.255.255
!
interface Tunnel1
ip unnumbered Loopback0
tunnel destination 10.0.1.1
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 1 dynamic
no routing dynamic
!
interface Tunnel2
ip unnumbered Loopback0
tunnel destination 10.0.1.2
```

```
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 2 dynamic
no routing dynamic
!
interface Tunnel3
ip unnumbered Loopback0
tunnel destination 10.0.1.3
tunnel mode mpls traffic-eng
tunnel mpls traffic-eng autoroute announce
tunnel mpls traffic-eng path-option 3 dynamic
no routing dynamic
!
interface Ethernet0/0
no ip address
shutdown
half-duplex
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Ethernet0/2
```

```
no ip address
shutdown
half-duplex
!
interface Ethernet0/3
no ip address
shutdown
half-duplex
!
interface Serial1/0
description Connected to P1 S1/3
ip address 10.1.1.14 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/1
description Connected to P2 S1/3
ip address 10.1.2.14 255.255.255.252
encapsulation ppp
ip ospf network point-to-point
mpls traffic-eng tunnels
```

```
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/2
description Connected to VRF1-CE2 S1/1
ip vrf forwarding vrf1
ip address 192.168.1.14 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/3
description Connected to VRF2-CE2 S1/1
ip vrf forwarding vrf2
ip address 192.168.1.14 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
router ospf 65000
mpls traffic-eng router-id Loopback0
mpls traffic-eng area 0
router-id 10.0.1.4
log-adjacency-changes
```

```
network 10.0.1.4 0.0.0.0 area 0
network 10.1.1.14 0.0.0.0 area 0
network 10.1.2.14 0.0.0.0 area 0
!
router bgp 65000
bgp router-id 10.0.1.4
bgp log-neighbor-changes
timers bgp 12 36
neighbor MPLS peer-group
neighbor MPLS remote-as 65000
neighbor MPLS update-source Loopback0
neighbor 10.0.0.1 peer-group MPLS
neighbor 10.0.0.2 peer-group MPLS
!
address-family ipv4
neighbor MPLS send-community extended
no neighbor 10.0.0.1 activate
no neighbor 10.0.0.2 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpnv4
neighbor MPLS send-community extended
```

```
neighbor 10.0.0.1 activate
neighbor 10.0.0.2 activate
exit-address-family
!
address-family ipv4 vrf vrf2
neighbor 192.168.1.13 remote-as 64512
neighbor 192.168.1.13 activate
neighbor 192.168.1.13 as-override
maximum-paths 2
no synchronization
exit-address-family
!
address-family ipv4 vrf vrf1
neighbor 192.168.1.13 remote-as 64512
neighbor 192.168.1.13 activate
neighbor 192.168.1.13 as-override
maximum-paths 2
no synchronization
exit-address-family
!
no ip http server
no ip http secure-server
!
no cdp run
```

!

control-plane

!

line con 0

exec-timeout 5 0

privilege level 15

password 7 070C285F4D06

logging synchronous

login

line aux 0

exec-timeout 0 1

login local

no exec

line vty 0 4

password 7 060506324F41

login

!

end

VRF1-C1

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

```
!
hostname VRF1-CE1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$TlJa$gZuE3jHfp6NnVSEfI/LpK.
!
no aaa new-model
memory-size iomem 5
no ip source-route
!
ip cef
no ip domain lookup
!
!
no ip bootp server
!
interface Loopback0
ip address 10.255.0.1 255.255.255.255
!
interface Ethernet0/0
ip address 10.10.10.1 255.255.255.0
half-duplex
```

```
no keepalive
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Ethernet0/2
no ip address
shutdown
half-duplex
!
interface Ethernet0/3
no ip address
shutdown
half-duplex
!
interface Serial1/0
description Connected to PE1 S1/2
ip address 192.168.1.1 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
```

```
interface Serial1/1
description Connected to PE2 S1/2
ip address 192.168.1.5 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
router bgp 64512
no synchronization
bgp log-neighbor-changes
timers bgp 12 36
redistribute connected
neighbor 192.168.1.2 remote-as 65000
neighbor 192.168.1.6 remote-as 65000
```

```
no auto-summary
!
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
password 7 070C285F4D06
logging synchronous
login
line aux 0
exec-timeout 0 1
login local
no exec
line vty 0 4
password 7 14141B180F0B
login
!
end
```

VRF2-C1

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname VRF2-CE1
!
boot-start-marker
boot-end-marker
!
enable secret 5 $1$XJlN$tmY3Xb1yxkN.Fmf3YM1Rs0
!
no aaa new-model
memory-size iomem 5
no ip source-route
!
ip cef
no ip domain lookup
!
no ip bootp server
!
interface Loopback0
```

```
ip address 10.255.0.1 255.255.255.255
!
interface Ethernet0/0
ip address 10.10.10.1 255.255.255.0
half-duplex
no keepalive
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Ethernet0/2
no ip address
shutdown
half-duplex
!
interface Ethernet0/3
no ip address
shutdown
half-duplex
!
interface Serial1/0
description Connected to PE1 S1/3
```

```
ip address 192.168.1.1 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
no fair-queue
!
interface Serial1/1
description Connected to PE1 S1/3
ip address 192.168.1.5 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
router bgp 64512
```

```
no synchronization
bgp log-neighbor-changes
timers bgp 12 36
redistribute connected
neighbor 192.168.1.2 remote-as 65000
neighbor 192.168.1.6 remote-as 65000
no auto-summary
!
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
password 7 05080F1C2243
logging synchronous
login
line aux 0
exec-timeout 0 1
login local
```

no exec

line vty 0 4

password 7 14141B180F0B

login

!

end

VRF1-C2

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname VRF1-CE2

!

boot-start-marker

boot-end-marker

!

enable secret 5 1t/.y$XkbRjbgYZG1Y87IqMABO11

!

no aaa new-model

memory-size iomem 5

no ip source-route

!

```
ip cef
no ip domain lookup
!
no ip bootp server
!
interface Loopback0
ip address 10.255.0.2 255.255.255.255
!
interface Ethernet0/0
ip address 10.10.20.1 255.255.255.0
half-duplex
no keepalive
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Ethernet0/2
no ip address
shutdown
half-duplex
!
interface Ethernet0/3
```

```
no ip address
shutdown
half-duplex
!
interface Serial1/0
description Connected to PE3 S1/2
ip address 192.168.1.9 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/1
description Connected to PE4 S1/2
ip address 192.168.1.13 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/2
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
```

```
no ip address
shutdown
serial restart-delay 0
!
router bgp 64512
no synchronization
bgp log-neighbor-changes
timers bgp 12 36
redistribute connected
neighbor 192.168.1.10 remote-as 65000
neighbor 192.168.1.14 remote-as 65000
no auto-summary
!
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
!
line con 0
exec-timeout 5 0
privilege level 15
password 7 13061E010803
```

logging synchronous

login

line aux 0

exec-timeout 0 1

login local

no exec

line vty 0 4

password 7 02050D480809

login

!

end

VRF2-C2

version 12.4

service timestamps debug datetime msec

service timestamps log datetime msec

service password-encryption

!

hostname VRF2-CE2

!

boot-start-marker

boot-end-marker

!

enable secret 5 1rOFl$Y0dQqpUouqCq/j1uituEL/

```
!
no aaa new-model
memory-size iomem 5
no ip source-route
!
ip cef
no ip domain lookup
!
no ip bootp server
!
interface Loopback0
ip address 10.255.0.2 255.255.255.255
!
interface Ethernet0/0
ip address 10.10.20.1 255.255.255.0
half-duplex
no keepalive
!
interface Ethernet0/1
no ip address
shutdown
half-duplex
!
interface Ethernet0/2
```

```
no ip address
shutdown
half-duplex
!
interface Ethernet0/3
no ip address
shutdown
half-duplex
!
interface Serial1/0
description Connected to PE3 S1/3
ip address 192.168.1.9 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/1
description Connected to PE4 S1/3
ip address 192.168.1.13 255.255.255.252
encapsulation ppp
no peer neighbor-route
serial restart-delay 0
!
interface Serial1/2
```

```
no ip address
shutdown
serial restart-delay 0
!
interface Serial1/3
no ip address
shutdown
serial restart-delay 0
!
router bgp 64512
no synchronization
bgp log-neighbor-changes
timers bgp 12 36
redistribute connected
neighbor 192.168.1.10 remote-as 65000
neighbor 192.168.1.14 remote-as 65000
no auto-summary
!
no ip http server
no ip http secure-server
!
no cdp run
!
control-plane
```

```
!
line con 0
exec-timeout 5 0
privilege level 15
password 7 00071A150754
logging synchronous
login
line aux 0
exec-timeout 0 1
login local
no exec
line vty 0 4
password 7 1511021F0725
login
!
end
```

CAPÍTULO V

FACTIBILIDAD TÉCNICA Y ECONÓMICA

5.1 Factibilidad Técnica

Una vez que sea levantada la red MPLS y esté completamente funcional podemos darnos cuenta que la migración de una tecnología WAN antigua en este caso Frame Relay a MPLS se pudo realizar de manera satisfactoria, ya que MPLS es una tecnología innovadora que no depende en su totalidad del hardware para funcionar puesto que las operaciones las realiza por medio del software implementado en los Routers, en este caso de Cisco es el IOS (Internetwork Operating System).

Para implementar una red MPLS, se debe tener un software que permita levantar servicios MPLS en los Routers de la WAN. Para ello se debe realizar un Upgrade de software IOS del Router para que posea características MPLS, esto diferencia de hacer un Update, que es solo realizar una actualización del IOS ya embebido en el Router con una versión más actual.

Una red MPLS permite usar VPNs con mejor eficiencia que las que se pueden usar en tecnologías como IP, Frame Relay o ATM, ya que MPLS puede integrar diferentes tipos de tráfico sobre una sola infraestructura compartida, permitiendo al proveedor

ofrecer nuevos servicios a sus clientes. MPLS en especial crea túneles con diferentes tipos de tráfico.

Una infraestructura con MPLS permite manejar e integrar de mejor manera diferentes tipos de tráfico dentro de las trayectorias LSPs.

En la infraestructura implementada con MPLS evidenciamos que se puede integrar la tecnología MPLS con otras tecnologías de redes de transmisión de datos, optimizando gradualmente los recursos de estas redes, permitiendo mejoras en los tiempos de respuesta de las aplicaciones, en especial las aplicaciones de tiempo real.

Por lo tanto, MPLS representa una considerable reducción de costos mejorando el funcionamiento de la infraestructura de red. Además provee al cliente de grandes y mejores beneficios que los que ofrece una tecnología WAN convencional sola permitiendo una proyección a futuro debido a que es una tecnología escalable.

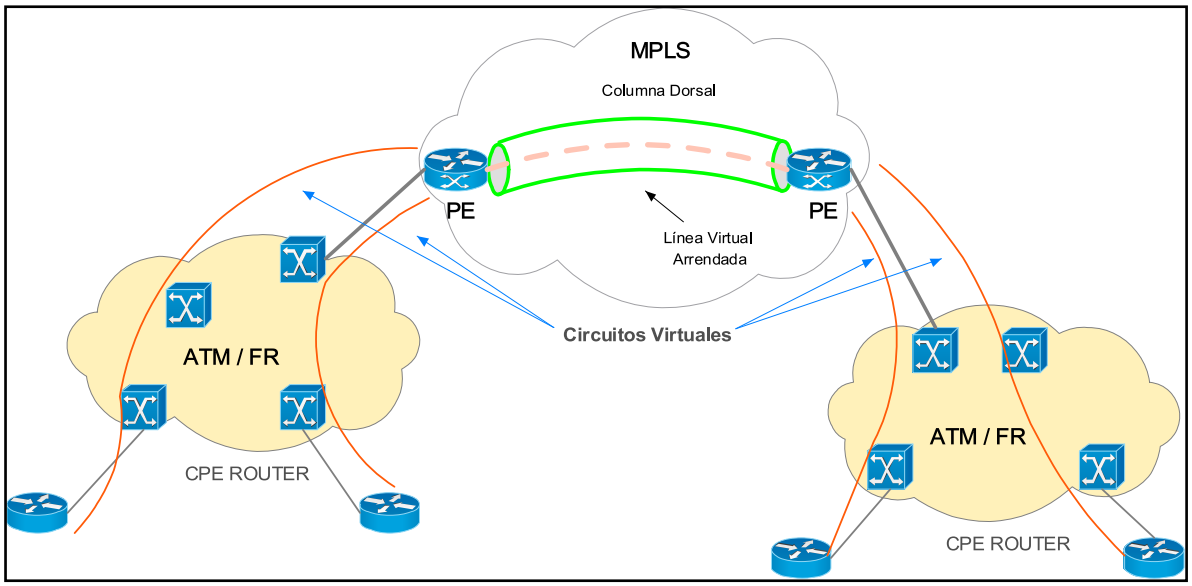


Figura 5. 1: ATM/Frame Relay sobre MPLS

MPLS surge como una óptima solución ya que supera las limitaciones de velocidad de ATM y el manejo de tráfico sensible de Frame Relay.

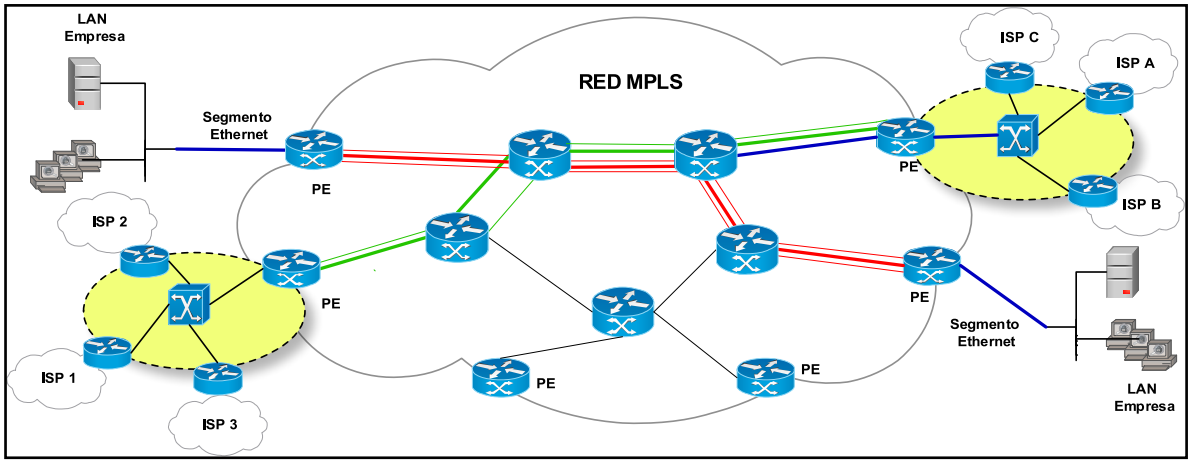


Figura 5. 2: IP sobre MPLS

Por todo esto, la tecnología MPLS proporciona beneficios tanto económicos como operativos en una solución empresarial mejorando la calidad de los servicios

proporcionados, solucionando problemas de retraso y compatibilidad con otras tecnologías.

5.1.1 Determinación de los requerimientos técnicos para la migración de la red

Para el diseño construido como ejemplo de una red MPLS en el capítulo anterior basamos el análisis en una red Frame Relay de un proveedor de servicio que se encarga de arrendar circuitos virtuales, dicha red funciona con Routers Cisco 3640 los cuales corren con software IOS (Sistema Operativo de Interconexión de Redes) Cisco IP c3640-i-mz.124-16 como sistema operativo del Router.

Este IOS Cisco necesita como características mínimas de memoria en el Router para funcionar, que el equipo tenga 64MB en DRAM y 16MB en FLASH.

Los Routers Cisco 3640 están diseñados como solución multiservicio para sucursales, escogidos principalmente por su flexibilidad, capacidad modular y alto rendimiento. Tienen como características técnicas las siguientes:

Características	Cisco 3640
Tipo de procesador	100-MHz IDT R4700 RISC
8 MB de memoria Flash	8 MB, ampliables a 32 MB
Memoria del sistema	16 MB DRAM, ampliables a 128 MB DRAM
Ranuras para módulos de red	Cuatro ranuras

Ethernet incorporado	No (utiliza módulo)
Alimentación	Corriente alterna o continua
Sistemas de alimentación redundantes	Sí, externos
Dimensiones (Al x An x Pr)	3,44 x 17,5 x 15,75 pulgadas
Rendimiento	Entre 50 y 70 kpps
Consola y puertos auxiliares	Sí (hasta 115,2 kbps)
Módulos de red intercambiables en actividad y fuentes de alimentación	No

Tabla 5. 1: Características de los Routers Cisco 3640

Esencialmente este modelo de Router se usa para sucursales multiservicio de alta capacidad con un máximo de 350 usuarios, que empleen accesos tanto para la Intranet y a la Extranet y tengan un alto índice de crecimiento.

Además, todos los Routers poseen módulos NM-4E y NM-4T para las conexiones de red. Estos módulos tienen las siguientes características:

NM-4E: módulo de red Ethernet de cuatro puertos LAN para 10BaseT RJ-45.

NM-4T: módulo de red serial de cuatro puertos para interfaces serie síncrona y admite una transferencia dúplex completa. Cada puerto cuenta con soporte para operaciones de dúplex completo y medio a velocidades T1 y E1. Todos los puertos utilizan conectores DB-60 idénticos que admiten cinco tipos de interfaces (RS-232, RS-449, RS-530, V.35, X.21) tanto en modo DTE como DCE.

Estos Routers han sido previamente ampliados a su memoria máxima DRAM y FLASH a 128 y 32 correspondientemente.

Para que la nueva red MPLS propuesta en este estudio de factibilidad quede operativa, no será necesaria una infraestructura nueva, se reutilizará la existente, debido a que la mayoría de hardware usado en la red Frame Relay se encuentra útil y vigente, no se necesitan mayores cambios en lo que respecta a hardware para realizar la migración de la red.

Básicamente, para poder migrar esta topología a MPLS, conservaremos las direcciones y subneting original gracias a que la infraestructura no necesita hacerse cambios.

Para poder correr MPLS en la red compuesta por Routers Cisco 3640 necesitaremos como requisito obligatorio hacer un upgrading o actualización del software IOS Cisco instalado previamente en los equipos, por un software IOS actual y de mejores características como lo es el IOS Cisco c3640-jk9s-mz.124-16a el mismo que es un IOS ENTERPRISE PLUS IPSEC 3DES para Routers 3640, con características plus de ruteo y de seguridades. El Router Cisco 3640 necesita 128 MB en DRAM y 32 MB en memoria Flash como requerimientos mínimos de memoria para poder correr este IOS.

Una vez hecho el upgrade del IOS, solo se debe aplicar las configuraciones realizadas previamente en esta guía, y obtendremos una red MPLS con servicios

integrados de VPN que permite al proveedor dueño de esta red migrada a MPLS poder integrarse con otras tecnologías como Frame Relay, ATM, IP, etc.

Pero en el caso de que no se desee usar este tipo de Router Cisco se puede aplicar las configuraciones de este estudio de factibilidad en cualquier Router Cisco que posea IOS que admita MPLS, y los conceptos de configuración sirven para equipos de cualquier otro fabricante. Por lo cual la migración a MPLS es factible en el aspecto técnico

5.2 Factibilidad Económica

MPLS como se ha establecido previamente, para una empresa o para cualquiera que desee migrar a esta tecnología, es una solución no solo en la parte tecnológica, sino también en la económica, ya que su implementación no implica costos exorbitantes.

Para saber la factibilidad económica se describirá un presupuesto necesario a proyectarse para la migración a MPLS, el cual nos va a indicar si es o no factible.

5.2.1 Establecimiento del presupuesto a proyectarse en la migración de la red

Debido a que la migración a MPLS en este caso se realiza a partir de una infraestructura que se encuentra en óptimo estado, se ahorra considerablemente en los costos de implementación.

Para establecer una aproximación del costo real que implica una migración a MPLS se usa como referencia la implementación del capítulo anterior.

Dado que para poder implementar MPLS en la estructura de la red necesitamos un software IOS acorde con las necesidades de la nueva tecnología debemos adquirirlo con un costo por licencia y también tenemos que cargarlo a los Routers de la infraestructura de red.

EL IOS usado en la implementación del capítulo anterior es un software de superior alcance, pero existen en el mercado IOS con características inferiores que también soportan MPLS.

El software embebido originalmente en los Routers Cisco 3640 es un Cisco IP, que posee solo las características básicas.

Modelo	Nombre	Descripción	Costo
S364C	c3640-i-mz	Cisco 3640 IOS IP	$189.30

Tabla 5. 2: Detalles del IOS básico para un Router Cisco 3640

Ya que el IOS está embebido de fábrica dentro del Router, este precio es solo referencial.

El IOS CISCO IP, solo tiene características básicas de enrutamiento, lo cual hace que no pueda ser usado para implementar MPLS a plenitud, para esto no es

necesario realizar una actualización del IOS ya que el problema no es la versión, sino son las características de enrutamiento las que limitan la implementación de MPLS, si los equipos están dentro del tiempo de garantía Cisco se puede hacer una actualización a la versión más reciente.

Entonces, se tiene que realizar un upgrade del IOS actual a un IOS de características MPLS, para ello usamos el IOS CISCO ENTERPRISE PLUS IPSEC 3DES Release 12.4.16a, que posee características avanzadas de enrutamiento y de seguridades, lo cual hace que sea necesario tener que comprarlo para implementarlo en cada uno de los Routers.

Modelo	Nombre	Descripción	Costo
S364AK9	c3640-jk9s-mz	Cisco 3640 IOS ENTERPRISE PLUS IPSEC 3DES	$2,145.40

Tabla 5. 3: Detalles de un IOS Enterprise con soporte MPLS para un Router Cisco 3640

Los IOS Cisco se tienen que comprar individualmente para cada uno de los Routers a implementarse por cuestiones de licencia propietaria de Cisco.

Entonces, a la compra del software IOS se suma el soporte técnico para realizar el upgrade, en el cual se debe considerar el respaldo de la configuración anterior, la instalación del nuevo IOS y verificación de funcionamiento con el nuevo IOS, considerando que el soporte técnico para este servicio bordea los 350 dólares y demora 2 horas para realizar el upgrade por cada Router, se tendrá que pagar para

los 10 Routers este servicio y se debe dividir la actividad de upgrade en 20 horas distribuidas en dos días para no perder productividad en el tiempo de migración.

Cantidad	Descripción	Costo unitario	Costo total
10	Cisco 3640 IOS ENTERPRISE PLUS IPSEC 3DES	2,145.40	21,454.00
10	Servicio técnico (Upgrade IOS)	350.00	3,500.00
		TOTAL:	**24,954.00**

Tabla 5. 4: Tabla de costos de implementación

Como se muestra en la tabla de precios, la inversión llega casi a los $25,000 por lo cual esta migración es una inversión fuerte, pero considerando los aspectos referidos en este estudio de factibilidad y las ventajas evidentes expuestas en el mismo documento sobre MPLS, podemos realizar la migración puesto que a la larga los beneficios superan a los costos de inversión.

A pesar del precio de la implementación, es un precio bajo en lo que respecta montar una nueva infraestructura de red, ya que un equipo que soporte nuevas tecnologías supera fácilmente los $5,000 haciendo que montar una infraestructura como la del capítulo anterior cueste más del doble que la implementación MPLS expuesta solamente en equipos.

Debido a que esta implementación muestra costos relativamente bajos respecto a montar una nueva infraestructura, ahorrando de manera considerable el capital para el proveedor y siendo MPLS también una solución que permite un mejor mantenimiento, se demuestra que esta es una solución económicamente factible para migrar.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 Conclusiones

- MPLS es una tecnología que ofrece mejores y mayores ventajas respecto a las tecnologías WAN convencionales, tanto a nivel económico, nivel técnico, en escalabilidad y flexibilidad.

- Tanto nacional como internacionalmente, hay una tendencia creciente de las empresas a migrar de redes exclusivamente ATM o Frame Relay e inclusive de redes híbridas a MPLS para solucionar sus problemas de conectividad, velocidad y disponibilidad de la información

- MPLS surge como una solución a los problemas de compatibilidad entre otras tecnologías, pudiendo transportar en forma transparente paquetes de distintos tipo de redes, convirtiéndose en el núcleo de una red multiservicio proyectándose como una base conceptual para tecnologías futuras de encaminamiento.

- Las tareas de administración y mantenimiento de la WAN se vuelven más sencillas para el proveedor de servicio gracias a la transparencia y

simplicidad de MPLS, lo cual permitirá al proveedor de comunicaciones tener una mejor calidad de servicio para sus clientes.

- MPLS es una solución viable en términos técnicos y económicos debido a que permite usar los mismos dispositivos de red los cuales por medio de configuraciones no tan complicadas pueden aumentar su funcionalidad, de esta manera se reduce considerablemente el precio final de la implementación de la solución MPLS haciéndola eficaz en el aspecto económico.

6.2 Recomendaciones

- Es aconsejable que el proveedor de comunicaciones tenga una red unificada con MPLS para solucionar problemas de conectividad y velocidad de redes WAN convencionales heredadas.

- Se puede aprovechar la estructura de pila de etiquetas que maneja MPLS para hacer a la red escalable, ya que se vuelve factible construir jerarquías de dominios globales de manera transparente.

- Se recomienda etiquetar de manera correcta y precisa los elementos de la red, así como también realizar los respectivos diagramas detallados para facilitar la tarea de mantenimiento; esto permite tener una mejor visión de la magnitud de una posible migración de la red.

- Antes de hacer un upgrade de un IOS en un Router es necesario estar completamente seguros que el equipo cumpla con las características y los requerimientos necesarios para soportar MPLS ya que comúnmente algunas versiones con características avanzadas de IOS necesitan mayor cantidad de memora DRAM y FLASH.

- Si se realiza la migración de una red se paralizan las actividades de los equipos, por lo que se recomienda aprovechar realizando un mantenimiento

preventivo de equipos y conectores, ya que con el tiempo las condiciones externas a las que se exponen los equipos pueden afectar su rendimiento.

- Como trabajo futuro se recomienda extender la investigación de MPLS en redes VPN de capa 3 con el fin de mostrar las ventajas comunicacionales que ofrece esta tecnología.

BIBLIOGRAFÍA

- Noonan, Wesley. (2004). Hardening Network Infrastructure: Bulletproof Your Systems Before You Are Hacked. McGraw-Hill/Osborne.

- Guichard, J. & Pepelnjak, I. (2000). MPLS and VPN Architectures. Cisco Press.

- Reagan, James.(2002). CCIP: MPLS Study Guide. Cisco Press.

- Luo, W., Pignataro, C., Bokotey, D. & Chan, A., (2005). Layer 2 VPN Architectures. Cisco Press

- Lobo, L. & Lakshman, U., (2005). MPLS Configuration on Cisco IOS Software. Cisco Press

- Gallaher, R., (2003). Rick Gallagher's MPLS Training Guide: Building Multi-Protocol Label Switching Networks. Syngress Publishing

- Alwayn, V. (2004). Advanced MPLS Design and Implementation. Cisco Press

- CISCO SYSTEMS, Material CCNA

- Manual Rápido de Configuración de un Router CISCO http://asignaturas.diatel.upm.es/rrss1/documentacion_archivos/LABORATORIO%20ACTUAL/manual_rapido_cisco.pdf

- Cisco: MPLS en Castellano

  http://www.slideshare.net/proydesa/cisco-mpls-en-castellano

- Diseño e implementación mediante el simulador Dynamips de una red MPLS para la conexión WAN de una empresa mediana con sus sucursales http://www.cib.espol.edu.ec/Digipath/D_Tesis_PDF/D-37484.pdf

- Análisis de requerimientos y alternativas tecnológicas

  http://bieec.epn.edu.ec:8180/dspace/bitstream/123456789/1036/5/T10838CAP2.pdf

- Manual Rápido de Configuración MPLS, BGP de un Router Cisco http://hondo.diatel.upm.es/manuales/Cisco/Manual%20Corto%20Cisco%20MPLS-BGP-vnp.pdf

- Análisis de factibilidad de migración de la red asynchronous transfer mode ATM de ANDINATEL a multi-protocol label switching http://bibdigital.epn.edu.ec/handle/15000/75

- Migración a redes basadas en MPLS: cómo evitar los errores cometidos por otros www.flukenetworks.com/fnet/es-es/StreamIt?Document=2821099

- Implementación de Redes MPLS-VPN Casos de Estudio

  http://www.cudi.edu.mx/primavera2002/presentaciones/MPLSVPN.pdf

- Investigación de Redes VPN con Tecnología MPLS http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/

HOJA DE LEGALIZACION DE FIRMAS

ELABORADAO) POR

_____

José Luis Pasquel Pasquel

COORDINADOR DE LA CARRERA

_____

ING. DANILO MARTINEZ

Lugar y fecha: Sangolquí, 30 de Agosto del 2010