ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

DISEÑO E IMPLEMENTACIÓN DE UN LABORATORIO QUE PERMITA EMULAR Y PROBAR SERVICIOS IP Y MPLS DE LA RED DE BACKBONE CISCO DE LA CORPORACIÓN NACIONAL DE TELECOMUNICACIONES CNT

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

CARLOS LUIS HIDALGO LLUMIQUINGA
carlos_hidalgok86@hotmail.com

DAVID ALEJANDRO LAGUAPILLO MUÑOZ
david_lagua5@hotmail.com

DIRECTORA: ING. MÓNICA VINUEZA R. MSc.
monica.vinueza@epn.edu.ec

Quito, Noviembre 2011

DECLARACIÓN

Nosotros, **Carlos Luis Hidalgo Llumiquinga** y **David Alejandro Laguapillo Muñoz**, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentada para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Carlos Luis Hidalgo Llumiquinga David Alejandro Laguapillo Muñoz

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por, **Carlos Luis Hidalgo Llumiquinga y David Alejandro Laguapillo Muñoz**, bajo mi supervisión.

_____

Ing. Mónica Vinueza R. MSc.

DIRECTORA DEL PROYECTO

AGRADECIMIENTO

A Dios, por guiarme y haber estado junto a mí todos los días dándome el valor y la sabiduría para cumplir satisfactoriamente cada una de mis metas, y seguir luchando día tras día.

A mis padres; Luis y Rosa, gracias por su apoyo incondicional y sobre todo por ese cariño y aliento en mis deseos de superación en los estudios, que hoy se ven reflejados en este Proyecto. A mis hermanos Diego y Roxana, con quienes he compartido mi vida en las buenas y las malas, gracias por estar a mi lado en todo momento.

A la CNT E.P., por su apoyo en el desarrollo de este Proyecto, en especial a todos los compañeros de la Gestión IP/MPLS, quienes me enriquecieron con sus conocimientos y brindaron las facilidades e información necesaria para culminar con éxito esta etapa importante de mi vida.

A la Ing. Monica Vinueza, por apoyar y guiar el desarrollo de este Proyecto con sus conocimientos, consejos y experiencia para poder concretarlo con éxito.

A mis amigos quienes me acompañaron y apoyaron en los malos y buenos momentos en esta trayectoria de aprendizaje, para ir cumpliendo cada uno de los objetivos planteados a lo largo de este aprendizaje.

Carlos Hidalgo

AGRADECIMIENTO

En primer lugar a mi familia, por guiarme, aconsejarme y sobre todo por darme su apoyo incondicional durante toda mi vida, especialmente en esta última etapa de mi carrera profesional en la que he desarrollado el presente proyecto.

A la Ing. Mónica Vinueza, que con sus consejos, sabiduría, experiencia e infinita paciencia ha sabido guiar la culminación satisfactoria de una etapa de mi vida.

Al personal que integra la gestión ATM/IPMPLS de la Corporación Nacional de Telecomunicaciones por colaborar con la información necesaria, pero sobre todo por su ayuda desinteresada que permitió la elaboración del proyecto.

A los buenos amigos, que han sabido apoyarme en los buenos y malos momentos que he pasado a lo largo de mi vida, pero que sobretodo han sabido darme ánimos para alcanzar los diferentes objetivos que me he planteado.

David Laguapillo

DEDICATORIA

Todo este trabajo se lo dedico a mi familia, quienes me han brindado su amor, confianza y apoyo, siendo los pilares en mi vida y en mis estudios, pero en especial a mí querida madre Rosita quien con su ejemplo y esfuerzo me llenó de fuerzas y ganas para superar cada una de mis metas.

Para mi Familia con todo el cariño y amor del mundo, todo mi esfuerzo y dedicación.

Carlos Hidalgo

DEDICATORIA

A mi madre que desde pequeño me ha inculcado los valores y principios necesarios para desarrollarme como persona, permitiéndome afrontar las diferentes adversidades que día a día se presentan.

A mi padre por enseñarme que con esfuerzo, dedicación y perseverancia puedo alcanzar todas las metas que me plantee, pero sobre todo por haberme comprendido a lo largo de mi vida.

A mi hermano por siempre estar a mi lado, quien a pesar de ser menor ha sabido ser un ejemplo de fortaleza, que sabe afrontar los diferentes problemas que se le presentan con buen ánimo.

David Laguapillo

ÍNDICE DE CONTENIDOS

TOMO I

TOMO II

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

ÍNDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

RESUMEN

El presente proyecto tiene como objetivo realizar el diseño e implementación de un laboratorio en el que se pueda probar y emular servicios IP y MPLS de la red de backbone Cisco de un proveedor de servicios. La Corporación Nacional de Telecomunicaciones CNT E.P. al implementar su nueva red de transporte de datos, vio la necesidad de implementar un laboratorio en el que se pueda desarrollar nuevos esquemas de configuración y corregir errores de los esquemas en producción, de esta manera el personal de la empresa se capacitará en la gestión de la red y reducirá los fallos.

En el primer capítulo se realiza una fundamentación teórica de los diferentes protocolos utilizados en la red de un proveedor de servicios. Se describe el y funcionamiento y las principales características de: el protocolo de conmutación de paquetes MPLS, los diferentes protocolos que permiten realizar la distribución de etiquetas con énfasis en LDP, el protocolo de enrutamiento interior IS-IS, el protocolo de enrutamiento exterior BGP y una breve descripción de la arquitectura TCP/IP.

En el segundo capítulo se muestra la estructura de la red de backbone IP/MPLS en producción, las capacidades de los diferentes equipos que conforman el laboratorio, y las tecnologías de acceso y transporte usadas por la CNT E.P.; se determinará los diferentes servicios que se pueden brindar con una red IP/MPLS como: calidad de servicio QoS; redes privadas virtuales, VPNs capa 2 y capa 3; ingeniería de tráfico y multicast.

En el tercer capítulo se procede a diseñar esquemas de red que permitan probar las diferentes funcionalidades de los equipos que conforman el laboratorio, se observará la manera de realizar las configuraciones básicas para el funcionamiento de los protocolos.

Los esquemas diseñados permiten realizar: la simulación de un backbone MPLS; pruebas de las funcionalidades del protocolo BGP; la creación y configuración de VPNs capa 2 punto a punto y en una topología hub and

spoke; el establecimiento, creación de VPNs capa 3 VRFs; pruebas para observar los diferentes algoritmos de QoS; la creación de túneles de ingeniería de tráfico; difusión de video por multicast y la agregación de servicios de capa 2 con la ayuda de *service instance.*

En el cuarto capítulo se determinan las configuraciones que permitan realizar las diferentes pruebas diseñadas, se verifica que estas se encuentren funcionando, y se observa los diferentes resultados de las pruebas realizadas en los diferentes esquemas de red.

En el capítulo cinco se presentan las conclusiones y recomendaciones obtenidas durante el desarrollo del presente proyecto.

PRESENTACIÓN

En la actualidad en el Ecuador existe una gran demanda dentro del entorno Tecnológico; y el sector de las Telecomunicaciones no es la excepción, debido a la creciente demanda de servicios como voz, video y datos, así como la necesidad de reducir costos aumentando la productividad. Es por esto que la Corporación Nacional de Telecomunicaciones CNT E.P. remplazó y potenció sus tecnologías, y dentro de este plan creó una red de transporte de última generación y de vanguardia como lo es MPLS, la cual soporta más aplicaciones y eleva la seguridad dentro de un ambiente WAN.

La capacidad de MPLS para integrar voz, vídeo y datos en una plataforma común con garantías de calidad de servicio (QoS), sumado a las mejoras del rendimiento y la disponibilidad que se obtienen con esta tecnología, así como su soporte de una amplia y escalable gama de servicios (VPNs, Multicast, etc), permite empaquetar más datos en el ancho de banda disponible y reducir los requerimientos de procesamiento a nivel de router. Se trata, pues, de una tecnología de red efectiva en costos, rápida y altamente escalable.

Con todo lo expuesto anteriormente se vio la necesidad de crear un laboratorio de pruebas que permitan la investigación de nuevas configuraciones y esquemas de red, que exploten todas las capacidades de MPLS, mejorando la utilización de los recursos del backbone MPLS de CNT E.P. y por ende ofertar a los clientes mejores y nuevos servicios.

Este proyecto se enfoca en la implementación del laboratorio de pruebas y en el desarrollo de diferentes esquemas de prueba y configuraciones para optimizar los servicios actuales y futuros que se pueden ofertar a los clientes de la Corporación Nacional de Telecomunicaciones CNT E.P.

CAPÍTULO 1

INTRODUCCIÓN Y ESTUDIO DE LA TECNOLOGÍA DE BACKBONE

Este primer capítulo consta de una introducción teórica general de las tecnologías MPLS (*Multiprotocol Label Switching*), IGP (*Interior Gateway Protocol*), BGP (*Border Gateway Protocol*), QoS (*Quality of Service*), *Routing*, *Switching*, TE (*Traffic Engineering*) describiendo sus principales características, ventajas y servicios que ofrecen.

CAPÍTULO 1

INTRODUCCIÓN Y ESTUDIO DE LA TECNOLOGÍA DE BACKBONE

1.1 *MULTIPROTOCOL LABEL SWITCHING* (MPLS) [1] [13] [18]

1.1.1 INTRODUCCIÓN

El gran crecimiento del Internet además de la mayor demanda de recursos de las nuevas aplicaciones y servicios obligó a realizar un cambio en las redes tradicionales como ATM (*Asynchronous Transfer Mode*), a pesar de que IP sobre ATM era una de las soluciones preferidas esta tiene como limitación la dificultad de administrar dos redes completamente diferentes, después con el incremento de la capacidad de transmisión de SDH/SONET (*Synchronous Digital Hierarchy / Syncronous Optical NETwork*) y DWDM (*Dense Wavelength Division Multiplexing*) frente a ATM se ve la necesidad de desarrollar una nueva tecnología de conmutación.

Se empiezan a desarrollar tecnologías propietarias como *Tag Switching* de Cisco, *Aggregate Route-Based IP Switching* de IBM las mismas que buscaban una integración entre el control de IP con la velocidad de conmutación de ATM creando redes más eficientes.

En 1997 la IETF (Internet *Engineering Task Force*) crea el grupo de trabajo *Multiprotocol Label Switching* (MPLS) para desarrollar una especificación común que unifique las diferentes soluciones propietarias, como resultado de este grupo se crea el estándar MPLS en el RFC 3031 cuyos principales beneficios son la ingeniería de tráfico, el soporte QoS, alta escalabilidad, soporte unicast, multicast prevención, rápida detección, y eliminación de lazos de enrutamiento, además del soporte de múltiples tecnologías de capa enlace de datos.

1.1.2 DEFINICIÓN [1] [18]

MPLS es una tecnología de transporte de datos que permite enviar paquetes en una red usando la información contenida en las etiquetas que se relacionan con las direcciones IP, las etiquetas se insertan entre las cabeceras de capa 3 y de capa 2, es una arquitectura que combina la rapidez de las tecnologías de conmutación de capa de enlace de datos con las de enrutamiento de capa red.

El objetivo principal de MPLS es crear una red de transporte flexible que permita incrementar el rendimiento y estabilidad de la misma, una de sus principales características como su nombre lo indica es el soporte multiprotocolo en capa enlace de datos y en la capa de red, permitiendo el uso de protocolos como *Asynchronous Transfer Mode* (ATM), FDDI, *Ethernet*, *Frame Relay* de capa 2 e IPv6, IPv4, IPX de capa 3 además de otros adicionales.

1.1.3 ELEMENTOS DE UNA RED MPLS [1] [2] [3] [13] [14] [18]

Los elementos que conforman una red MPLS se indican en la figura 1.1

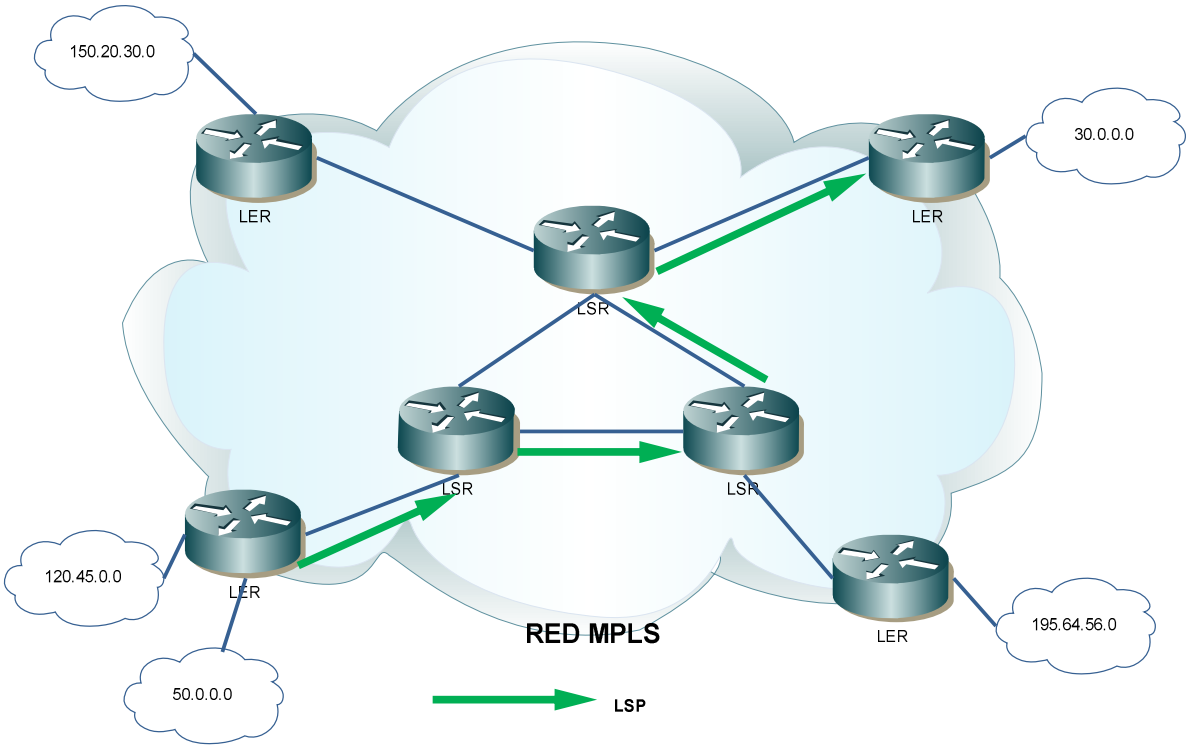


Figura 1.1: Elementos de una red MPLS [13]

1.1.3.1 *Label Switchet Router* (LSR) [2]

Los LSR son dispositivos de gran velocidad ubicados en el núcleo de la red que implementan los componentes de control y envío de MPLS, estos envían los paquetes en base al valor de la etiqueta encapsulada en el paquete, también pueden enviar paquetes de capa 3. La figura 1.2 indica los componentes que integran un LSR.

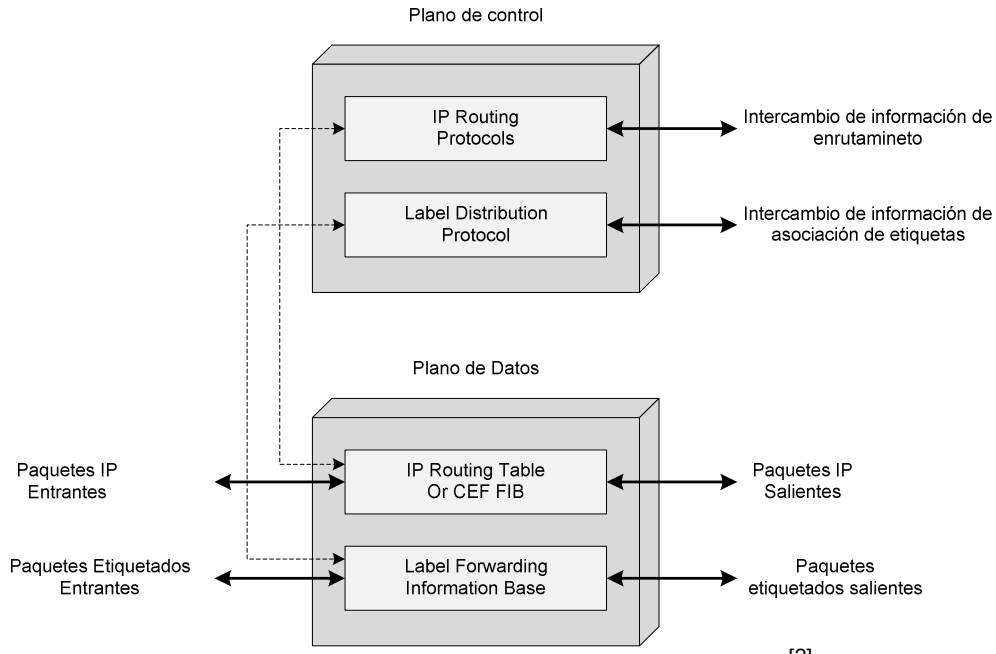


Figura 1.2: Componentes de un LSR [2]

Los LSRs son routers IP, switches ATM que tienen habilitado los protocolos de MPLS, para tener un entendimiento en común de la etiquetas usan un protocolo de distribución de etiquetas (LDP) o sus extensiones como *Border Gateway Protocol* (BGP), *Resourse Reservation Protocol* (RSVP) o *Constraint based* LDP (CR-LPD), se encargan de intercambiar las etiquetas de los paquetes entrantes por otras y las envía al siguiente salto.

1.1.3.2 *Label Edge Router* (LER) [2]

Los LER son equipos ubicados en los extremos de una red, que combinan el enrutamiento tradicional con la conmutación MPLS, son puntos de interconexión entre esta y otras redes como ATM, FDDI, *Frame Relay*, Ethernet, etc. Son elementos de entrada salida conocidos como router de de ingreso y egreso.

Dentro de las funciones de un LER está la de determinar la FEC (*Forwarding Equivalence Classes*) adecuada que permita asignar la etiqueta para el siguiente salto de un paquete que ingresa en la red, retira la etiqueta de los paquetes que salen a otra red o cambia la misma si el paquete continua dentro de la red.

1.1.3.3 *Forwarding Equivalence Class* (FEC) [3] [13]

Una FEC es una representación de una agrupación de paquetes que comparten características similares, como: dirección IP, tipo de tráfico, origen, destino, etc. Que tendrán el mismo tratamiento durante su transporte en la red para lo cual circularan por el mismo trayecto LSP (*Label Switched Path*) hasta llegar a su destino.

La asignación de un paquete a una determinada FEC se realiza únicamente al momento en que esta ingresa a la red, si bien a una FEC se pueden asociar diferentes tipos de flujos de datos un mismo flujo pertenece únicamente a una FEC al mismo tiempo.

Las FECs permiten tener una amplia gama de posibilidades de clasificación dependiendo de la cantidad de información que se considere para determinar la equivalencia lo que permite tener un tratamiento diferenciado para los diferentes flujos de datos haciendo escalable a la red. Por ejemplo una FEC sería un conjunto de paquetes cuya dirección de destino tenga un prefijo particular y un mismo puerto de destino como: 192.168.3.9 y 192.168.3.54 comparten el prefijo 192.168.3.0/26 y el puerto de destino 80 pertenecen a una misma FEC.

1.1.3.4 *Label Switched Path* (LSP) [3] [13]

Un LSP es una conexión unidireccional entre varios LSRs, es un camino específico a través de la red MPLS que empieza en el LER de ingreso y termina en el de egreso, para obtener una comunicación bidireccional se define un LSP diferente para el tráfico de retorno.

El LER de ingreso establece que paquetes se asocian a un determinado LSP en base al FEC al que pertenece y se procederá a colocar una etiqueta en el paquete

la cual está asociada a un LSP, esta servirá para la conmutación dentro del núcleo de MPLS donde se ignorará la cabecera de capa red del paquete.

Se pueden diseñar LSPs para que satisfagan los requerimientos de un determinado tipo de tráfico o aplicaciones, para esto se deben tomar en cuenta las características de los mismos y garantizar parámetros como el número de saltos, el ancho de banda, tamaño adecuado de los buffers, retardo, perdida de paquetes, etc. De manera que se obtenga un tratamiento diferenciado para cada uno de los flujos que se envíen a través de la red.

1.1.3.5 Etiqueta [3] [18]

La etiqueta es un conjunto de 32 bits que usado como identificador corto y de longitud fija, es usado para señalar una determinada FEC, que usualmente tiene un significado local. La etiqueta colocada en un determinado paquete representa la FEC a la cual este paquete ha sido asignado.

La etiqueta generalmente se asigna en función de la dirección de la capa de red es por esto que se puede tener la percepción de que es una versión simplificada de la dirección IP del paquete, a diferencia de IP que da la información necesaria para determinar el host al que pertenece esta información, el valor de la etiqueta únicamente tiene un número acordado entre dos LSRs que representa un LSP para tener una conexión al siguiente salto.

El significado local de una etiqueta hace referencia a que ésta tendrá validez de un router a otro, pero que para el siguiente salto el valor cambiará por el que hayan acordado el siguiente par de routers, las asociación de una etiqueta a un FEC se da en base a una evento que indique la necesidad de tal asociación, como el ingreso de un nuevo flujo de datos que necesite un tratamiento diferente al de los ya establecidos.

1.1.3.5.1 *Formato de la Etiqueta MPLS* [3]

La figura 1.3 muestra el formato de la etiqueta MPLS compuesta de 32 bits agrupados en 4 campos.

Figura 1.3: Formato de la etiqueta MPLS [3]

Etiqueta: es un campo de 20 bits al inicio de la cabecera, el valor numérico de este campo corresponde a un identificador de la etiqueta y representa a un FEC durante el proceso de envío, no todos lo valores son permitidos por lo que los valores reservados se indican en la tabla 1.1.

Etiqueta	Descripción
0	Es la etiqueta explicita nula (NULL) de IPv4. Este valor es permitido únicamente en la parte inferior de la pila de etiquetas e indica que la pila puede ser removida y que el envío del paquete puede ser hecho en base al *header* de IPv4.
1	Es una etiqueta de alerta para un router, es una etiqueta análoga a la opción de router *alert* disponible en los paquetes IP, este valor puede estar en cualquier parte de pila excepto en el fondo de la pila.
2	Es análogo al valor de 0 pero para IPv6.
3	Es la etiqueta implícita nula. Es una etiqueta que un nodo MPLS puede asignar y distribuir, pero que nunca aparece en la encapsulación se utiliza para el retiro de etiqueta en el penúltimo salto.
4-15	Reservado para uso futuro.

Tabla 1.1- Valores de las etiquetas reservadas [2]

Experimental (EXP): es un campo de tres bits que puede ser utilizado como una equivalencia para el campo ToS (*type of service*) estándar de IP en el campo CoS (*class of service*) experimental en MPLS, también se lo puede utilizar para garantizar los servicios cuando se utiliza las operaciones de clasificación de paquetes DiffServ.

***Stack* (S):** Las etiquetas MPLS pueden ser apiladas una encima de la otra. El bit S es usado para indicar cual etiqueta está en la cima de la pila, en cuyo caso se le asignará el valor de 1, el valor de 0 se asignará para el resto de las etiquetas

TTL: El TTL (Time To Live) tiene el mismo significado que en IP (*Hop Limit Field* en IPv6), al ingresar en la red se toma el campo TTL del paquete IP se lo reducirá en 1 y se copiará este valor al TTL de la etiqueta, encada salto por un router se lo disminuirá en 1 su valor, si la cuenta llega a 0 se descarta el paquete.

1.1.3.5.2 *Pila de Etiquetas* [14]

Los routers que soportan MPLS pueden necesitar más de una etiqueta en cada paquete, para transportarlo a través de una red MPLS. Para esto se desarrolla una estructura jerárquica denominada pila de etiquetas la misma que tiene características LIFO (*Last-In First-Out*), esta característica se indica en la figura 1.4, donde la última etiqueta colocada es la primera en salir, en cada nodo MPLS únicamente se procesa el paquete en base a la etiqueta que está en la cima de la pila. Un paquete sin etiquetar se puede ver como un paquete con la pila de etiquetas vacía n = 0.

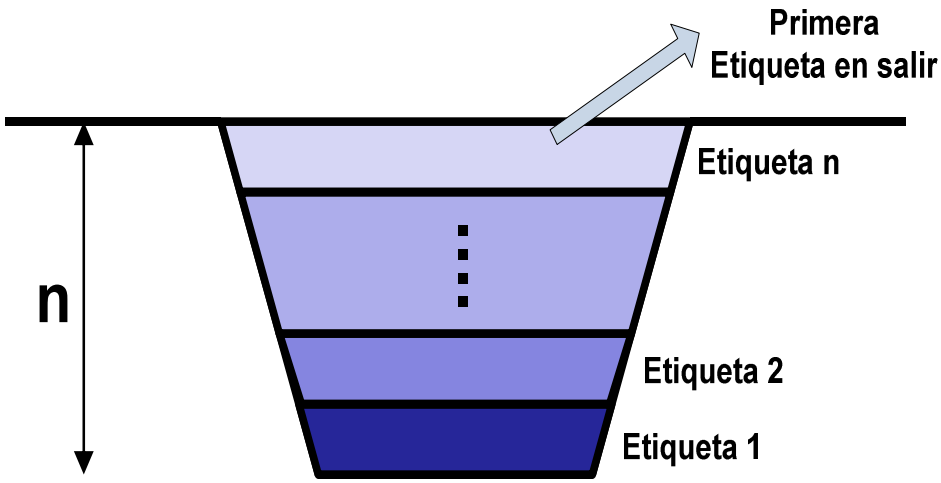


Figura 1.4: Pila de etiquetas MPLS [14]

1.1.3.6 Funciones sobre las Etiquetas [3] [18]

Cuando un paquete es recibido por un router MPLS se pueden realizar varias operaciones en la etiqueta que se encuentra en la cima de la pila de etiquetas, las operaciones pueden ser de *aggregate*, *push*, *pop*, *swap* o *untag*.

- En una operación *aggregate* se retira la etiqueta de la cima de la pila y se realiza una búsqueda de nivel 3.

- En una operación *push*, se coloca una etiqueta o un conjunto de las mismas sobre la pila de etiquetas que se encuentra en el paquete recibido.
- En una operación *pop*, se remueve la etiqueta de la cima de la pila y se reenvía el resto del paquete ya sea que contenga mas etiquetas o sea un paquete de capa 3.
- En una operación *swap*, se cambia la etiqueta que está en la cima de la pila por otra de diferente valor.
- En una operación *untag* se retira la etiqueta que está en la cima de la pila y se envía el paquete IP al siguiente salto. A este proceso se lo llama "desencapsulado" y es usualmente efectuado por el router de Egreso.

1.1.3.7 Multiprotocolo Arriba y Abajo [3] [18]

Basándose en la descripción de la componente de envío se tiene que no es específica para una tecnología de capa red en particular por esta razón la misma parte de envío se puede usar tanto para IP como para IPX, esto hace que MPLS sea una tecnología adecuada para múltiples protocolos de capa red.

La capacidad de soporte multiprotocolo se indica en la figura 1.5 donde no solo hace referencia a los protocolos de capa red, sino que su funcionamiento se hace extensible virtualmente a cualquier protocolo de capa enlace de datos, de aquí proviene el nombre *multiprotocol label switching*.

Figura 1.5: Soporte multiprotocolo de MPLS [1]

Para dar este soporte la encapsulación depende de la tecnología utilizada y puede realizarse de dos maneras:

Utilizando una cabecera *shim,* la misma que se inserta entre la cabecera de capa red y la de enlace de datos, usada en tecnologías que no permiten el envío de información en la cabecera como Ethernet o *Point-to-Point*.

Ó haciendo uso de la cabecera de enlace de datos, donde la información de la etiqueta se envía en determinados campos de la cabecera como en el *Virtual Path Identifier/Virtual Channel Identifier* (VPI/VCI) de ATM y el *Data Link Control Identifier* (DLCI) de *Frame Relay*.

En la figura 1.6 se muestra las formas de encapsulamiento MPLS sobre varias tecnologías de capa enlace de datos.

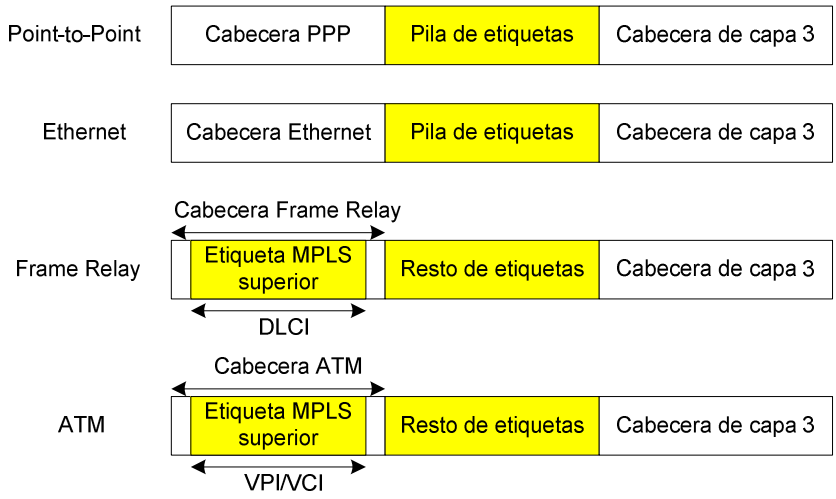


Figura 1.6: Encapsulación protocolos de capa enlace [13]

1.1.4 ARQUITECTURA MPLS [2] [3]

La arquitectura se divide en dos componentes:

- El componente de envío también conocido como plano de datos
- El componente de control al que se lo conoce como plano de control

El componente de envío es el responsable del reenvío de los paquetes de la entrada a la salida a través de un router o un switch.

El componente de control es el responsable de la construcción y el mantenimiento de la tabla de envío, cabe recalcar que todos los nodos implementan los dos planos, el de control y el de datos.

En la figura 1.7 se muestra la arquitectura de MPLS en la que se indican tanto el plano de datos como el plano de control.

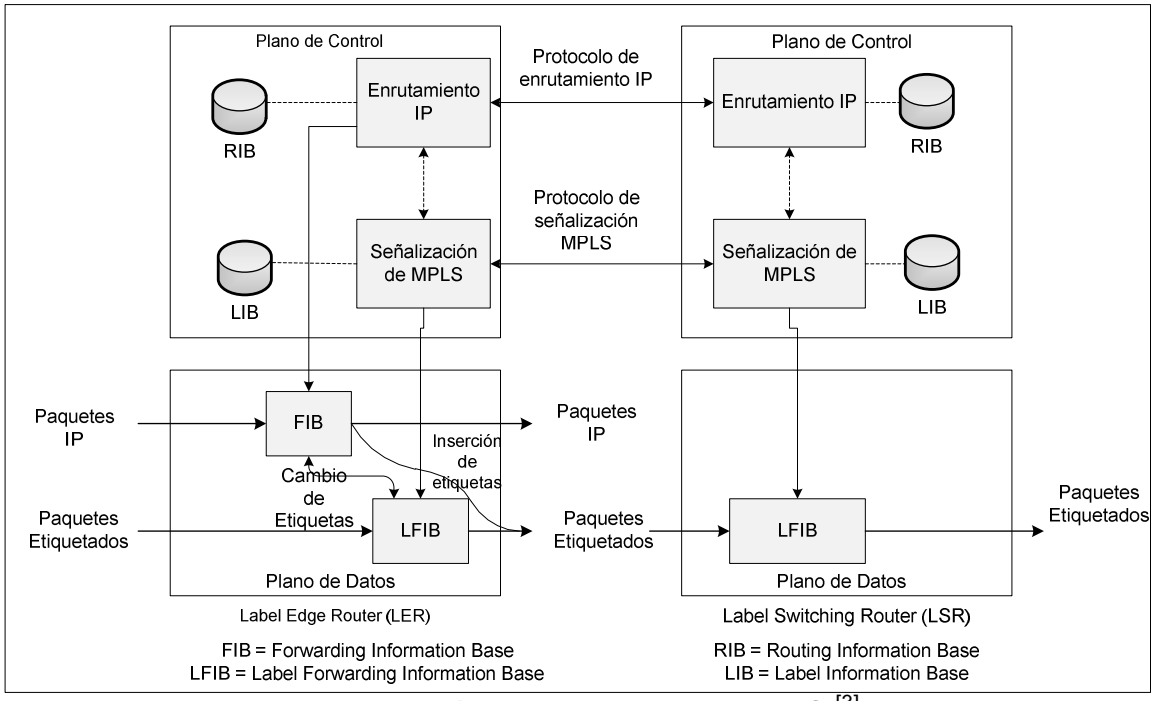


Figura 1.7: Arquitectura de MPLS [3]

1.1.4.1 Plano de Datos [2] [3]

El plano de envío de MPLS es el responsable de enviar los paquetes basándose en los valores contenidos en las etiquetas, también usa la *label forwarding information base* (LFIB), almacenada en un nodo MPLS para enviar los paquetes etiquetados. También mantiene una *Label Information Base* (LIB) que contiene la información acerca de las etiquetas asignadas por el nodo local y la asociación de estas con las recibidas de los otros nodos.

***Label Forwarding Information Base* (LFIB):** La LFIB mostrada en la figura 1.8 mantenida por un nodo MPLS está compuesta de una secuencia de entradas las mismas que consisten de una etiqueta entrante y una o más subentradas. Cada subentrada consiste de una etiqueta de salida, una interfaz de salida, y una dirección de siguiente salto, estas dentro de una entrada individual pueden tener

varias etiquetas de salida este caso especial se da con tráfico *multicast* donde se puede tener múltiples interfaces de salida, las entradas también pueden contener información de los recursos que el paquete puede usar o de la cola en la que debe ser colocado. Un nodo puede mantener una única tabla, una por cada interfaz o una combinación de ambas, en el caso de múltiples tablas se usará la correspondiente a la interfaz de entrada por la que llega el paquete.

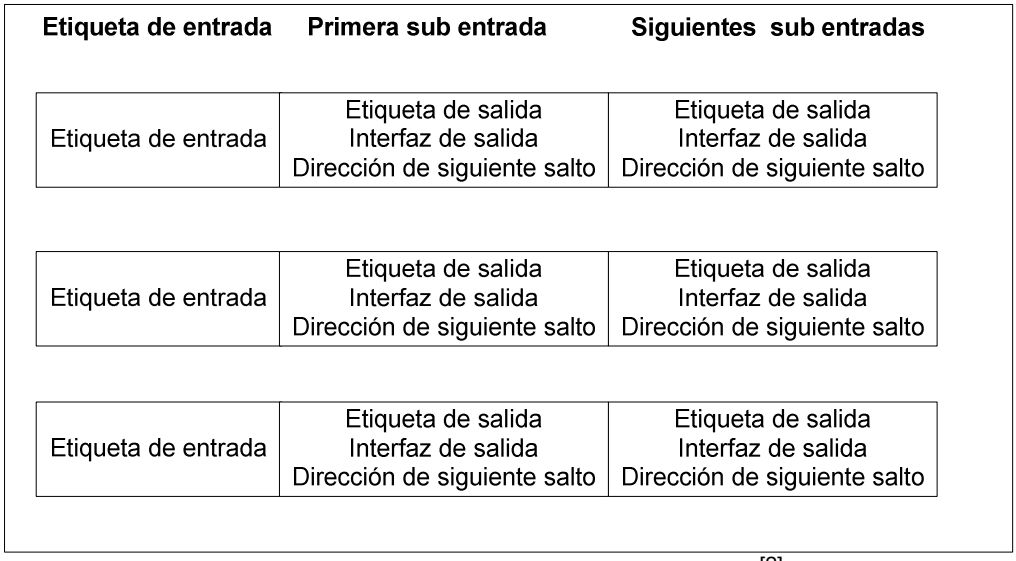


Figura 1.8: Estructura de la LFIB [2]

Algoritmo de envío de etiquetas: este algoritmo se basa en el intercambio de etiquetas, un nodo MPLS mantiene una única entrada en la tabla LFIB para un valor encontrado en la etiqueta de un paquete el mismo que se usa como índice de la tabla, después de que una etiqueta encuentra una coincidencia el router reemplaza la etiqueta del paquete por otra cuyo valor se encuentra almacenado en una de las subentradas, la misma que especifica la interfaz de salida y la información del siguiente salto, en caso de que especifique una cola el paquete se colocará en la misma.

1.1.4.2 Plano de Control [2] [17]

El plano de control de MPLS es responsable de mantener y actualizar las LFIB, todos los nodos MPLS deben ejecutar un protocolo de enrutamiento IP para intercambiar información de enrutamiento con otros nodos MPLS en la red, lo cual permitirá generar una tabla de enrutamiento.

A pesar de que se puede utilizar cualquier protocolo de enrutamiento se prefieren los protocolos de estados de enlace sobre los de vector distancia como OSPF e IS-IS, debido a que estos dan a cada nodo una vista completa de la topología de la red, la información de asociación de una etiqueta puede distribuirse usando *Label Distribution Protocol* (LDP) o con los protocolos de enrutamiento modificados.

Los protocolos de enrutamiento como OSPF inundan de información a un conjunto de routers que no tienen que ser necesariamente adyacentes, mientras que la información de la asociación de etiquetas solo se distribuye entre routers adyacentes, por esta razón los protocolos de estado de enlace no son aptos para la distribución de etiquetas.

En cambio al usar protocolos como BGP o PIM que también se pueden usar para distribuir las etiquetas, se simplificará la operación del sistema pues no se necesitan dos protocolos diferentes, además mantiene correspondencia entre la información de enrutamiento y las etiquetas obligatorias.

Las etiquetas intercambiadas entre dos nodos MPLS adyacentes se usan para construir la LFIB los mismos que se pueden combinar con un conjunto de módulos de control diferentes. El módulo se encarga de asignar y distribuir un conjunto de etiquetas, así como de mantener otro tipo de información de control. Se usa un IGP para definir la unión y correspondencia entre un FEC y la dirección de siguiente salto. Los módulos de control de MPLS son:

Unicast Routing Module: Este módulo construye la tabla FEC usando IGPs convencionales como IS-IS, OSPF, etc. En base a la tabla de enrutamiento se intercambian las asociaciones de las etiquetas con los nodos adyacentes para las subredes que se encuentran en las tablas.

Multicast Routing Module: Este módulo construye la tabla FEC usando un protocolo de enrutamiento *multicast* como *Protocol Independent Multicast* (PIM). La tabla de enrutamiento *multicast* se utiliza para intercambiar las asociaciones con los nodos adyacentes para esto se suele usar PIM v2 con extensiones MPLS.

Traffic Engineering Module: Este módulo permite especificar explícitamente el LSP el cual se establecerá a través de una red para propósitos de ingeniería de tráfico, utiliza las definiciones de túneles MPLS y la aplicación de IS-IS u OSPF para construir las tablas FEC. El intercambio de las asociaciones a las etiquetas se realiza mediante *Resource Reservation Protocol* (RSVP) o *Constraint-based Routing* LDP (CR-LDP), los cuales son un conjunto de extensiones que permite el enrutamiento basado en restricciones.

Virtual Private Network (VPN) Module: Este módulo utiliza las tablas de enrutamiento por VPN para las tablas FEC, la construcción de estas se realiza utilizando los protocolos que están configurados entre los routers del CPE y los LERs del proveedor de servicios, el intercambio de la información de las asociaciones a las etiquetas se realiza utilizando BGP dentro de la red del proveedor.

Quality of Service (QoS) Module: Este módulo es similar al de *unicast* y funciona de la misma manera.

1.1.5 OPERACIONES DE MPLS [1] [13] [14] [17] [18]

1.1.5.1 Selección de la Ruta

La selección de la ruta hace referencia al método usado para seleccionar un LSP para un FEC en particular, MPLS soporta los siguientes modos de selección:

El Enrutamiento *hop by hop* permite que cada nodo seleccione el siguiente salto para cada FEC de manera independiente. Esta es la manera tradicional en que se realiza el enrutamiento en las redes IP.

En el Enrutamiento explícito de un LSP un nodo no escoge el siguiente salto de manera independiente, sino que el router de ingreso o el egreso especifican algunos o todos los LSRs por los que pasa el LSP. En caso de que se especifique por un solo router todo el LSP se lo conoce como enrutamiento estricto explícito, en cambio si solo se especifica una parte se lo conoce como enrutamiento explícito libre.

La secuencia de LSRs que sigue un LSP en el enrutamiento explícito puede escogerse en la configuración, ó puede escogerse de manera dinámica por un nodo, este tipo de enrutamiento se usa para múltiples propósitos como ingeniería de tráfico o políticas de enrutamiento.

1.1.5.2 Extracción de la Etiqueta en el Penúltimo LSR [4]

MPLS permite una opción en la cual la etiqueta se puede retirar en el penúltimo salto, esto quiere decir que antes de llegar al LER en el último LSR se puede retirar la etiqueta, se puede hacer debido a que la etiqueta que se envía del LSR al LER en este escenario no tiene ninguna función y no hay necesidad de transportarla en el paquete, este comportamiento se puede observar en la figura 1.9.

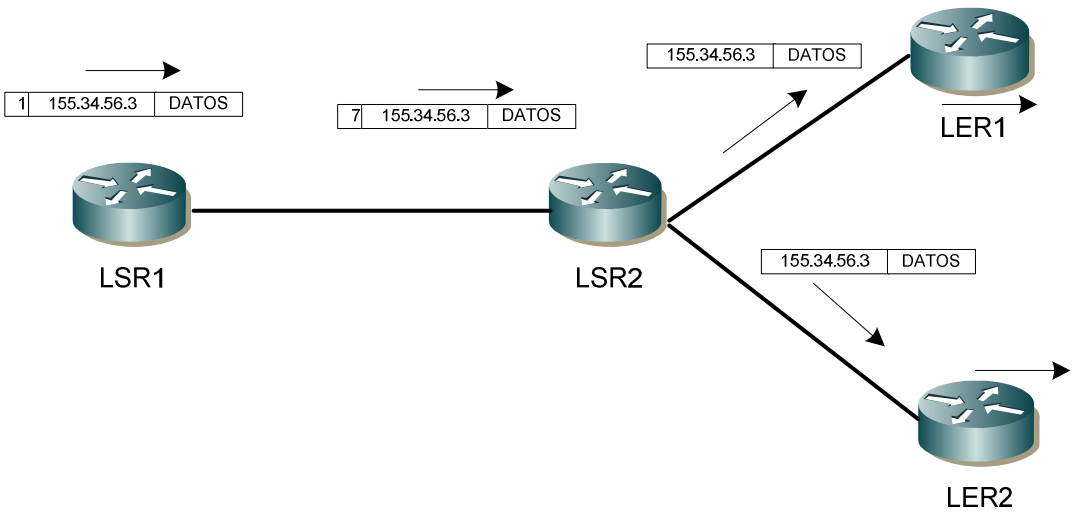


Figura 1.9: Extracción de la etiqueta en el penúltimo salto [4]

El retirar la etiqueta tiene la ventaja de reducir el procesamiento en el LER, esto debido a que cuando llega un paquete etiquetado al dispositivo de salida este primero realiza una búsqueda en sus tablas, basada en la información que llega en la etiqueta, una vez determina que debe ser retirada la elimina y procesa el resto del paquete en base a la información de capa red, al retirarla en el penúltimo salto se elimina la necesidad de esta primera búsqueda.

Se justifica el uso de este operación sobre las etiquetas, debido a que los routers de ingreso o egreso de una red MPLS realizan más procesamiento que los

internos, al ingreso de un paquete se debe asignar una etiqueta en base al contenido de la capa red, en cambio al salir el siguiente salto se determina en base a esta información, cabe recalcar que esta es una opción que no todos lo dispositivos MPLS deben soportar.

1.1.5.3 Establecimiento LSP [2]

Se puede establecer un LSP de dos maneras:

- Control independiente
- Control ordenado

Estos dos métodos pueden coexistir en una misma red sin que esto ocasione problemas de interoperabilidad, el método independiente converge y establece un LSP rápidamente debido a que el establecimiento y asociación de una etiqueta se puede realizar en cualquier momento; un LSP se establece inmediatamente después de la convergencia de los protocolos de enrutamiento. En cambio en el método ordenado las asociaciones de la etiquetas deben de propagarse por toda la red antes de que el LSP se establezca, sin embargo esto previene la formación de bucles.

1.1.5.3.1 *Establecimiento Mediante Control Independiente*

En el método de control independiente cada LSR realiza la partición de los prefijos de destino en FECs, se le asigna una etiqueta para cada FEC y estas asociaciones se anuncian a sus vecinos. El LSR crea una entrada en la tabla LFIB usando el mapeo entre las FECS y el siguiente salto, la información para asociar un FEC con el siguiente salto se la obtiene de un protocolo de enrutamiento unicast como OSPF o IS-IS.

En la LFIB se almacena información de los siguientes campos: etiqueta de entrada, etiqueta de salida, siguiente salto y la interfaz de salida, el LSR crea una asociación local entre una FEC y una etiqueta cualquiera seleccionada del pool de etiquetas libres, almacenado en la LIB y actualiza la LFIB. Las etiquetas de entrada son un conjunto de etiquetas seleccionadas del pool, el siguiente salto es

un conjunto de direcciones de capa 3 asociadas con las FECs, y la interfaz de salida es aquella usada para alcanzar el siguiente salto.

Una vez se crean las asociaciones locales el LSR envía las actualizaciones a sus vecinos usando LDP o las extensiones que modifican a los protocolos de enrutamiento, la información de asociación está compuesta de una dupla <prefijo de dirección, etiqueta, donde el prefijo identifica a una FEC y la etiqueta contiene el valor de la misma.

Cuando un LSR recibe un mensaje con información de asociación de etiqueta de un vecino, este comprueba si tiene una asociación local en la LFIB, si esta existe, actualiza el campo etiqueta de salida en su LFIB con el valor recibido, completando la información necesaria para iniciar el envío de paquetes.

En caso de recibir un mensaje con la información de asociación y no se disponga de una asociación para la FEC en la LFIB, se puede mantener la información para una asociación futura o descartarla, en cuyo caso LDP provee los mecanismos para retransmisión, la información de asociación de una etiqueta se distribuye únicamente a las routers adyacentes. Para compartir esta información deben tener al menos una subred común con alguna interfaz del LSR local.

1.1.5.3.2 *Establecimiento Mediante Control Ordenado*

En este método el LSR de ingreso o egreso inicia la configuración del LSP. La asignación de la etiquetas, está controlada en una forma ordenada desde en egreso hasta el ingreso de un LSP. La configuración del LSP puede ser iniciada por ambos extremos. El que inicia el LSP hace la selección del FEC y todos los LSRs que atraviese el LSP los usan, el establecimiento ordenado tiene como requerimiento que todas las asociaciones de etiqueta se propaguen por todos los LSRs antes de que LSP sea establecido, esto resulta en un tiempo de convergencia más alto en comparación con el tiempo usado por el control independiente.

1.1.6 FUNCIONAMIENTO DE MPLS [3] [17]

Las redes MPLS usan las etiquetas para enviar los paquetes, al momento que un paquete ingresa a la red el LER lo asigna a una FEC única para su transporte por la red.

La FEC que se asigna al paquete se codifica en el valor de la etiqueta asignada, estos paquetes ya etiquetados pueden ser enviados por la red, en los siguientes saltos dentro de la red no se debe realizar un análisis de la información de la cabecera de capa red. La etiqueta se usa como un índice en la tabla para buscar el siguiente salto y la nueva etiqueta; se reemplaza la etiqueta por esta nueva y se envía al siguiente salto.

Finalmente en el nodo de salida LER se remueve la etiqueta y se realiza una búsqueda en base a la cabecera de la capa red y se envía al siguiente salto fuera de la red MPLS.

El usar etiquetas para el envío de paquetes tiene algunas ventajas sobre el envío tradicional:

En envío MPLS puede ser realizado por switches, los mismos que deben tener la capacidad de cambiar, buscar y reemplazar las etiquetas, pero no deben analizar la información de capa red.

Basándose en el hecho de que un paquete se asigna a una FEC al ingresar a la red, un mismo paquete que ingrese por dos routers diferentes se etiquetará de diferente manera en cada uno, como resultado las decisiones que dependen del router de ingreso se pueden realizar fácilmente, en redes tradicionales esto no se puede hacer debido a que la identidad del router de ingreso no viaja con el paquete, tomando como base que a un mismo LER llegan varios paquetes por diferentes interfaces a cada interfaz se le puede asignar a un FEC diferente con una etiqueta que lo identifica los que es la base de MPLS VPN (*virtual prívate networks*).

En las redes con ingeniería de tráfico se hace que los paquetes sigan un camino en particular, el cual es seleccionado de manera explícita antes de que el paquete ingrese en la red.

En una red MPLS la etiqueta puede ser usada para representar una ruta por lo que se elimina la necesidad de que el paquete lleve la información de la ruta a seguir. Esto es la base para el soporte de ingeniería de tráfico de MPLS.

La clase de servicio que un paquete necesita puede ser determinada por el LER de ingreso el cual puede aplicar diferentes umbrales de descarte, políticas de administración para controlar los diferentes paquetes. Los siguientes saltos usan *per-hop behaviors* (PHBs) para cumplir con el *service policy*.

MPLS permite que se deduzca total o parcialmente de la etiqueta la prioridad de la clase de servicio. En este caso la etiqueta representa la combinación de una FEC y la prioridad de la clase de servicio. Esta función es la base de calidad de servicio (QoS) en MPLS.

1.2 PROTOCOLOS DE DISTRIBUCIÓN DE ETIQUETAS [19] [27]

Un protocolo de distribución de etiquetas es un conjunto de procedimientos y mensajes a través de los cuales los routers de conmutación de etiquetas “LSRs” pueden localizar a sus homólogos y establecen asociaciones con estos, con la función de mapear las FECs e indican las rutas a seguir por los paquetes. Dos LSR que intercambian esta información son llamados pares de distribución de etiquetas, y entre ellos hay adyacencia de distribución de etiquetas.

Los protocolos de distribución de etiquetas se pueden clasificar de la siguiente forma:

Protocolos de enrutamiento implícitos, permite el establecimiento de LSPs pero no ofrece características de ingeniería de tráfico.

- Label Distribution Protocol (“LDP”).
- Border Gateway Protocol (“BGP”).

- Intermediate System to Intermediate System (“IS-IS”).

Protocolos de enrutamiento explícitos, es idóneo para ofrecer ingeniería de tráfico y permite la creación de túneles.

- Constraint-Based Routing LDP (“CR-LDP”).
- Resource Reservation Procotol – Traffic Engineering (“RSVP-TE”).

1.2.1 *LABEL DISTRIBUTION PROTOCOL* (“LDP”) [19]

Es un nuevo protocolo definido para la distribución de etiquetas, es un conjunto de los procedimientos y los mensajes por los que los LSRs (*Label Switched Routers*) establecen LSPs (*Label Switched Paths*) a través de una red, asignando la información de enrutamiento de la capa red directamente a la capa de enlace de datos en rutas de conmutación.

LDP asocia un FEC con cada LSP que crea. La FEC asociada con un LSP especifica que paquetes son mapeados por un LSP. Los LSPs se extienden a través de una red, por cada LSR la etiqueta asignada al siguiente salto dado por la FEC.

Cuando dos LSRs utilizan conjuntamente un protocolo de distribución de etiquetas para intercambiar información de asociaciones de etiquetas a FECs, se les denomina “LDP *peers*”, respecto a la información de las asociaciones que intercambian.

1.2.1.1 Mensajes LDP [20] [21]

Todo LSR que soporte el protocolo LDP debe mantener sesiones LDP con otros LSR o LER que hagan lo mismo. Durante una sesión LDP se generan diversos tipos de mensajes con la finalidad de, dar a conocer a otros enrutadores que el enrutador está activo, mantener el conocimiento de sesiones activas, comunicar las asociaciones de etiquetas o FECs que el LSR haga, solicitar etiquetas a otros LSR, comunicar cuando una asociación ya no es válida, entre otras, el protocolo

LDP mantiene el dominio MPLS en coherencia, en cuanto a las etiquetas y las relaciones que puedan tener con otros FECs en la red.

Los mensajes LDP son de suma importancia ya que debido a estos se mantiene un correcto funcionamiento de MPLS, y se han definido cuatro tipos de mensajes LDP.

En la figura 1.10 se indica los tipos de mensajes LDP y su intercambio para establecer una sesión LDP.

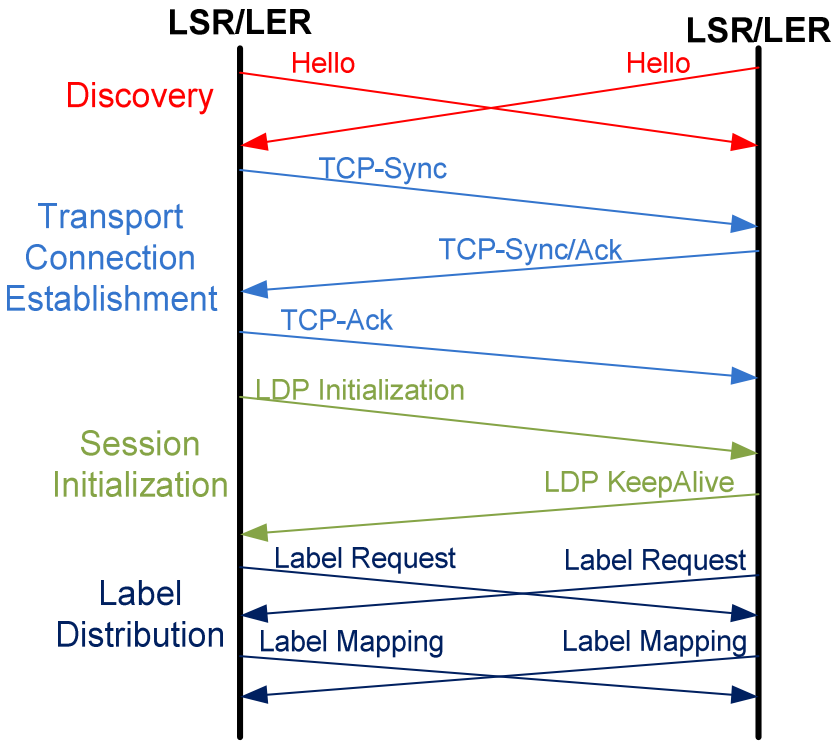


Figura 1.10: Intercambio de mensajes LDP [39]

1.2.1.1.1 *Descubrimiento (Discovery)*

Este mensaje es utilizado por cada LSR para informar de su disponibilidad como nodo de un nuevo LSP al resto de LSRs del dominio MPLS. El mensaje que se transmite es un mensaje de “Hello” el que se transmite periódicamente sobre UDP. Cuando otro LSR recibe “Hello” comenzará el proceso de establecimiento de sesión mediante *“Adjacency Messages”*

1.2.1.1.2 *Sesión (Session)*

Utilizados para establecer, mantener y liberar sesiones LDP entre LDP peers. Se tienen cuatro mensajes:

- *Mensaje "Initialization":* es el primer mensaje enviado para establecer la conexión TCP necesaria para la sesión LDP entre "*peers*".
- *Mensaje "Keep Alive":* se envía si no hay otros mensajes que intercambiar, para mantener activa la conexión
- *Mensaje "Address":* informa a su "*peer*" de su dirección
- *Mensaje "Address Withdraw":* informar de cambio de dirección

1.2.1.1.3 *Anuncio (Advertisement)*

Utilizados para intercambiar (una vez establecida la sesión entre dos "peers") información específica sobre la gestión y distribución de etiquetas de cada LSP. Se tiene cinco mensajes:

- *Mensaje "Label Mapping":* para mandar al "*peer*" la etiqueta adecuada según FEC-LSP.
- *Mensaje "Label Request":* para solicitar al "*peer*" el envío de la etiqueta de la FEC correspondiente.
- *Mensaje "Label Abort Request":* para anular una petición de etiqueta previa.
- *Mensaje "Label Withdraw":* para avisar al "*peer*" de que deje de usar la etiqueta correspondiente a una FEC enviada previamente.
- *Mensaje "Label Release":* para indicar al "*peer*" que no va a necesitar más la etiqueta correspondiente a una FEC determinada.

1.2.1.1.4 *Notificación (Notification)*

Para indicar errores que causarán el fin de la sesión o información del estado de la sesión.

1.2.1.2 Formato del PDU LDP [13]

Un paquete LDP siempre comienza con una cabecera LDP como se ilustra en la figura 1.11

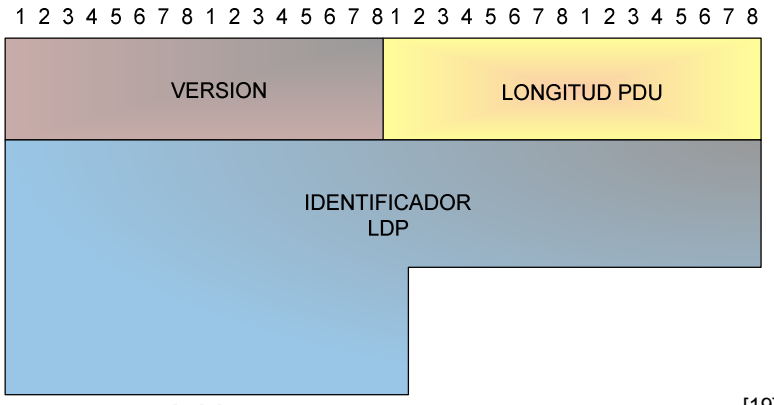


Figura 1.11: Formato de la cabecera PDU-LDP [19]

El PDU LDP está compuesto por una cabecera (LDP *Header*) y de su mensaje (LDP mensaje), un PDU LDP puede transportar varios mensajes LDP.

La cabecera PDU-LDP se compone de tres campos:

Versión: Este campo informa del tipo de versión del protocolo, es un campo de dos octetos y actualmente la única versión de LDP es 1.

Longitud PDU: Es un campo de dos octetos que indica la longitud total del PDU-LDP excluyendo los campos versión y longitud.

Identificador LDP: El identificador LDP es un campo de 6 octetos usado en particular para identificar un espacio de etiquetas, los primeros cuatro octetos son un identificador de LSR (LSR-ID), los siguientes dos octetos dependen del espacio de etiquetas, si el PDU-LDP pertenece a un espacio global de etiquetas estos dos octetos se colocan en 0, pero si pertenecen a un espacio de etiquetas por interfaz este valor es un número único asignado por el originador de la PDU-LDP.

Seguido de la cabecera PDU-LDP existen uno o más mensajes LDP cuyo formato se indica en la figura 1.12, los cuales no son necesariamente relacionados entre sí.

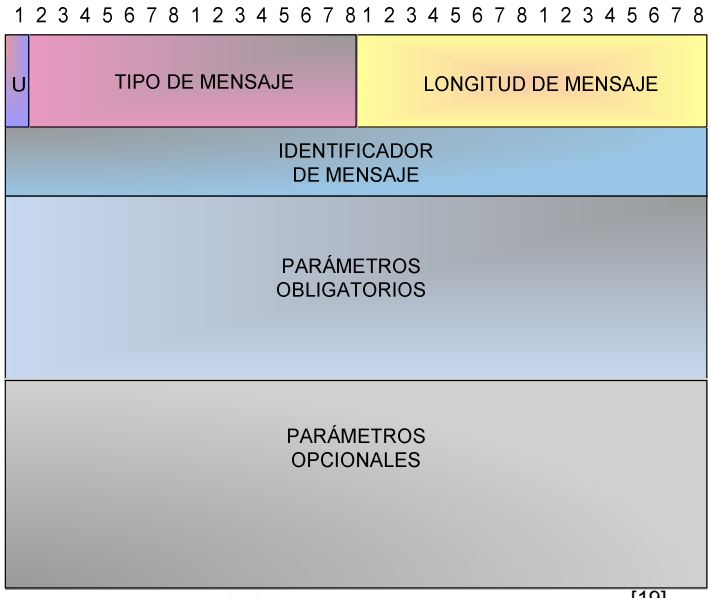


Figura 1.12: Formato mensaje LDP [19]

U (Unknown): Es un bit que define la acción que se debe tomar cuando se recibe un mensaje desconocido si este bit es 0 se envía una notificación al originador del mensaje, en cambio si el bit U es 1 este mensaje desconocido es ignorado.

Tipo de Mensaje: Es un campo de 15 bits que identifica el tipo de mensaje.

Longitud del Mensaje: es la longitud de un conjunto de campos después del campo longitud del mensaje (ID Mensaje + Parámetros obligatorios + Parámetros opcionales), en bytes.

Parámetros Obligatorios y Opcionales: Los parámetros obligatorios y los parámetros opcionales dependen de los tipos de mensaje enviados. Estos parámetros son a menudo codificados usando el esquema TLV (Tipo/Longitud/Valor), la cual es una forma común de codificación de valores arbitrarios de datos en un paquete.

1.2.1.3 Codificación TLV (Tipo/Longitud/Valor) [13]

Todos los mensajes LDP tienen una estructura común que usa un esquema de codificación TLV el cual se muestra en la figura 1.13.

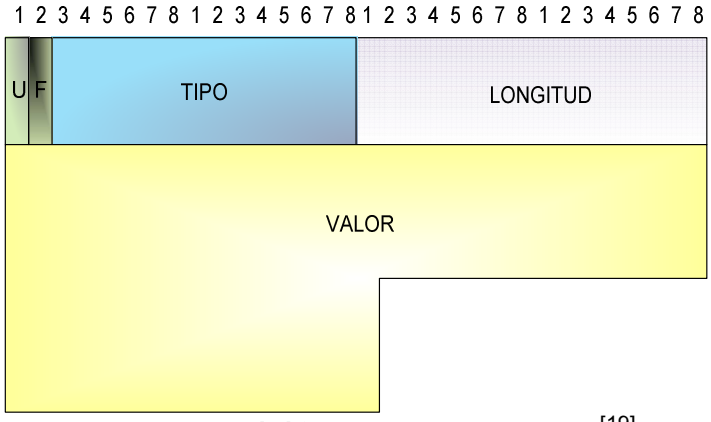


Figura 1.13: Formato LDP TLV [19]

U (Unknown): Es un bit que define la acción que se debe tomar cuando se recibe un TLV desconocido si este bit es 0 se envía una notificación al originador del mensaje y todo el mensaje es ignorado, en cambio si el bit U es 1 el TLV desconocido es ignorado y el resto del mensaje se procesa como si no existiera el TLV.

F (Forward): Este bit toma relevancia únicamente cuando el bit U se establece en 1, así si F=0, el TLV desconocido no es desviado con el resto del mensaje y si F=1, el TLV es desviado con el resto del mensaje.

Tipo: Este campo es de 14 bits e indica el tipo de datos que se envían en el campo valor del TLV para poder interpretarlos.

Longitud: Este campo de 16 bits indica la longitud de los datos que lleva el campo valor.

Valor: Este campo es de longitud variable y contiene la información del mensaje y su interpretación depende del campo tipo.

1.2.2 *CONSTRAINT-BASED ROUTING* LDP (CR-LDP) [21]

La restricción de enrutamiento basado en LDP es un mecanismo que soporta los requerimientos de ingeniería de tráfico, este enrutamiento explícito está basado en restricciones, donde la restricción es la ruta explicita, al igual que cualquier otro LSP un CR-LSP es un camino a través de una red MPLS.

La diferencia es que mientras que los LSPs son configurados exclusivamente sobre la base de la información, en las tablas de enrutamiento o de un sistema de gestión, el CR-LSP está basada en restricciones que se calcula en un punto en el borde de la red en función de criterios, incluyendo pero no limitado a la información de enrutamiento.

La intención es que esta funcionalidad ofrezca las características especiales deseadas a los LSP con el fin de apoyar mejor el tráfico enviado por el LSP. La razón de la creación de CR-LSP podría ser que se quiere asignar determinado ancho de banda o de otro tipo de servicios a las características de clase LSP.

Constraint Routing puede seleccionar la trayectoria más larga (en términos de costo), pero con menos carga de tráfico del que se tomaría con enrutamiento convencional, por lo que al mismo tiempo que *Constraint Routing* incrementa la utilización de la red, agrega mayor complejidad a los cálculos de enrutamiento.

CR-LDP utiliza UDP para descubrir “LDP *peers*” y TCP para el control, administración y petición de etiquetas.

1.2.3 PROTOCOLO DE GATEWAY EXTERIOR (*BORDER GATEWAY PROTOCOL* “BGP”) [28]

BGP ofrece una gran escalabilidad para redes MPLS, jugando un papel importante en la separación entre plano de control y el plano de reenvío. El uso de etiquetas para el envío de información agregada, y el uso de diferentes jerarquías de enrutamiento transforman a la red en una altamente escalable.

Las diferentes partes de la cadena transmitirán únicamente información requerida para llevar a cabo su función específica. Por ejemplo, enrutadores LSRs

necesitan mantener la información de etiquetamiento y la información de la red interna para conmutar los paquetes a su destino.

La información VPN se entregará sólo a los routers LERs que tienen conocimiento de las redes privadas virtuales y no a todos los routers de borde.

BGP es un protocolo utilizado para llevar información de enrutamiento externo, por ejemplo información de enrutamiento de Internet. En una red MPLS que se utiliza para proporcionar servicios de Internet y servicios L3 VPN BGP se suele llevar en la tabla de enrutamiento de Internet, la información de enrutamiento de los clientes IPv4/IPv6 y la información de enrutamiento VPNv4 con etiquetas VPN.

El túnel MPLS es un mecanismo que permite a los routers LSRs el envío de paquetes utilizando etiquetas sin la necesidad de buscar sus destinos en tablas de enrutamiento IP. Sólo routers LERs miran a sus destinos en la tabla de enrutamiento. Esto significa que los routers LERs son los únicos que necesitan tener esta información, por lo que necesitan ejecutar BGP.

En resumen, BGP se utiliza para llevar la siguiente información:

- Información de enrutamiento de Internet.
- Información de los clientes de enrutamiento.
- Información de enrutamiento con etiquetas VPNv4 VPN.

En algunas aplicaciones MPLS BGP también se utiliza para distribuir información de la etiqueta superpuesta en sus actualizaciones.

1.2.4 PROTOCOLO DE RESERVA DE RECURSOS-INGENIERÍA DE TRÁFICO (RSVP-TE) [5]

RSVP es un protocolo de señalización para la reserva de recursos, cuando se combina RSVP y MPLS se puede definir una sesión con mayor flexibilidad. Este protocolo permite crear túneles LSP, para el establecimiento de los túneles LSP el protocolo de señalización utiliza el modelo *downstream* bajo demanda.

El protocolo RSVP requiere que el dominio MPLS soporte encaminamiento explícito para facilitar la gestión del tráfico. Se debe añadir (*EXPLICIT_ROUTE*) en los mensajes de *Path* para tener una ruta explícita.

El protocolo RSVP-TE es una extensión del protocolo RSVP original, que fue diseñado para ejecutar la distribución de etiquetas sobre MPLS. RSVP-TE soporta además la creación de rutas explícitas con o sin reserva de recursos. Una de las características adicionales más importantes de este protocolo es que permite el re-enrutamiento de los túneles LSP, con el fin de dar una solución ante caídas de red, congestión y cuellos de botella.

Originalmente el IETF propuso a RSVP-TE como el protocolo de señalización principal, ya que este era utilizado por la mayoría de las compañías de Interneten MPLS y porque la tendencia es utilizar un protocolo de señalización RSVP.

1.3 APLICACIONES DE MPLS

La ventaja de la arquitectura MPLS es la facilidad para soportar diferentes aplicaciones entre las que se pueden nombrar:

- Calidad de Servicio “QoS”.
- Ingeniería de Tráfico.
- Redes Virtuales Privadas “VPN”.
- Soporte Multiprotocolo.

1.3.1 CALIDAD DE SERVICIO “QoS” [21]

QoS consigue el uso eficiente de los recursos de una red de datos permitiendo garantizar la asignación de los recursos necesarios a aplicaciones que así lo necesiten, sin arriesgar el desempeño de las demás aplicaciones, dándole al administrador de una red un mayor control sobre su red.

QoS debe trabaja en toda la infraestructura de la red para asegurar calidad de servicio “*End to End”,* asigna recursos a las aplicaciones en función a sus requerimientos, estos recursos se refieren principalmente al ancho de banda.

QoS se basa en prioridades para asignar los recursos a las aplicaciones, algunas aplicaciones pueden tener prioridades más altas que otras, sin embargo QoS garantiza que todas las aplicaciones tengan los recursos necesarios para completar sus transmisiones en el tiempo.

1.3.2 INGENIERÍA DE TRÁFICO [15]

La Ingeniería de Tráfico establece rutas dinámicamente y prevé la asignación de recursos en base a la demanda, así como la optimización del uso de la red, MPLS permite la asignación de recursos en las redes para balancear la carga dependiendo de la demanda y proporciona niveles diferentes de asignación de recursos dependiendo de las demandas de tráfico que los usuarios generen sobre la red.

En MPLS se analizan flujos de paquetes con su respectivo QoS y demanda tráfico predecible, permitiendo de este modo prever rutas en base a flujos individuales, siendo posible que existan diferentes flujos entre canales similares pero dirigiéndose hacia y por enrutadores diferentes.

MPLS puede re-enrutar inteligentemente las rutas si en algún momento la red se ve amenazada de llegar a congestionarse, es decir que MPLS es capaz de cambiar las rutas de los flujos de paquetes dinámicamente conforme a las demandas de tráfico de cada flujo.

1.3.3 REDES VIRTUALES PRIVADAS "VPN" [21]

MPLS permite que el tráfico de una red atraviese la Internet de una manera eficiente, transparente para el usuario y de forma privada para el resto de usuarios de la red, eliminando cualquier tráfico externo y protegiendo la información.

Las VPN creadas con tecnología MPLS proporcionan mayores características como lo son una mayor capacidad de expansión y ser más flexibles en cualquier red, principalmente IP. MPLS se encarga de reenviar paquetes a través de túneles privados utilizando etiquetas que actúan como códigos postales, la

etiqueta tiene un identificador que cumple la función de marcar unívocamente dicha VPN y aísla el tráfico de esta de otras VPNs.

1.3.4 SOPORTE MULTIPROTOCOLO [21]

MPLS es capaz de alojar y trabajar a la par con diversas tecnologías de red ya existentes tales como IP, ATM y Frame Relay. Los routers MPLS pueden trabajar con routers IP, al igual que los switches MPLS pueden trabajar con switches normales, lo que facilita la introducción de dicha tecnología a redes existentes. Siendo esta una gran ventaja para conseguir redes mixtas con el adicional de QoS para optimizar y expandir los recursos.

Siendo MPLS de esta forma una tecnología innovadora que se puede aplicar a redes nuevas, como a redes ya existentes.

1.4 MODELO DE REFERENCIA TCP/IP [23]

1.4.1 INTRODUCCIÓN

La arquitectura TCP/IP esta hoy en día ampliamente difundida, a pesar de ser una arquitectura de facto, en lugar de ser uno de los estándares definidos. Esta arquitectura se empezó a desarrollar a partir de 1972 como base de la ARPANET (red de comunicaciones militar del gobierno de los EE.UU), y con la expansión de la Internet se ha convertido en una de las arquitecturas de redes más difundida.

TCP/IP es la base de Internet, y sirve para comunicar todo tipo de dispositivos, computadoras que utilizan diferentes sistemas operativos, minicomputadoras y computadoras centrales sobre redes de área local (LAN) y área extensa (WAN).

1.4.2 ARQUITECTURA TCP/IP [19] [24]

TCP/IP está compuesto por cuatro capas o niveles, cada nivel se encarga de determinados aspectos de la comunicación y a su vez brinda un servicio específico a la capa superior. Estas capas son las mostradas en la figura 1.14.

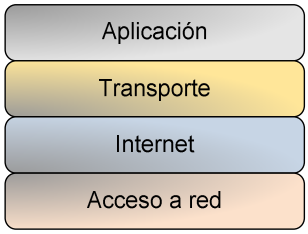


Figura 1.14: Capas del modelo TCP/IP [41]

1.4.2.1 Capa de Acceso a la Red [19] [24]

La capa de acceso a la red es la capa inferior de la pila TCP/IP. El modelo TCP/IP no define ningún protocolo en específico para esta capa, ni las características del medio de transmisión, los protocolos de esta capa proporcionan al sistema los medios para enviar los datos a otros dispositivos conectados a la red.

Por lo tanto, la capa de acceso a la red contiene especificaciones relacionadas con la transmisión de datos por una red física de manera transparente sean estas redes LAN, MAN o WAN, que utilicen diferentes tecnologías como Ethernet, Token Ring, ATM, Frame Relay, FDDI, línea telefónica, ISDN, etc.

1.4.2.2 Capa Internet [19] [24]

La capa Internet se encuentra por encima de la capa Acceso a la Red y cuyo propósito es el enviar paquetes desde cualquier red a cualquier red destino en la *internetwork*, dichos paquetes viajan de forma independientemente al destino, sin importar la ruta y las redes que recorrieron para llegar hasta su destino, en consecuencia en esta capa se realiza la determinación de la mejor ruta y la conmutación de paquetes.

En el proceso de envío no se ofrecen garantías de entrega ni de orden, debido a que en esta capa la integridad de los datos no es verificada, y el mecanismo de verificación se lo deja a las capas superiores (Transporte o Aplicación).

El protocolo específico que preside esta capa se denomina Protocolo Internet(IP), pero no es el único también existen otros protocolos como Internet*Control Message Protocol* (ICMP) el cual se encarga de entre varias cosas la de realizar pruebas de conectividad, o Internet*Group Management Protocol* (IGMP) los cuales van encapsulados en un datagrama IP.

1.4.2.3 Capa Transporte [19] [24]

La capa transporte permite la comunicación entre aplicaciones que se ejecutan en maquinas remotas, estableciendo una comunicación punto a punto.

En la capa transporte se hallan definidos dos protocolos, el protocolo TCP (*Transmission Control Protocol*) el cual permite enviar los datos de extremo a extremo de una conexión, con la posibilidad de un mecanismo de detección y corrección de errores, y el protocolo UDP (*User Datagram Protocol*) que al contrario de TCP no ofrece ningún mecanismo de detección y corrección de errores, reduce al máximo la cantidad de información que se incluye en la cabecera de cada datagrama, produciendo una mayor rapidez en el procesamiento de los datagramas a costa de sacrificar la fiabilidad en la transmisión de datos.

1.4.2.4 Capa Aplicación [19] [24]

La capa aplicación es la capa más alta de la estructura jerárquica del protocolo TCP/IP, en esta capa se encuentran las diferentes aplicaciones y proceso con los cuales interactúa e intercambia información la capa transporte, en esta capa se encuentran definidos varios protocolos que dan soporte a aplicaciones de conexión remota, correo electrónico, transferencia de archivos entre otras.

Los protocolos más comunes que se encuentra en la capa aplicación esta, HTTP (Hypertext Transport Protocol), HTTPS (Hypertext Transport Protocol Secure), FTP (File Transfer Protocol), SMTP (Simple Mail Transport Protocol), POP (Post Office Protocol), DNS (Domain Name System), DHCP (Dynamic Host Configuration Protocol), TELNET (Telecommunication Network), TFTP (Trivial File Transport Protocol), LDAP (Lightweight Directory Access Protocol), SSH (Secure Shell).

1.4.3 PROTOCOLO IP [22] [24]

El protocolo IP es el gran protagonista de la capa Internet, debido a que este protocolo interactúa por un lado con los protocolos host a host de alto nivel y por

otro con el protocolo de la red local, La figura 1.15 muestra la relación que existe entre los protocolos de TCP/IP.

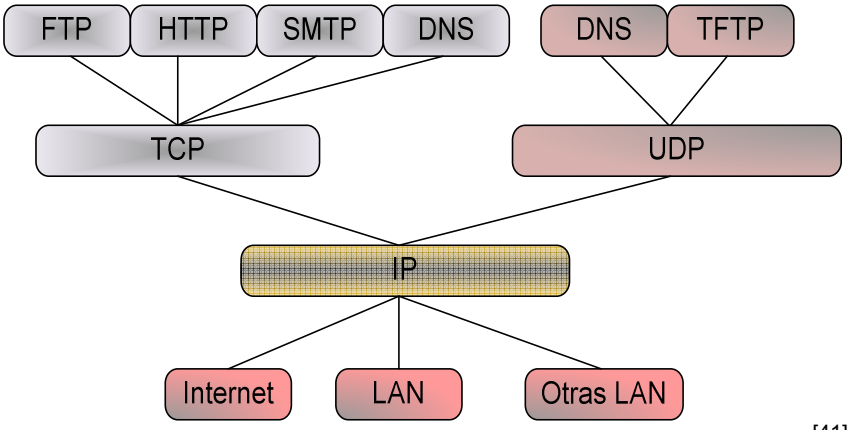


Figura 1.15: Relación entre los Protocolos de TCP/IP [41]

El protocolo Internet se encuentra diseñado para redes de conmutación de paquetes no orientadas a conexión, es decir que cuando se requiere intercambiar datos “datagramas IP” entre dos sitios, para establecer la sesión no se necesita del intercambio previo de información, de igual forma IP no se encarga de comprobar si se han producido errores de transmisión, esta función es confiada a las capas superiores a toda esta función se la conoce como la técnica del mejor esfuerzo.

El protocolo IP cubre tres aspectos importantes:

- Define la unidad básica para la transferencia de datos en una red, especificando el formato exacto de un Datagrama IP.
- Realiza las funciones de enrutamiento.
- Define las reglas para que los Host y Routers procesen paquetes, los descarten o generen mensajes de error.

Un datagrama es el formato que debe tener un paquete de datos en la capa de red. La Figura 1.16 representa la estructura de un datagrama: muestra las seis primeras palabras de la cabecera y el punto desde el que se comienzan a transmitir los datos.

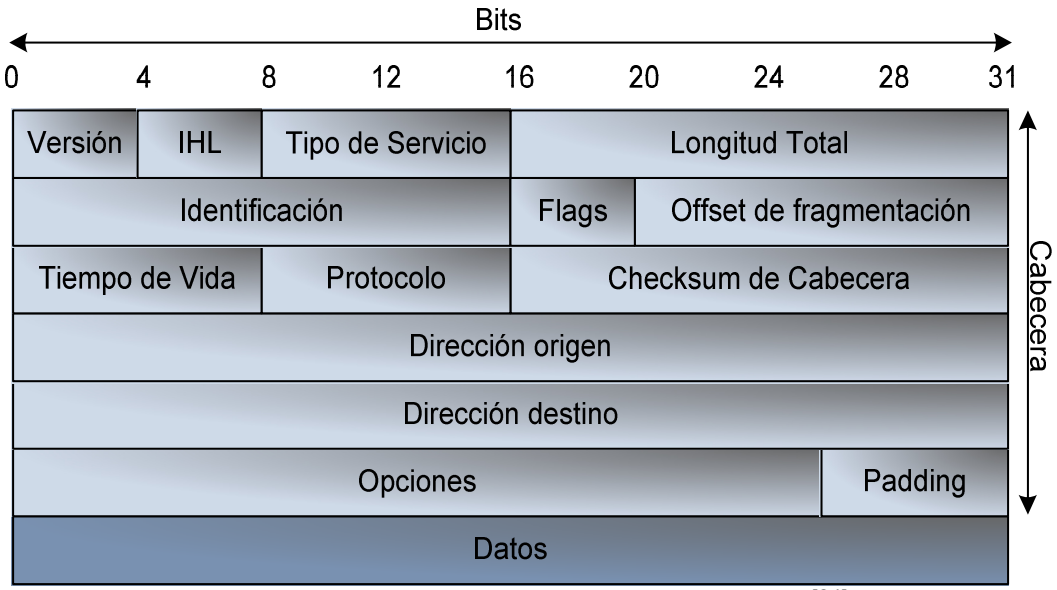


Figura 1.16: Formato del datagrama IP [24]

Versión: El campo versión de 4 bits indica el formato de la cabecera Internet, la versión del protocolo IP, IPv4 = 4 (0101) e IPv6 = 6 (0110).

IHL (*Internet Header Length*): *Campo de 4 bits que* indica la longitud de la cabecera IP en palabras de 32 bits, como mínimo se tiene una longitud de 5.

ToS: PPPDTRC0: El campo de 8 bits nos indica de una manera abstracta los parámetros para especificar una especie de QoS; los 3 primeros bits indican la prioridad de un datagrama IP, se disponen de 8 combinaciones posibles de prioridad, pero 2 se encuentran reservadas para uso interno de la red. Los bits D,T,R y C fueron bits ideados para especificar el retraso, el flujo de salida de datos, la fiabilidad y el costo D, el retraso (0: normal, 1: bajo), T el throughput y R la fiabilidad (0: normal, 1: mejor), C el costo (0: normal, 1: bajo).

Longitud Total: Campo de 16 bits que especifica la longitud de todo el datagrama IP, en octetos, permite un máximo 65535 octetos.

Identificación: Campo de 16 bits que se utilizan para distinguir fragmentos de distintos datagramas, mediante el uso de números de secuencia.

Banderas (*Flags*): Campo de 3 bits, el primer de estos es un bit reservado, seguido de un bit denominado DF (*Don`t fragment*), indica si el datagrama puede

ser o no fragmentado si este bit es 0 el datagrama puede ser fragmentado y si esta en 1 no puede ser fragmentado, a continuación se tiene el MF (*More Fragment*), indica si el datagrama es un fragmento de datos, si este bit esta en 0 indica que es el último de los fragmentos o el datagrama no ha sido fragmentado, si en cambio esta en 1, indica que es uno más de los fragmentos e indica que existen más fragmentos.

Offset: Campo de 13 bits, se utiliza cuando se fragmenta e indica el desplazamiento (en palabras de 64-bits) de ese datagrama dentro del fragmento, el primero es cero.

TTL: Campo de 8 bits, indica el número de saltos (o tiempo) máximo para el datagrama. Este campo se modifica “en el camino” y disminuye en cada salto.

Protocolo: Campo de 8 bits, que indica el protocolo de nivel superior que se transporta en el datagrama IP (1=ICMP, 6=TCP, 17=UDP).

Checksum: Campo de 16 bits, que realizan una suma de control sobre la cabecera únicamente, esta suma es calculada y verificada en cada punto donde es procesada debido a que algunos campos de la cabecera son modificados.

Dirección origen y dirección destino: Campos de 32 bits cada uno, indica la dirección de la fuente y la dirección de destino del datagrama.

Opciones: Campo de longitud variable, las opciones pueden aparecer o no, pero que deben reconocerse. El relleno sirve para que toda la cabecera sea múltiplo de 32-bits, los campos opcionales pueden llegar hasta valores de 40 bytes.

Existen varias versiones del protocolo IP, IPv4 es en la actualidad la más empleada, aunque el crecimiento exponencial en el tamaño de las redes compromete cada vez más su operatividad.

El número de equipos que IPv4 puede direccionar comienza a ser insuficiente, para lo cual se ha desarrollado la versión IPv6, con una capacidad de direccionamiento muy superior a IPv4, pero totalmente incompatible.

1.4.4 PROTOCOLOS DE TRANSPORTE [6] [30]

1.4.4.1 *Transmission Control Protocol* (TCP)

El Protocolo Control de Transmisión fue diseñado para proporcionar un flujo de datos confiables sobre redes no confiables, es un protocolo de transporte orientado a conexión, ofreciendo de esta manera que los datos sean entregados sin errores sin omisión y en secuencia, las aplicaciones solicitan establecer una conexión a su extremo previo a su envío por la conexión TCP establece una conexión punto a punto en la cual los dos extremos pueden intercambiar datos en ambas direcciones y en esta conexión ofrece la confiabilidad de los datos, garantizando que los datos no sean perdidos, duplicados o lleguen con errores de transmisión, TCP cumple un gran número de funciones como lo son:

- Asociar puertos con conexiones.
- Establecer conexiones usando un acuerdo en tres pasos.
- Realizar un arranque lento para evitar sobrecargas.
- Dividir los datos en segmentos para su transmisión.
- Numerar los datos.
- Manejar los segmentos entrantes duplicados.
- Calcular las sumas de control.
- Regular el flujo de datos usando las ventanas de envío y recepción.
- Terminar las conexiones de manera ordenada.
- Abortar conexiones.
- Marcar datos urgentes.
- Confirmación positiva de retransmisión.
- Cálculo de los plazos de retransmisión.
- Reducir el tráfico cuando la red se congestiona.
- Indicar los segmentos que llegan en desorden.
- Comprobar si las ventanas de recepción están cerradas.

1.4.4.2 *User Datagram Protocol* (UDP)

El protocolo de datos de usuario fue diseñado para ofrecer a las aplicaciones un mecanismo de envío de un flujo de datos en bruto si tener la necesidad de

negociar una conexión, siendo este un protocolo no orientado a la conexión, y debido a esta característica el protocolo no puede ofrecer detección de errores, acuses de recepción, ni realizar un control de flujo, pudiendo llegar los datos de una manera desordenada, el protocolo UDP es utilizado para aplicaciones en las cuales se disponen de flujos de datos masivos y su información transmitida no es lo suficiente rentable ni propensa a retardos con respecto a la cantidad de datos transmitidos.

1.4.4.3 Puertos TCP y UDP

En TCP y UDP existe el concepto de puertos, donde un puerto es la interfaz que se encuentra entre la capa transporte y el proceso local “una Aplicación”, identificando de esta forma las diferentes aplicaciones emisoras y receptoras, para que una aplicación pueda acceder a la red y pueda enviar datos a través de ella, debe hacerlo a través de un puerto, un puerto para enviar el flujo de datos y en el otro extremo de la conexión la aplicación receptora lo hace a través de otro puerto.

Los puertos se identifican mediante un número decimal que va desde el 0 hasta el 65535, tanto en TCP como en UDP. Los fabricantes que implementan TCP disponen de una gran libertad para asignar números de puertos a los procesos, aunque la Autoridad de Números Asignados de Internet (IANA) ha dedicado un rango que va desde el 0 al 1.023 a una serie de procesos comunes (RFC 1700) como telnet, ftp, pop3, smtp, etc.

Cada vez que un cliente quiere una conexión pide al sistema operativo que le asigne un número de puerto en desuso, sin reservar. Al finalizar la conexión, el cliente devuelve el puerto al sistema y lo puede utilizar otro cliente.

1.5 PROTOCOLOS IGP Y EGP [31]

1.5.1 INTRODUCCION:

El enrutamiento es el proceso de traslado de datos desde una red a otra, el enrutamiento es innecesario a menos que existan múltiples redes en diferentes

rangos de direcciones o diferentes combinaciones de direcciones IP y máscaras de subred. Si una red se va a conectar a la Internet, se debe pensar sobre la ejecución de más de un tipo de protocolo de enrutamiento.

Dominios de enrutamiento individuales son interconectados para formar redes más grandes, tales como Internet, que permite transferencia de datos de un dominio de enrutamiento a otro en una extensión geográfica extensa. Los routers usan protocolos de enrutamiento para conocer varios lugares dentro de los dominios de la red local o remota. Los dos tipos básicos de protocolos de enrutamiento son los IGP y EGP.

1.5.2 FUNDAMENTOS

1.5.2.1 Sistemas Autónomos [8] [9]

Un sistema autónomo (*autonomous system* “SA”) se define como un conjunto de routers o redes que comparten una política de enrutamiento y se encuentran bajo una sola administración técnica, generalmente usan un solo protocolo de enrutamiento interior (IGP) o un conjunto de estos. Otros proveedores de servicio lo miran con una sola entidad, que tiene un número identificador asignado. Para intercambia la información de enrutamiento entre dominios surge BGP.

Los protocolos de enrutamiento exterior y la división en sistemas autónomos surgen para disminuir el crecimiento de las tablas de enrutamiento y proporcionar una vista estructurada de Internet dividida en redes más pequeñas y manejables que definen su propio conjunto de reglas y políticas asociadas a sus necesidades y servicios ofrecidos. Se agrupan en tres categorías:

1.5.2.1.1 *SA de Conexión Única*

Un sistema de conexión única mostrado en la figura 1.17, es aquel que alcanza redes exteriores a su dominio a través de un único punto de salida este tipo de configuración se da entre un proveedor y su cliente donde en el lado del cliente la configuración se facilita pues al tener una única salida con una ruta por defecto se envía todo el tráfico.

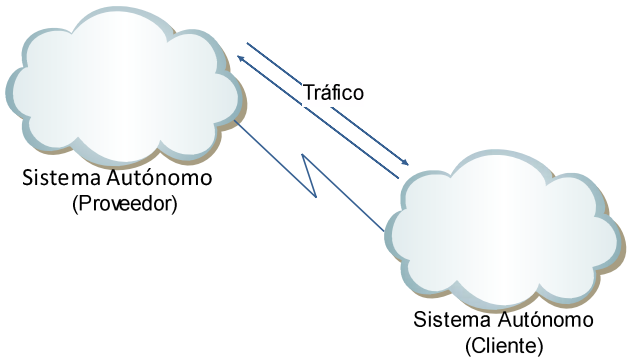


Figura 1.17: Sistema autónomo de conexión única [9]

En el lado del proveedor se tiene tres opciones, una es enumerar las subredes del cliente como entradas de su router; no se usa este método si el cliente tiene varias subredes discontinuas; el segundo método es usar un IGP entre el cliente y el proveedor lo cual no es muy usado por la inestabilidad que presentan este tipo de enlaces y el tercer método es utilizar una sesión BGP entre el cliente y el proveedor donde se usa un número de SA del rango privado.

1.5.2.1.2 *SA de Múltiples Conexiones sin Tránsito*

Un SA que tiene más de un punto de salida al exterior se conoce como de múltiples conexiones, para lo cual se conectará con dos o más sistemas autónomos, esto se observa en la figura 1.18; el término sin tránsito hace referencia a que aquel tráfico cuyo origen y destino están fuera del SA no pasará a través de él. Este tipo de sistemas solo publican sus propias rutas, en caso de que una ruta sea aprendida de algún otro SA estas no se propagan de esta manera filtra el tráfico.

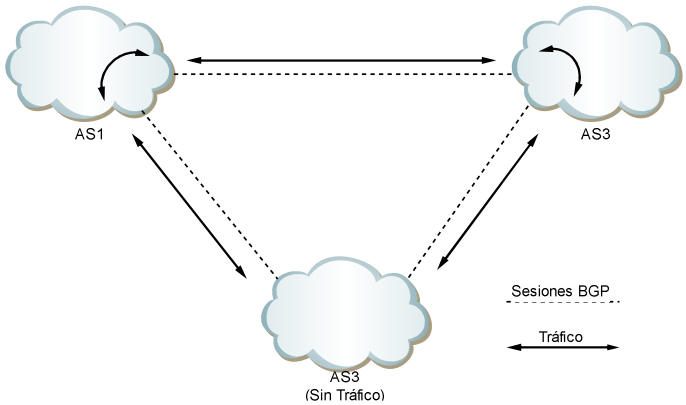


Figura 1.18: Sistemas de múltiples conexiones [9]

1.5.2.1.3 *SA de Tránsito con Múltiples Conexiones.*

Un SA de este tipo tiene múltiples conexiones con otros SA y el tráfico originado en otros SA puede pasar a través de él, este tipo de sistemas publica sus rutas y las que aprende de sus vecinos. Esto se observa en la figura 1.19.

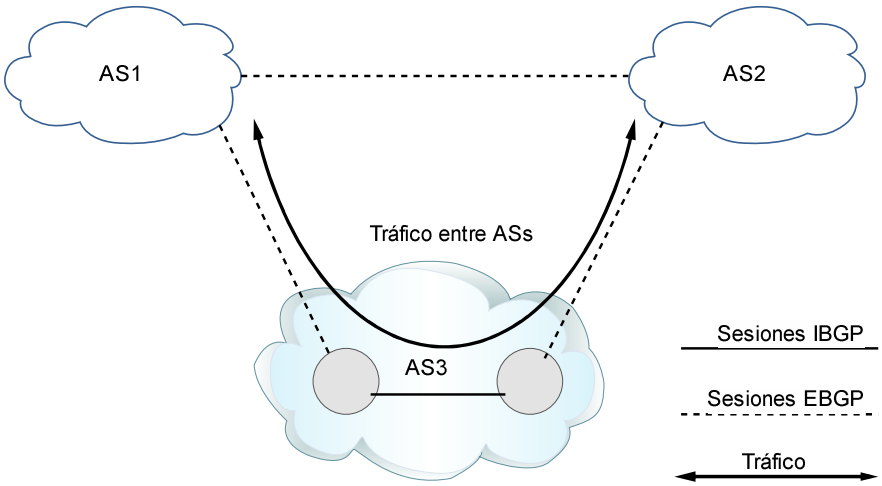


Figura 1.19: Sistemas autónomos de múltiples conexiones [8]

1.5.2.2 IGP (*Interior Gateway Protocol*)

IGP hace referencia a los protocolos de pasarela interior, los cuales han sido optimizados para encargarse del encaminamiento de paquetes dentro de un grupo de routers que se encuentran bajo la administración de una sola entidad o único dominio, a lo cual se lo conoce como sistema autónomo.

1.5.2.3 EGP (*Exterior Gateway Protocol*)

EGP hace referencia a los protocolos de pasarela exterior, los cuales han sido optimizados para encargarse del encaminamiento de información de enrutamiento entre sistemas autónomos.

1.5.3 IS-IS [7] [16] [32] [33] [34] [35] [36]

1.5.3.1 Introducción

El protocolo de Sistema Intermedio a Sistema Intermedio “IS-IS” fue desarrollado por *Digital Equipment Corporation* como parte de DECnet Fase V. Fue estandarizado por ISO en 1992 como ISO 10589 para la comunicación entre los

dispositivos de red que son llamados los sistemas intermedios por la ISO. El propósito de IS-IS era hacer posible el encaminamiento de datagramas usando ISO en desarrollo OSI *protocol stack* llamado CLNS.

El IS-IS fue desarrollado al mismo tiempo en que el Internet*Engineering Task Force* "IETF" desarrollaba un protocolo similar llamado OSPF. El IS-IS fue extendido más adelante al encaminamiento de datagramas usando protocolo IP, esta versión del encaminamiento IS-IS fue llamado IS-IS integrado.

El IS-IS se ha conocido más extensamente en los últimos años, y se ha convertido en una alternativa viable al OSPF en redes de empresas. Sin embargo un análisis detallado, tiende a demostrar que el OSPF tiene características que moderan el tráfico, especialmente conveniente a las redes de empresa, mientras que el IS-IS tiene características de estabilidad especialmente convenientes a la infraestructura de un ISP.

1.5.3.2 Definición

Sistema Intermedio - Intermedio es un protocolo de estado de enlace similar a OSPF que se utiliza con las grandes empresas y clientes ISP, se encarga del enrutamiento de los paquetes entre los sistemas intermedios, utiliza una base de datos de estado de enlace y se ejecuta el algoritmo SPF Dijkstra para seleccionar las rutas más cortas. El protocolo ISIS no está diseñado para encaminar entre Sistemas autónomos, un trabajo que es realizado por un *Exterior Gateway Protocol* (EGP), por ejemplo *Border Gateway Protocol* (BGP).

El protocolo de enrutamiento de Sistema Intermedio a Sistema Intermedio (IS-IS) converge rápidamente y es muy escalable. Es además un protocolo muy flexible que ha destacado las características límites como Multiprotocol Label Switching Traffic Engineering (MPLS/TE).

Especificado originalmente por la ISO, es un protocolo dinámico, de estado de enlace, ínter dominio y de interior (IGP), muy escalable y que converge rápidamente. Opera en un ambiente de servicio sin conexión OSI (CLNS),

seleccionando rutas sobre una métrica de costo asignada manualmente a los enlaces por un administrador como el valor de la ruta a un router vecino.

Características de IS-IS

- Enrutamiento jerárquico
- Comportamiento sin clases
- Inundación rápida de nueva información
- Convergencia rápida
- Muy escalable
- Sintonizador de tiempo flexible

1.5.3.3 Terminología OSI [35]

En una red OSI, existen cuatro entidades dispuestas: los Host, las Áreas, el Backbone, y un dominio. Un dominio es una porción de una red OSI que está bajo una autoridad administrativa en común, dentro de cualquier dominio OSI, pueden existir una o más áreas definidas.

Un área es una entidad lógica, formada por un grupo de routers contiguos y los enlaces que lo interconectan entre sí, todos los routers de una misma área intercambian información sobre todos los host que ellos pueden alcanzar, las áreas se conectan desde y hacia el backbone, y todos los routers que coexisten en el backbone saben cómo alcanzar todas las áreas que se encuentran enlazadas al mismo.

El término Sistema Final (ES) se refiere a cualquier host o nodo sin enrutamiento, mientras que el término Sistema Intermedio (IS) se refiere a un router, esto se muestra en la figura 1.20.

Un NSAP es un punto conceptual en el borde entre la capa red y la capa de transporte, es la ubicación en la cual los servicios de red OSI se proveen a la capa de transporte, cada entidad de la capa de transporte es asignada a un simple NSAP.

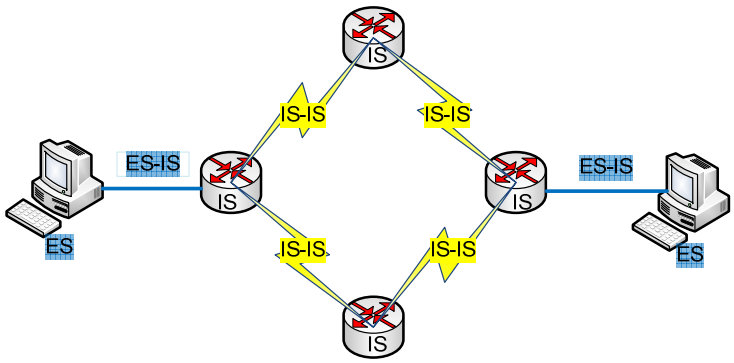


Figura 1.20: Sistemas Intermedios y sistemas finales [26]

1.5.3.4 ES-IS e IS-IS [35]

ISO ha desarrollado estándares para dos tipos de protocolos de red usados en enrutamiento. Esos dos protocolos son ES-IS e IS-IS. El protocolo de descubrimiento ES-IS es usado para enrutamiento entre Sistemas Finales y Sistemas Intermedios comúnmente es usado con protocolos de enrutamiento para proveer movimientos de datos end-to-end por una red, el enrutamiento entre sistemas finales y sistemas intermedios es referido en algunas ocasiones como enrutamiento de nivel 0. El protocolo de enrutamiento IS-IS es usado para enrutamiento jerárquico entre sistemas intermedios.

1.5.4 IS-IS INTEGRADO. [32] [35] [36]

IS-IS integrado es una implementación del protocolo IS-IS para enrutamiento de múltiples protocolos. IS-IS integrado etiqueta las rutas CLNP, sobre la cual IS-IS basa la base de datos de estado y enlace, con información de redes IP y subredes. IS-IS provee una alternativa a OSPF en el mundo IP, mezclando ISO CLNS y enrutamiento IP en un protocolo. Además, IS-IS puede ser usado solamente para enrutamiento IP, o solamente para enrutamiento ISO o para una combinación de los dos.

IS-IS integrado es desarrollado extensivamente en un ambiente IP solamente en la primera fase de las redes de proveedores de servicios de Internet (ISP). El grupo de trabajo IS-IS de la IETF desarrolló la especificación para IS-IS integrado, RFC 1195.

IS-IS es uno de los pocos protocolos que provee un entramado integrado para procesamiento concurrente de más de un protocolo de capa de red. Otros protocolos de enrutamientos, como OSPF, usualmente soportan enrutamiento para un solo tipo de protocolo de capa 3.

IS-IS no fue diseñado específicamente para enrutamiento IP, más, el correcto comportamiento general para el enrutamiento IP en Internet ha llevado a la IETF a revisar el RFC 1195, para incorporar características propietarias fuera del rango del diseño del 1195, para proveer usabilidad, flexibilidad y escalabilidad.

El protocolo IS-IS integrado provee enrutamiento dinámico para ambientes de *interworking* IP e ISO. IS-IS integrado tiene las siguientes características:

- Usa ISO IS-IS para distribuir información de enrutamiento.
- Provee servicios de enrutamiento ISO e IP.
- Las rutas solo dentro de un dominio ISO.
- Realiza la distribución de información del estado de enlace, para el enrutamiento.
- Basado en el algoritmo de enrutamiento *shortest-path-first.*
- IS-IS integrado provee enrutamiento IP con las siguientes capacidades:
    - Definición de enlaces con direccionamiento IP, subredes y métrica.
    - Envía información de enrutamiento IP dentro de las PDUs de los paquetes ISO IS-IS.
    - Configurando un área para soportar IP o ambos IP y CLNP.

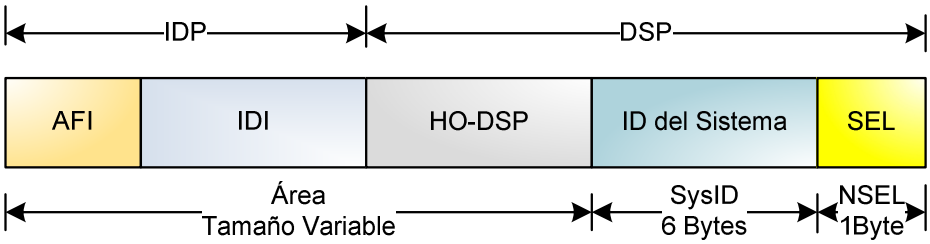
1.5.5 DIRECCIONES NSAP [7] [36]

Para el funcionamiento de IS-IS son necesarias las direcciones CLNS "*Connectionless Network Service*" incluso si el router solo está configurado con IP, el direccionamiento de la capa de red en OSI es efectuado aplicando las direcciones CLNS, y se denominan NSAP "*Network Service Access Points*".

La dirección NSAP identifica cualquier sistema en una red OSI, estas direcciones poseen varios formatos que son usados para varios sistemas, dependiendo de los

diferentes protocolos se pueden usar representaciones diferentes de NSAP. Una dirección NSAP es usada por cada dispositivo, y no por cada interfaz.

La estructura de direccionamiento NSAP se muestra en la figura 1.21:



Tamaño total NSAP mínimo de 8 bytes y máximo de 20 bytes

IDP	Initial Domain Part
DSP	Domain Specific Part
AFI	Authority and Format Identifier
IDI	Initial Domain
HO-DSP	High Order Domain Specific Part
SEL	NSAP Selector (NSEL)
Area	Area prefix in an NSAP

Figura 1.21: Estructura de direccionamiento NSAP [7]

PDUs de estado de enlace “LSP”, PDUs Hello, y otras PDUs de enrutamiento son PDUs formateadas según la estructura OSI, así, cada router IS-IS requiere una dirección OSI, IS-IS usa la dirección OSI en los PDUs LSPs para identificar al router, y de esta manera construye la tabla topológica, y construye el árbol de enrutamiento IS-IS subyacente. Las direcciones NSAP contienen la dirección OSI del dispositivo y proveen un enlace a los procesos de capas superiores. Las direcciones NSAP pueden ser vistas como el equivalente a la combinación de una dirección IP y el identificador del protocolo de capa superior de un encabezado IP.

Una dirección NSAP consiste de tres partes, la dirección del área, el ID del sistema y el byte selector NSAP. La dirección del área es un campo de largo variable compuesto de ocho octetos ordenados, excluyendo el ID del sistema y el byte selector. El ID del sistema es el identificador del ES o IS en un área, tiene un largo fijo de seis bytes en el diseño del IOS Cisco. El byte N-Selector es un identificador de servicio. El rol del byte N-Selector es análogo al de un puerto o socket en TCP/IP.

***Authority and Format* ID (AFI)**: Un byte, actualmente un valor binario entre 0 y 99, indica el dominio de direccionamiento superior asociado con el NSAP y la sintaxis de la sección DSP, los dominios de direccionamiento de nivel superior originan varios subdominios, que se les asigna un valor en el campo de la IDI. Cada dominio de primer nivel especifica su propio formato, para el campo de la IDI los valores asignados se observan en la tabla 1.2.

Address Domain	*DSP Syntax*		
	Decimal	***Binary***	***Character***
X.121	36	37	-
ISO DCC	38	39	-
F.69	40	41	-
E.163	42	43	-
E.164	44	45	-
ISO 6523 ICD	46	47	-
Local	48	49	50

Tabla 1.2- Tabla de valores AFI. [7]

***Inter-Domain* ID (IDI):** Identifica el dominio.

***Inter-Domain Part* (IDP):** Consiste del AFI e IDI juntos. Esto es aproximadamente equivalente a una red IP classfull. En formato decimal.

***High-Order* DSP (HODSP):** Usado para subdividir el dominio en áreas. Esto es aproximadamente equivalente a una subred en IP.

***System* ID:** Identifica un dispositivo OSI individual, un dispositivo tiene una dirección, así como en DECnet, mientras que en IP una interfaz tiene una dirección.

***NSAP-Selector* (NSEL):** Identifica un proceso en el dispositivo. Esto es aproximadamente equivalente a un puerto o socket TCP/IP. Los valores de este campo se observan en la tabla 1.3.

Valores NSEL	Servicios de Usuario de Red
0x00	Capa Enrutamiento (por ejemplo, IS-IS)
0x21	DECNet fase IV capa Transporte
0x22	Capa transporte OSI TP4

Tabla 1.3- Valores NSAP-Selector[7]

***Domain-Specific Part* (DSP)**: Comprendido del HODSP, el ID del sistema y el NSEL en formato binario.

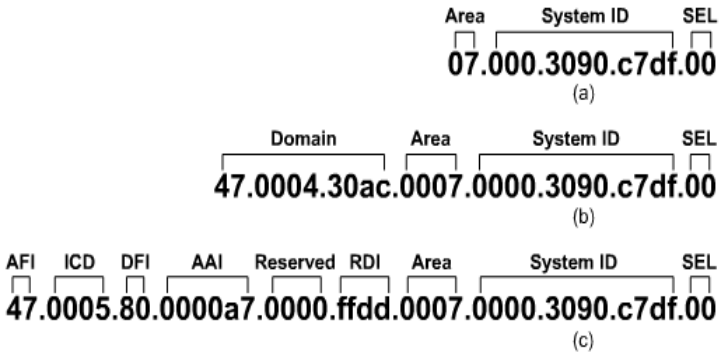


Figura 1.22: a) formato de 8 byte el área ID y el ID del sistema. b) formato NSAP OSI. c) formato NSAP gobernado por el perfil OSI (GOSIP) [7]

El protocolo Internet se encuentra diseñado para redes de conmutación de paquetes no orientadas a conexión, es decir que cuando se requiere intercambiar datos “datagramas IP” entre dos sitios, para establecer la sesión no se necesita del intercambio previo de información, de igual forma IP no se encarga de comprobar si se han producido errores de transmisión, esta función es confiada a las capas superiores a toda esta función se la conoce como la técnica del mejor esfuerzo.

1.5.6 NETs (*NETWORK ENTITY TITLE*) [7] [35] [36]

Una dirección NSAP con un valor NSEL de 00 es usado para identificar un dispositivo, la cual es la dirección de red de este dispositivo, y en este caso, el NSAP es conocido como un NET, el 00 indica que no hay una entidad de capa de transporte asociada con esta dirección, por esa razón, la NSAP de un router es

referida siempre como una NET, y de esta manera la NET se encuentra determinado por el ID del área y el ID del sistema.

En general. La gran diferencia entre el estilo de direccionamiento NSAP y el direccionamiento estilo IP es que se usa una simple dirección NSAP para todo el router, y no como IP con una dirección IP por interfaz.

Es posible configurar múltiples NETs en un router, pero un router no está siempre en más de un área, si múltiples NETs son configuradas en el mismo router, todas ellas deben tener el mismo ID de sistema. Las NETs son usadas por los routers para identificarse a sí mismos en las LSPs y formar lo básico para el cálculo de rutas OSI. Las direcciones que comienzan con el valor AFI = 49, son consideradas como direcciones privadas. Esas direcciones son ruteadas por IS-IS. Sin embargo, este grupo de direcciones no debe ser publicado a otras redes CLNS, las direcciones que comienzan con valor AFI de 39 y 47, respectivamente, representan el dato ISO de código de país y designado código internacional ISO.

1.5.7 LAS PDUs DE IS-IS [35]

Las PDUs IS-IS son encapsuladas directamente dentro de una trama de la capa de enlace de datos de OSI. No hay cabecera CLNP ni tampoco cabecera IP.

Los paquetes IS-IS tienen tres categorías, los PDU Hello, PDUs estado de enlace “LSP”, PDUs secuencia

- PDU Hello (ESH, SH, Hello IS-IS {IIH}) usadas para establecer y mantener las adyacencias.
- LSP usadas por IS-IS para distribuir información de estado y enlace. Hay pseudonodos y no-pseudonodos los LSPs son independientes para el nivel 1 y el nivel 2.
- PDUs de Secuencia dentro de los cuales se pueden describir dos tipos:
    - El número de secuencia completo de PDU (CSNP) usado para distribuir una base de datos completa del estado de enlace en el router. Las CSNPs son usadas para distribuir información a otros router de LSPs que pueden estar con fecha incorrecta o desaparecida de su

propia base de datos, asegurando que la misma información se encuentre en todos los router y que se encuentren sincronizadas.

- Número de secuencia parcial de PDU (PSNP) – Usado para acusar recibo y consultar información de estado y enlace.

1.5.7.1 Formato de los PDUs IS-IS [36]

Las PDUs IS-IS se compone de una cabecera y una serie de campos de longitud variable que contienen información específica relacionada con enrutamiento, y estos dependen de la función que cumpla el PDU, cada campo de longitud variable contiene una etiqueta tipo la cual almacena un código que identifica el tipo de información que se envía en la PDU IS-IS y la forma como se debe tratar la etiqueta valor, por ejemplo el código 128 simboliza un mensaje IP.

La etiqueta longitud la cual almacena la extensión de la siguiente etiqueta que se denomina valor, la cual puede tomar la forma de diferentes tipos de información, como rutas IP, vecinos IS, o autenticación, el tipo de información dependen del código que se tenga en la etiqueta tipo.

Por esa razón, la abreviación TLV es usada para tipo, longitud y valor del campo de longitud variable, siendo un formato que proporciona flexibilidad y extensibilidad al protocolo IS-IS ya que cuando sale un protocolo nuevo que se quiere integrar en IS-IS, sólo hace falta crear un TIPO nuevo de TLV.

1.5.7.1.1 *La cabecera IS-IS*

Discriminador de protocolo de enrutamiento intradominio: identificador de la capa de red asignado a IS-IS en la ISO 9577. el valor binario es 10000011 (0x83).

Indicador de longitud: Específica la longitud de la cabecera, fijado en bytes.

Versión/ID de protocolo Extensión: Actualmente tiene un valor de 1.

Longitud de ID: Longitud del campo de identificación de sistema “SysID”. Si este campo está puesto en 0, implica una longitud de seis bytes, un valor de 255

implica una longitud de 0 bytes. Otros posibles valores son de 1 a 8 para longitud real en bytes.

Reservado: Bits reservados, no son utilizados se establecen con un valor de 0 que indica reservado.

Tipos de PDU: Específica el tipo de PDU IS-IS que transporta.

Versión: El valor es 1.

Direcciones de área máximas: Número de direcciones por área IS. Los valores están entre 1 y 254 para números actuales. Cero implica un máximo de tres direcciones por área IS.

El formato de la cabecera IS-IS se muestra en la figura 1.23, los campos son:

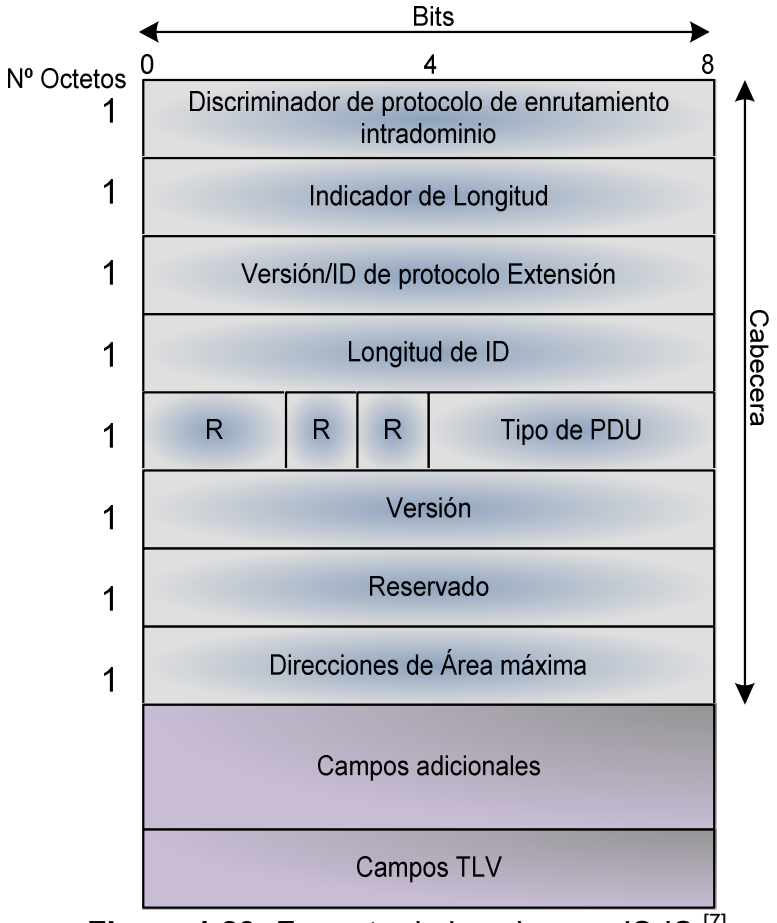


Figura 1.23: Formato de la cabecera IS-IS [7]

1.5.7.1.2 *PDU IS-IS LAN HELLO*

Además de la cabecera común de un paquete IS-IS en el caso de la PDU IS-IS LAN Hello se tienen como campos adicionales de cabecera los siguientes campos:

Reservado/tipo de circuito: Como campo reservado se establecen los 6 primeros bit, seguidos de 2 bits que con un valor = 0 indica reservado, con un valor = 1 indica nivel 1, con un valor 2 indica nivel 2, y con un valor 3 indica nivel 1 y 2.

ID de origen: Indica la identificación del sistema "SysID" del router transmisor.

Timer de espera: Establece el tiempo que debe esperar el router receptor por los hellos del router transmisor antes de eliminar la adyacencia y declarar muerto este router.

Longitud de PDU: Longitud de la PDU completa, cabecera fija y TLVs.

Reservado/prioridad: El octavo bit de este byte se encuentra reservado y su valor establecido con un valor = 0, los restantes 7 bit son usado para establecer la prioridad del sistema intermedio designado "DIS" de nivel 1 o nivel 2. Este valor es copiado desde el IIH del DIS.

LAN ID: Un campo compuesto de la identificación del sistema del DIS, de 1 a 8 bytes, más un octeto de orden bajo asignado por el DIS LAN de nivel 1.

En el caso de los paquetes IS-IS hello, estos son rellenados a su tamaño máximo de la unidad de transmisión (MTU), con la ayuda del relleno se obtiene la detección temprana de errores a causa de problemas en la transmisión, pero de igual forma se tienen inconvenientes, en el caso de interfaces de alta velocidad el relleno puede causar el abuso de enormes buffers y en interfaces de baja velocidad causar el desperdicio de ancho de banda, afectando a aplicaciones sensibles al tiempo tales como voz sobre IP (VoIP).

Al final del paquete IS-IS se encuentran los campos de longitud variable, es aquí donde se almacenan la información TLV, en el caso de encontrar un código que

no sea reconocido este paquete es ignorado. El formato del PDU IS-IS LAN HELLO se muestra en la figura 1.24.

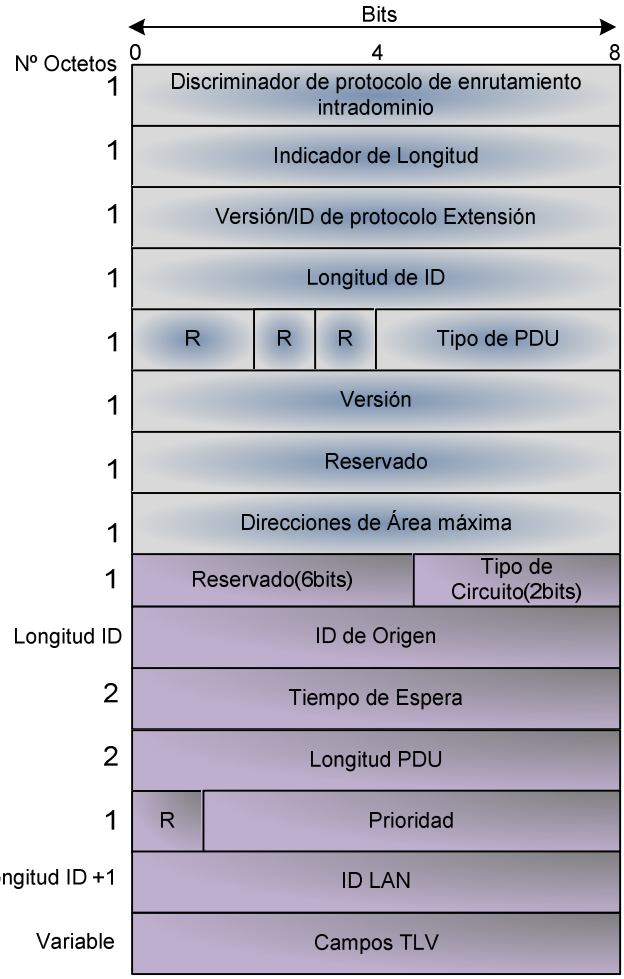


Figura 1.24: Formato PDU IS-IS LAN HELLO [7]

1.5.7.1.3 *PDU de Estado y Enlace IS-IS (LSP)*

Longitud de la PDU: Longitud de la PDU completa, cabecera fija y TLVs.

Tiempo de vida restante: tiempo restante en segundos antes que las LSP expiren.

LSP ID: Distingue LSPs unos de otros y para identificar los routers de origen, consiste de tres componentes, el ID del sistema, el ID del pseudonodo y el número de fragmentación LSP

Número de secuencia: Es un valor de secuencia para las LSPs, es usado para sincronización, un valor de secuencia mayor indica nuevas LSP. Permitiendo de esta manera a los routers que reciben las LSP asegurarse usar sólo las últimas

LSPs en su cálculo de rutas, y evitar que LSPs duplicadas ingresen dentro de las tablas topológicas.

Cuando hay un cambio, el número de secuencia es incrementado y una nueva versión de la LSP es generada con el nuevo número de secuencia. Cuando un router se reinicia, el número de secuencia es puesto en uno, pero el router puede entonces recibir sus propias LSPs de vuelta desde los vecinos. Los cuales tendrán el último número de secuencia correcto antes de que el router se reinicie. El registra este número y rehúsa su propio LSP con el próximo número de secuencia mayor

Checksum: Es calculado desde el ID fuente hasta el final de la PDU. Usado para detectar errores de chequeo. El Checksum es calculado sobre la LSP recibida y revisada contra el checksum dentro de la LSP.

Partición (P): Octavo bit del octeto. Cuando está en uno, significa que el originador del LSP soporta reparación de partición.

Bit Atachado (ATT): Desde el bit 4 hasta el bit 7 del octeto. Cuando cualquiera de estos bits están en uno, indican que el originador esta unido a otra área usando la siguiente métrica: el bit 4: por defecto, el bit 5: retardo, bit 6: coste, el bit 7: error.

OL (Bit de sobrecarga): Bit 3, cuando está en uno, indica que la base de datos LSP del origen está sobrecargada y sería evitada en el cálculo de rutas a otros destinos, debido a que los recursos de procesamiento y memoria son limitadas.

Tipo IS: Los bits 1 y 2 son usados para indicar el tipo de LSP, nivel 1 o nivel 2 cuando sólo el bit 1 esta puesto indica nivel 1 IS. Si ambos están puestos, ellos indican nivel 2 IS.

Varios tipos de campos TLV se puede incluir en una LSP para propagar diferentes tipos de información de enrutamiento.

En un paquete IS-IS LSP mostrado en la figura 1.25, además de la cabecera común IS-IS se disponen los siguientes campos:

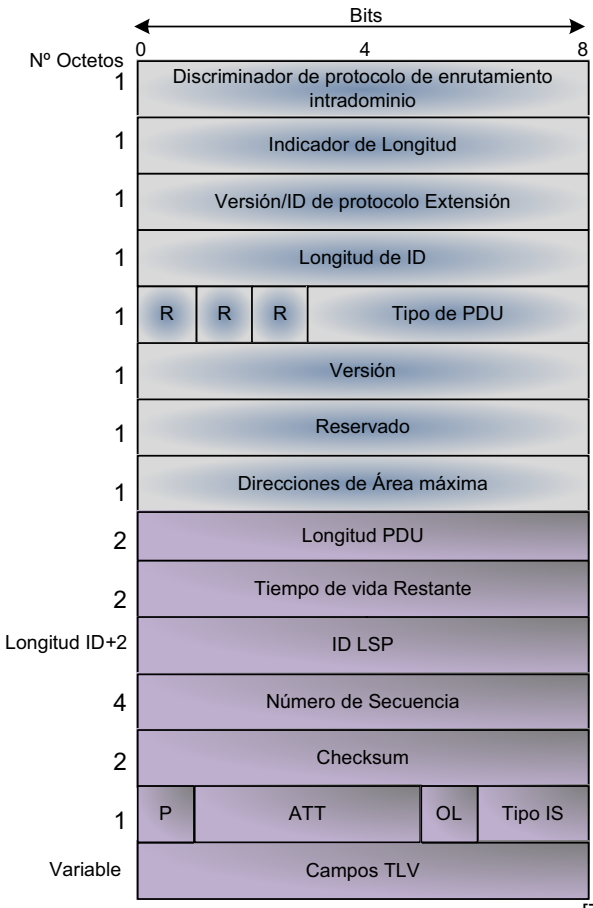


Figura 1.25: Formato PDU LSP IS-IS [7]

1.5.8 NIVELES DE ENRUTAMIENTO EN IS-IS [35]

Nivel 1 (L1): Routers internos responsables del enrutamiento entre sistemas finales ES en un área y la comunica con otro nivel 1 IS en la misma área, y mantienen una base de datos LSP de nivel 1, la cual define el marco del área y los puntos de salida hacia otras áreas vecinas.

Nivel 2 (L2): El nivel 2 IS enruta entre áreas de nivel 1 y forma un backbone de enrutamiento ínter área, los routers L2 almacenan una base de datos separada, la cual contiene solo la información topológica Inter.-área.

Nivel 1 y Nivel 2 (L1L2): En este nivel los routers se encargan del enrutamiento intra-área, conectando a los router L1 dentro del área y el enrutamiento L2 inter-área conectando al router L2 en el backbone, los routers actuando como si estos fuesen dos routers IS distinto, los routers L1L2 operan dos procesos diferentes, un proceso de enrutamiento L1, con su propia tabla topológica L1 y tabla de

adyacencias, para manejar la asociación con otros routers L1 y ES, y un proceso de enrutamiento L2, con una tabla topológica y una tabla de adyacencias independiente, para manejar las asociaciones con los router de backbone vecinos, para lo cual los routers L1L2 soportan una función L1 para comunicarse con los otros router L1 dentro de su área y mantener la información LSP L1 en una base de datos LSP L1. Ellos informan a los otros router que tienen un punto de salida para el área. Ellos también soportan una función L2 para comunicarse con el resto del backbone y mantener una base de datos topológica separada de la base LSP L1.

Con enrutamiento IS-IS, OSI distingue el enrutamiento en 3 niveles, para simplificar el diseño y la operación del router, en la figura 1.26 se muestran los niveles de enrutamiento en IS-IS.

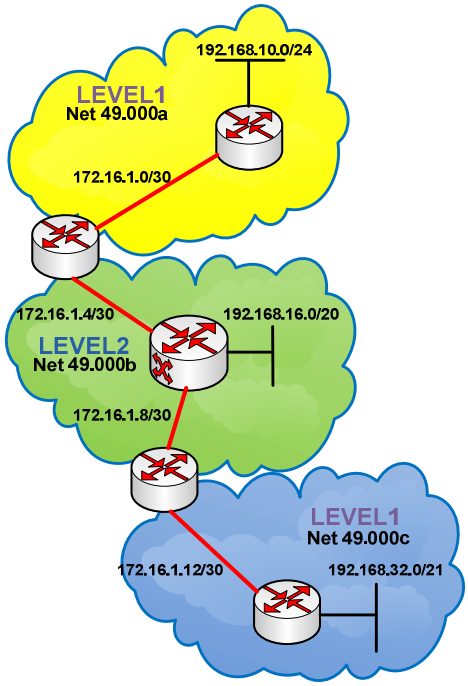


Figura 1.26: Niveles de Enrutamiento IS-IS [35]

1.5.9 SISTEMAS INTERMEDIOS DESIGNADOS (DIS) Y PSEUDONODOS (PSN)

El Sistema Intermedio Designado (DIS) es responsable de conducir la inundación sobre la LAN y así para mantener la sincronización, para lo cual crea y actúa en

nombre de un pseudonodo “un nodo virtual”. Todos los router en la LAN, incluyendo el DIS, forman una adyacencia con el pseudonodo. En vez de inundar y que la sincronización de la base de datos tome lugar sobre n*(n-1) adyacencias, el pseudonodo habilita la reducción de la inundación y la sincronización de la base de datos para ocurrir solo sobre las adyacencias formadas con el pseudonodo. En una LAN, uno de los router será elegido el DIS basado en la prioridad. La prioridad por defecto es 64 el rango configurable es de 0 a 127 si las interfaces tienen la misma prioridad, el router con el mayor SNPA es seleccionado.

1.5.10 PROTOCOLO DE GATEWAY EXTERIOR *(BORDER GATEWAY PROTOCOL)* BGP [12] [25] [26] [37]

El protocolo de Gateway fronterizo es un protocolo de enrutamiento que permite intercambiar información de asequibilidad de redes entre diferentes sistemas autónomos, la selección de una ruta es diferente de la que se maneja dentro del sistema autónomo pues dentro de este se usan métricas como ancho de banda, menor número de saltos, menor retardo, etc. Mientras que en los protocolo de enrutamiento exterior la selección obedece a criterios o acuerdo de tipo político, administrativo, económico que se llegan entre diferentes proveedores de servicio.

Basándose en la experiencia ganada en EGP (Exterior Gateway Protocol) se desarrolla un BGP para que permita solventar las necesidades anteriormente descritas. Actualmente BGP se encuentra en la versión 4 cuya definición se encuentra en el RFC1771.

BGP es protocolo de enrutamiento interdominios que no impone restricciones sobre la topología de la red adyacente, permite soporte de CIDR eliminado el concepto de clases usado en redes IP tradicionales lo que permite hacer agregación de rutas reduciendo el tamaño de las tablas de enrutamiento, asume que dentro del sistema autónomo se usa un IGP (como OSPF o IS-SI) para el enrutamiento.

Es importante tomar en cuenta que para aplicar el conjunto de políticas que ofrece BGP se debe guiar en la regla: que un portavoz BGP pública a un SA vecino únicamente las rutas que el router usa. Esta regla refleja el comportamiento de

Internet en el que una ruta se elige salto a salto, por esta razón algunas políticas que requieren una técnica enrutamiento en la fuente no pueden ser soportadas, sin embargo pueden soportar cualquier política basada en el paradigma del enrutamiento salto a salto; como Internet se basa en esta política BGP es altamente aplicable como protocolo de enrutamiento entre SA para Internet.

BGP usa TCP como protocolo de capa transporte lo cual permite asegurar que los datos se enviarán de forma confiable simplificando la complejidad de BGP ya que no necesita implementar un protocolo específico que asegure la entrega de los datos; se usa el puerto 179 para establecer las conexiones.

1.5.10.1 Como Trabaja BGP [8] [9] [10] [25]

BGP se define como un protocolo por vector de ruta que se utiliza para el transporte de información de enrutamiento entre diferentes sistemas autónomos, el término vector de ruta hace referencia a que BGP envía un conjunto de números de SA por los que un prefijo de red ha atravesado para alcanzar un SA remoto, el principal uso para este conjunto es la prevención de lazos de enrutamiento.

Los routers que ajuntan BGP se denominan portavoces BGP, en caso de que dos routers formen una sesión BGP mediante una conexión TCP para intercambiar información de enrutamiento se los denomina como iguales o vecinos, la conexión se realiza a través del puerto 179, al iniciar una sesión se intercambian mensajes *OPEN* que permiten determinar los parámetros de configuración de la conexión.

Uno de los mecanismos más interesante de BGP es que posee un mecanismo para cerrar las conexiones de una manera elegante, para esto al producirse un error de que puede ser un desacuerdo, incompatibilidad de los parámetros, algún cambio que realice el administrador u otros se envía un mensaje *NOTIFICATION* con el código de error correspondiente y se finaliza la conexión, esto asegura que no se desperdicien recursos en reintentar la conexión además de que permite que se envíen todos los mensajes pendientes antes de la finalización.

Al iniciar una sesión BGP, si la parte de negociación se establece con éxito entre un conjunto de portavoces BGP se da un primer intercambio de todas las rutas, después de este primer intercambio solo se envían las actualizaciones con cambios en la red, lo que permite reducir el uso del ancho de banda como del CPU, en comparación con otros protocolos que envían las actualizaciones de forma periódica.

Para enviar los diferentes cambios en la red se usan los mensajes *UPDATE* donde se envían los destinos que se pueden alcanzar a través de un portavoz BGP, en estas actualizaciones se envían también los diferentes atributos de la ruta de acceso (como el vector de ruta, grado de preferencia, etc.), adicionalmente en este mensaje se puede enviar información del retiro de una ruta incorrecta. En caso de cambios en una ruta no es necesario que se la retire, basta con publicar una sustitución de ruta.

Para el mantenimiento de una sesión BGP se envían de forma periódica mensajes *KEEPALIVE* en caso de que no se reciban estos durante un periodo de tiempo la sesión se termina, el costo de estos no es muy alto si se considera que se envía cada 60 segundos un mensaje de 19 bytes lo cual da una tasa de 2,5 bps para mantenimiento de la sesión.

BGP tiene un número de versión de la tabla, con cada cambio en la red; la tabla se incremente en un valor de uno, en caso de que el número de versión de la tabla se incremente rápidamente se concluye que la red esta inestable y se tomarán mediadas para corregir estos errores.

1.5.10.1.1 *Proceso de enrutamiento*

BGP es un protocolo relativamente simple y flexible, un router al recibir un mensaje de UPDATE con las diferentes rutas, ejecuta diferentes políticas de enrutamiento o filtros sobre las actualizaciones, para luego pasarlas a sus iguales. Se requiere una implementación adicional para guardar todas las actualizaciones BGP en una tabla de enrutamiento diferente, separada de la tabla de enrutamiento IP, en caso de que existan varias rutas a un mismo destino no se

envían todas las rutas, solo se envía la mejor ruta a un vecino. Las rutas locales válidas generadas por el sistema y las mejores rutas aprendidas de los vecinos BGP se instalan en la tabla de enrutamiento IP.

La manera de modelar el proceso BGP es pensando que cada portavoz BGP tiene diferentes conjuntos de rutas y diferentes motores de políticas aplicados a las rutas, este modelo se muestra en la figura 1.27 y lo conforman:

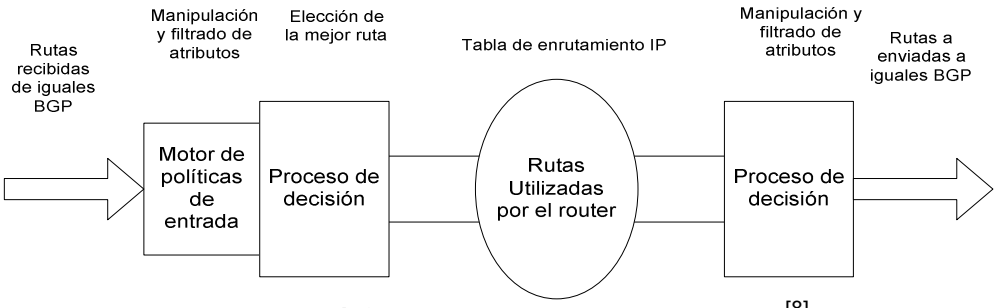


Figura 1.27: Proceso de Enrutamiento [8]

Un conjunto de rutas que ingresan al router de sus iguales.

- Un motor de políticas de entrada.
- Un proceso que permite decidir que rutas utilizará.
- Una cantidad de rutas utilizadas por el router.
- Un motor de políticas de entrada.
- Un conjunto de rutas que el router envía a sus iguales.

1.5.10.1.2 *Motor de políticas de entrada*

El motor de políticas de entrada se usa para el filtrado de rutas y la manipulación de los atributos, para realizar el filtrado se usan lo diferentes atributos disponibles como prefijos IP, AS_PATH, etc. BGP también manipula los atributos de la ruta con la finalidad de influir en el proceso de decisión y afectar a las rutas que se utilizan para llegar a un destino, las diferentes políticas que se utilizan son configuradas por un operador.

1.5.10.1.3 *Rutas utilizadas por el router*

Las mejoras rutas que sean identificadas en el proceso de decisión se colocan en el Loc-RIB, estas rutas pueden ser publicadas a vecinos o se pueden colocar en la tabla de enrutamiento IP, si una ruta no está en el Loc_RIB no puede colocarse en el Adj.RIB-Out para su publicación a otros iguales. Además de publicar las rutas que un router recibe de sus vecinos también se lo puede configurar para originar actualizaciones sobre las redes que tiene dentro de su sistema autónomo.

1.5.10.1.4 *Motor de políticas de salida*

Es igual al motor de políticas de entrada pero se lo aplica a las rutas de salida. Las que se han seleccionado como las mejores rutas, además de las que se generan localmente son entregadas a este motor para su procesamiento. El motor de salida aplica filtros y modifica algunos de los atributos de BGP antes de enviar la actualización, con el motor de políticas de salida también se distingue entre iguales internos y externos, por ejemplo las rutas aprendidas de un vecino interno no se pueden publicar a otro igual interno

1.5.10.1.5 *Publicación y almacenamiento de rutas*

Para propósitos de este protocolo una ruta está definida como una unidad de información que realiza una unión entre un destino y los atributos de ruta hacia ese destino.

Una ruta se publica entre un par de portavoces BGP en los mensajes de *UPDATE*, el destino de este es el sistema cuya dirección IP se indica en el campo *Network Layer Reachability Information* (NLRI) y la ruta es la información reportada en los campos de atributo de ruta del mismo mensaje.

Las rutas son almacenadas en las *Routing Information Bases* (RIBs), las cuales son nombradas como *Adj-RIBs-In*, la *Loc-RIB*, y la *Adj-RIBS-Out*. La información del siguiente salto para las diferentes rutas locales se encuentra almacenadas en la *forwarding information base* (FIB).

Al momento que se decide publicar una ruta, se puede modificar o añadir atributos de camino de la ruta antes de publicársela a su igual.

1.5.10.1.6 *Bases de información de enrutamiento de BGP*

Las bases de información de enrutamiento (RIB) por sus siglas en ingles (*Routing Information Base*) dentro de un portavoz BGP constan de los siguientes partes:

Adj-RIB-In: Almacena información de enrutamiento que ha sido aprendida de los mensajes de enrutamiento entrantes, las rutas que este contiene se pueden utilizar como entradas válidas en el proceso de decisión.

Loc_RIB: contiene la información de enrutamiento local que son el mejor camino hacia cada destino disponible, son rutas que el portavoz BGP ha seleccionado al aplicar las diferentes políticas a la información que se almacena en la *Adj-RIB-In*.

Adj-RIB-Out: Almacena la información que el router BGP local ha seleccionado para enviar a sus vecinos en mensajes *UPDATE*.

Aunque en este modelo se presentan tres diferentes tipos de bases de información de enrutamiento en una implementación práctica del protocolo se almacena una copia de la información con punteros para ahorrar memoria.

1.5.10.1.7 *Proceso de decisión de BGP*

Cuando BGP tiene muchas rutas de la misma longitud de prefijo hacia un mismo destino, BGP elige la mejor ruta hacia un destino basándose en el valor de los atributos. A continuación se muestra como BGP elige la mejor ruta:

Si el próximo salto es inaccesible la ruta se ignora.

Si es accesible prefiere la ruta con el mayor valor de preferencia local.

Si no hay rutas originadas localmente y la preferencia local es la misma se prefiere la ruta con el AS_PATH más corto.

En caso de que la longitud del AS_PATH sea la misma, prefiere la ruta con el origen más bajo donde IGP es más bajo que EGP y EGP es más bajo que *INCOMPLETE*).

Si el tipo de origen es el mismo, prefiere la ruta con el MED mas bajo, siempre que las rutas sean originadas en el mismo SA.

En caso de que los valores de MED sean los mismos prefiere las rutas EBGP a las rutas IBGP.

Si todos los escenarios anteriores son iguales, prefiere la ruta que puede ser alcanzada mediante el vecino IGP más próximo.

Finalmente si la ruta interna es la misma, la decisión se toma en base a ROUTER_ID prefiriéndose la ruta con el RID más bajo.

1.5.10.2 EBGP e IBGP [8] [9] [11] [38]

Aunque el uso más extendido de BGP es el proporcionar una topología entre dominios libre de bucles, BGP también se usa dentro de un sistema autónomo para proporcionar a los routers internos la información de accesibilidad de destinos externos. Si la conexión entre dos BGP iguales se establece dentro de un SA se denomina BGP interno (IBGP), en cambio si esta sesión se establece entre dos iguales de diferentes SA se conoce como BGP externo (EBGP), esto se muestra en la figura 1.28.

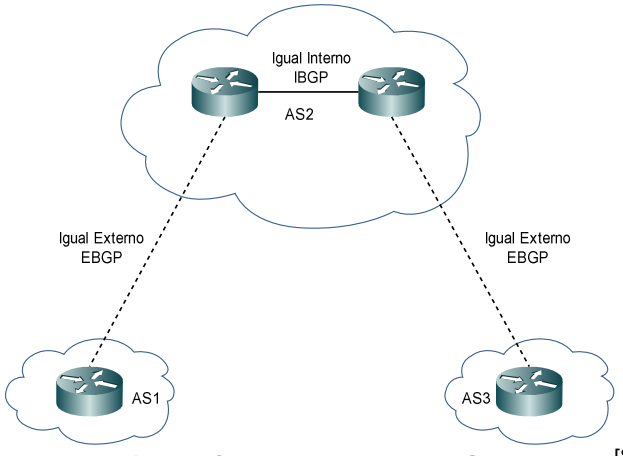


Figura 1.28: Conexiones de IBGP e EBP [8]

En el proceso de negociación de una sesión BGP los routers comparan los números de SA y determinan si son iguales internos o externos. La diferencia entre EBGP e IBGP se manifiesta en cómo cada igual procesa las actualizaciones de enrutamiento que llegan de otros iguales, también en la forma en que distintos atributos BGP son transportados sobre conexiones internas en comparación con las externas.

Una de las restricciones que se deben de tomar en cuenta es que los vecinos BGP externos deben estar físicamente conectados, en caso de que no estén físicamente conectados BGP por defecto ignora cualquier mensaje de *UPDATE* de su igual externo. Para evitar bucles de enrutamiento dentro de un SA BGP no vuelve a publicar a los iguales internos las rutas que aprende de otros iguales IBGP, por esta razón es importante mantener un malla dentro del SA.

1.5.10.3 Formato de la Cabecera BGP

La cabecera BGP está compuesta de 19 bytes repartidos en 16 bytes del campo marcador seguido de 2 bytes para el tamaño y un byte para el campo tipo, cabe recalcar que dependiendo del tipo de mensaje a esta cabecera le seguirán o no una porción de datos, el formato de la cabecera BGP se muestra en la figura 1.29.

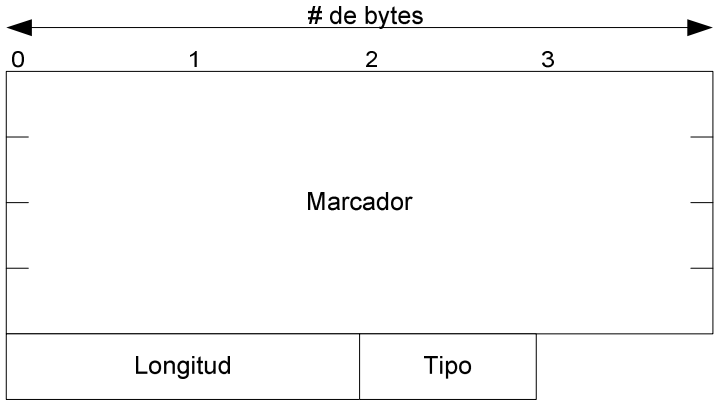


Figura 1.29: Formato del mensaje de la cabecera [25]

Marcador: Este campo de 16 octetos es un valor que el receptor del mismo puede predecir, se lo usa para detectar perdida de sincronización entre dos pares BGP y para autenticar mensajes entrantes BGP, en caso de ser un mensaje OPEN o si el mensaje OPEN no lleva información de autenticación debido a que es opcional,

todos los bits de este se establecen en 1, en el otro caso se puede calcular el valor del campo en base al mecanismo de autenticación que se utilice como por ejemplo la opción de MD5 para firma de TCP.

Longitud: Este campo de 2 bytes indica la longitud total del mensaje BGP en octetos incluyendo la cabecera, esto permite localizar en el flujo de datos de la capa transporte el siguiente mensaje, el valor de este campo puede ser de mínimo 19 bytes y no más de 4096 bytes.

Tipo: Este campo de un bit indica el código del tipo de mensaje los mismos que pueden ser:

- *OPEN*
- *NOTIFICATION*
- *KEEPALIVE*
- *UPDATE*

1.5.10.3.1 *Formato del mensaje open*

Después de que se establece una conexión de capa transporte se envía un mensaje *OPEN* de cada nodo, si este mensaje es admitido se intercambia un mensaje de *KEEPALIVE* para confirmar la aceptación del mismo, una vez que se ha intercambiado este mensaje se pueden intercambiar mensajes *UPDATE*, *NOTIFICACTION* indistintamente, el tamaño mínimo del mensaje es de 29 bytes.

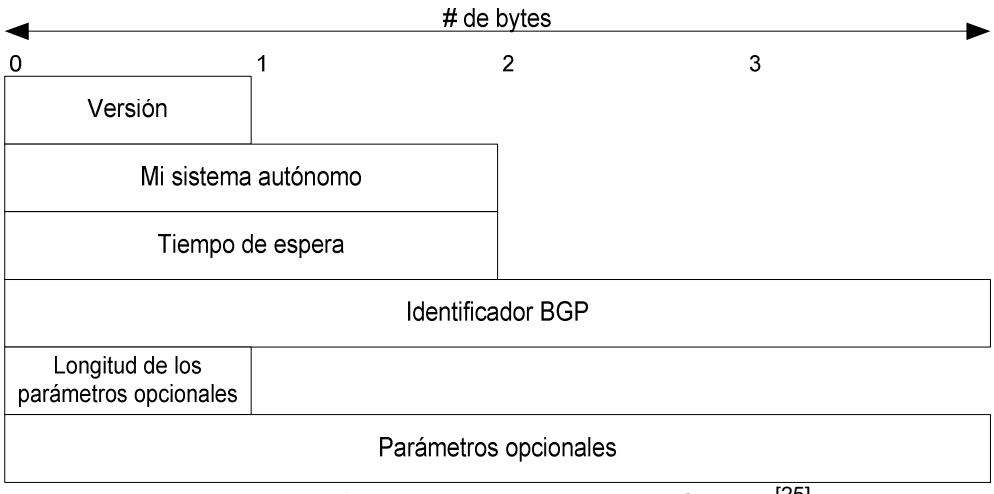


Figura 1.30: Formato Mensaje OPEN [25]

El formato del mensaje *OPEN* mostrado en la figura 1.30 consta de los siguientes campos:

Versión: Este campo de 1 byte indica la versión del protocolo usado en el mensaje, para establecer la versión adecuada los routers vecinos reinician las sesiones hasta encontrar la versión común más alta soportada por los 2, generalmente se usa la versión 4 de BGP.

Sistema autónomo: Este campo de 2 bytes indica el número del sistema autónomo del que envía el mansaje.

Tiempo de espera: Este campo de 2 bytes indica el número de segundos que el emisor del mensaje propone como valor para tiempo de espera entre la recepción de dos mensajes exitosos *UPDATE* o *KEEPALIVE*. Este valor es un contador que inicia en cero hasta el valor de este campo, con la recepción de un mensaje este se reinicia a 0, en caso de sobrepasar este valor se puede considerar que el vecino está inactivo.

Para escoger el tiempo de espera los routers BGP negocian con su vecino y se escogen el tiempo más bajo entre el suyo y el de su vecino, puede que el valor del tiempo de espera sea 0 en cuyo caso significa que los temporizadores no se reinician y se considera que la conexión siempre está activa en caso de no ser el valor mínimo permitido es 3 segundos.

Identificador BGP: Es un campo de 4 bytes que indica el identificador BGP del que envía el mensaje, este valor es una dirección IP que se asigna como identificación del router, el cual es calculado al inicio de la sesión BGP y corresponde a la dirección IP más alta asignada a una de las interfaces físicas o virtuales.

Longitud de los parámetros opcionales: Es de 1 byte e indica la longitud total del campo parámetros opcionales en octetos. Si tiene un valor de cero significa que no tiene parámetros opcionales en el mensaje.

Parámetros opcionales: Este es un campo opcional que contiene una lista de parámetros opcionales que se utilizan en la negociación para establecer una sesión BGP. Utiliza una codificación (Tipo de parámetro, longitud del parámetro, valor del parámetro) conocida como TLV, el tipo de parámetro es un campo de un octeto que identifica de manera única los parámetros individuales, el campo longitud de parámetro de un byte indica el largo del campo valor de parámetro en octetos. El último campo es de tamaño variable y se interpreta de acuerdo al valor que se tenga en el campo tipo, por ejemplo se define el valor de 1 para información de autenticación. En la figura 1.31 se muestra el formato de los parámetros opcionales.

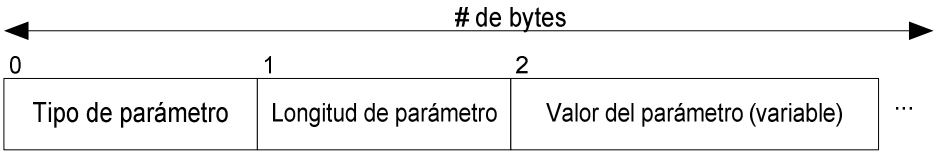


Figura 1.31: Formato de los Parámetros Opcionales [25]

1.5.10.3.2 *Mensajes Keepalive*

Estos mensajes se intercambian periódicamente entre iguales BGP para asegurar que son accesibles, se usa para evitar que el tiempo de espera no expire para que la sección continúe activa, se recomienda usar una velocidad de envío de un tercio del valor del temporizador de espera, este tiempo puede ser ajustado por el administrador de acuerdo a sus necesidades tomando en cuenta que no se puede enviar con una frecuencia superior a 1 segundo.

1.5.10.3.3 *Notificación*

Los mensajes de notificación se envían siempre que se detecta una condición de error, luego de enviar el mensaje la conexión se cierra, el mensaje adicional a la cabecera BGP mostrado en la figura 1.32 contiene los siguientes campos:

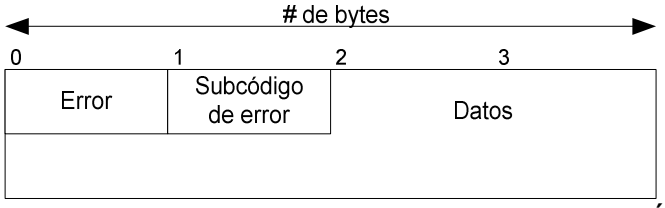


Figura 1.32: Formato del mensaje NOTIFICACIÓN [25]

El mensaje de NOTIFICACIÓN está compuesto del código de error de 1 byte que indica el tipo de notificación, el subcódigo de error que proporciona información más específica sobre la naturaleza del error y un campo de datos que contiene datos usados para el diagnóstico el error como una mala cabecera, SA erróneo, etc. Los diferentes códigos de error se muestran en la tabla 1.4.

Código de error	Subcódigo de error
Error en cabecera de mensaje.	Conexión no sincronizada.
	Longitud del mensaje incorrecto.
	Tipo de mensaje incorrecto.
Error en el mensaje OPEN	Número de versión no soportado.
	SA Igual erróneo
	Identificador BGP incorrecto.
	Parámetro opcional no soportado.
	Fallo de autenticación
	Temporizador de espera inaceptable.
	Capacidad no soportada.
Error en el mensaje UPDATE	Lista de atributos mal formada.
	Atributo conocido no reconocido.
	Atributo conocido perdido.
	Error en los flags del atributo.
	Error en la longitud del atributo.
	Atributo de origen erróneo.
	Bucle de enrutamiento en el SA.
	Atributo NEXT_HOP erróneo.
	Error en atributo opcional.
	Campo de red erróneo.
	SA_PATH mal formado.
Temporizador de espera expirado	N/A
Error de la máquina de estado finito	N/A
Cesar (para errores fatales adicionales a los mencionados)	N/A

Tabla 1.4- Posibles errores y sus sub códigos [8]

1.5.10.3.4 *Formato del mensaje update*

Este tipo de mensajes se usa para transferir información de enrutamiento entre pares BGP, se pueden enviar actualizaciones, eliminación de rutas o ambos, en base a estos mensajes se construye una topología de rutas libres de lazos que describen la relación que existe entre varios sistemas autónomos. Los campos adicionales a la cabecera BGP se muestran en la figura 1.33.

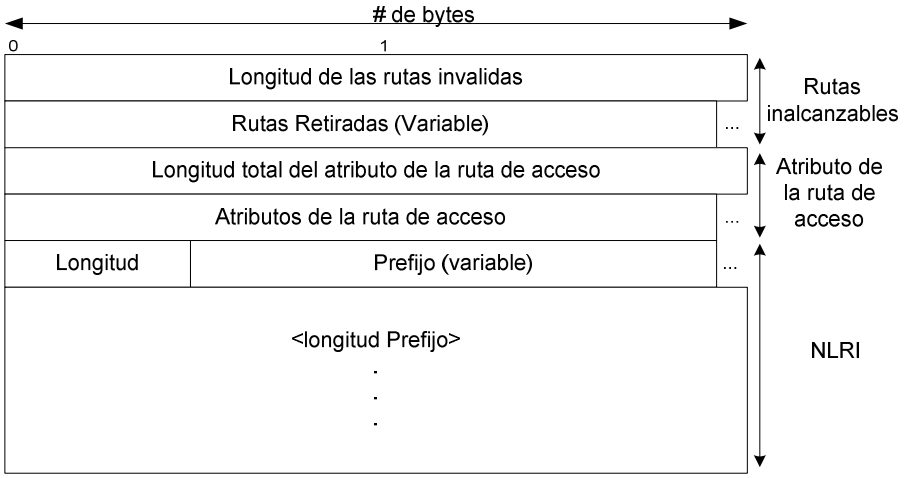


Figura 1.33: Formato del mensaje UPDATE [8]

Rutas Inalcanzables:

Longitud de las rutas inválidas: Este campo de 2 octetos indica la longitud total en octetos del campo rutas retiradas, en un mensaje se puede especificar si se eliminan varias rutas al mismo tiempo o no se debe retirar ninguna, en caso de que este campo tenga el valor de cero indica que no existen rutas a ser eliminadas por lo que se elimina el campo rutas retiradas

Rutas retiradas: Este campo contiene una lista de actualizaciones de rutas (prefijos de direcciones IP) que no están disponibles o que no se encuentran más en servicio por lo que deben ser eliminadas de las tablas de enrutamiento, cada uno de estos prefijos se representa con una de la forma <longitud, prefijo>, cuyos campos se muestran en la figura 1.34.

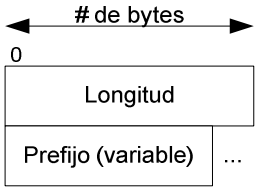


Figura 1.34: Campo Rutas Retiradas [25]

Longitud: Este campo indica la longitud en bits del prefijo de la dirección IP, una longitud de cero indica que abarca todas las direcciones IP.

Prefijo: Este campo contiene el prefijo de dirección IP seguido de un conjunto de bits que permita completar el tamaño en octetos.

Atributo de la Ruta de Acceso:

Longitud total del atributo de la ruta de acceso: Este campo de 2 bytes indica la longitud total del campo atributos de camino en octetos.

Atributos de la ruta de acceso: Estos atributos son un conjunto de parámetros que se utilizan para llevar información específica de la ruta como información de la ruta de acceso, grado de preferencia el NEXT_HOP y la información de agregación, estos parámetros se utilizan para la selección de la ruta.

Cada atributo es una secuencia de bits de tamaño variable, cada uno de estos atributos es una tripleta de la forma (tipo de atributo, tamaño del atributo, valor del atributo) que también es de tamaño variable, el tipo de atributo es un campo de 2 bytes que consta de un flags de atributo de 1 byte y un código de tipo de atributo de 1 byte como se muestra en la figura 1.35:

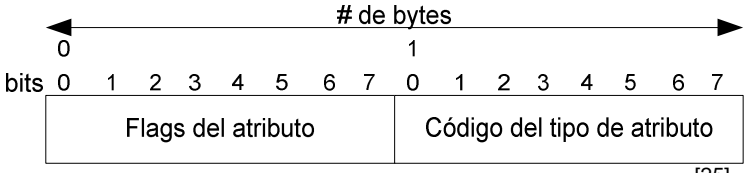


Figura 1.35: Atributos de la ruta de acceso [25]

El bit más significativo del campo flags del atributo (bit 0) es el bit opcional, define si el atributo es opcional (con un valor de 1) o si es conocido (con el valor de 0). El segundo bit más significativo del campo flags de atributo (bit 1) es el bit

transitivo, define si el atributo opcional es transitivo (con el valor de 1) o si es intransitivo (con el valor de 0). En el caso de los atributos conocidos son siempre transitivos por que el valor de este atributo será 1.

El tercer bit más significativo del campo flags de atributo (bit 2) es el bit parcial, define si la información contenida en el atributo transitivo opcional es parcial (con el valor de 0) o completa (con el valor de 1), para los atributos conocidos y para los atributos intransitivos el bit parcial debe ser 0. El cuarto bit más significativo del campo flags de atributo (bit 3) es el bit de extensión de tamaño, define si el tamaño del atributo de es 1 byte (si el valor es 0) o de 2 bytes (si el valor es 1) en caso de que supere el valor de 255.

Los cuatro bits menos significativos del campo flags no se usan por lo que se coloca el valor de 0 y en la recepción deben ser ignorados. Estos bits definen cuatro categorías para los atributos de la ruta de acceso que se detallan a continuación:

Obligatorio conocido: Estos atributos se encuentran presentes en los mensajes *UPDATE BPG*, son soportados por todas las implementaciones del protocolo, en caso de pérdida de uno de estos atributos se genera un mensaje de NOTIFICACIÓN y se termina la sesión, esto se debe a que todas la implementaciones de BGP contienen un conjunto de atributos estándar. Estos campos deben ser pasados a los otros vecinos BGP.

Discrecional conocido: Si bien estos atributos son reconocidos por todas las implementaciones de BGP, al ser discrecionales pueden o no enviarse en los mensajes *UPDATE BGP*.

Transitivo opcional: una ruta de acceso puede contener uno o más de estos atributos y no es necesarios que sea soportado por todas las implementaciones de BGP, si uno de estos atributos no es reconocido se busca el flag transitivo, si este está activo (valor de 1) deberá aceptarse el atributo y pasarlos a los otros portavoces BGP.

Intransitivo opcional: al igual que el transitivo pueden no ser soportados por todas las implementaciones BGP, si uno de estos atributos no es reconocido y el flag transitivo no se encuentra activo (valor de 0) el atributo debería ser ignorado y no pasarlo a otros portavoces BGP.

Los siguientes octetos de los atributos de la ruta de acceso representan el valor del atributo y se deben interpretar en base a las flags del atributo y al código del tipo del atributo. Los valores y usos de los atributos son los siguientes:

***ORIGIN* (código de tipo 1):** es un atributo obligatorio conocido, que define el origen de la información de la ruta, el octeto de datos puede asumir los siguientes valores:

- *IGP:* la información de accesibilidad de capa red es originada en el interior del SA.
- *EGP:* la información de accesibilidad de capa red es aprendida vía un EGP.
- *INCOMPLETE:* información de accesibilidad de capa red es aprendida por otros medios.

Este atributo se utiliza para la toma de decisiones con este se establece una clasificación de preferencia entre múltiples rutas escogiéndose la que tenga un tipo de origen más bajo, el orden de preferencia es IGP sobre EGP y EGP sobre *INCOMPLETE*.

***SA_PATH* (código de tipo 2):** Es un atributo conocido obligatorio que está compuesto por una secuencia de números de sistemas autónomos que representa el camino por el que atraviesa una ruta, cada uno de estos segmentos se representa por una tripleta <tipo del segmento de ruta, longitud del segmento de ruta, valor del segmento de ruta> que se detalla a continuación:

El tipo de segmento de ruta es un campo de un octeto que define los siguientes valores:

- *SA_SET* es una lista desordenada de sistemas autónomos que una ruta en el mensaje de *UPDATE* ha atravesado.

- *SA_SEQUENCE* es una lista ordenada de sistemas autónomos que una ruta en el mensaje de *UPDATE* ha atravesado.

El tamaño del segmento de ruta es un campo de un byte que contiene el número de SAs que se encuentran en el campo valor del segmento de ruta. El valor del segmento de ruta contiene uno o más números de SA codificados en campos de 2 bytes.

Cuando un router BGP advierte una ruta a otro portavoz BGP dentro de un mismo sistema autónomo el atributo *SA_PATH* no se modifica, si este atributo este vacío es decir tiene un valor de 0 en el campo longitud del segmento de ruta, representa que la ruta ha sido generada dentro del sistema autónomo y que estas únicamente se han enviado dentro del mismo.

El otro caso se tiene cuando se advierte una ruta a iguales BGP externos, el SA que origina la ruta añade su número de SA, un router que recibe una ruta antes de pasarla a otro SA añade el número de su propio SA y lo envía a otros EBGP, la lista que se forma representa todos los números de SA por los que la ruta ha pasado y están en un lista *SA_SEQUENCE* pues los números están ordenados de manera secuencial y el número del SA que generó la ruta queda al final de la lista antes del código ORIGIN.

***NEXT_HOP* (código de tipo 3):** Es un atributo conocido obligatorio con un valor que define la dirección IP del router fronterizo que debe ser usado como el siguiente salto para los destinos listados en el campo de accesibilidad de la capa red del mensaje *UPDATE*, si se utiliza en el contexto de un IGP varía pues el próximo salto para llegar a un destino es la dirección IP de la interfaz del router que está directamente conectado y que anuncio la ruta, la definición de BGP es un poco elaborada y puede ser de las siguiente forma:

- En caso de ser una sesión EBGP el próximo salto es la dirección IP del vecino que anunció la ruta.
- En las sesiones IBGP, en las rutas que se originan dentro del SA el próximo salto corresponde a la dirección IP del router que anunció la ruta.

- Si el SA aprende una ruta por un EBGP, el próximo salto es la dirección del vecino EBGP del que la ruta fue aprendida, dentro del SA esta dirección no se altera cuando se propaga a otro router IBGP.
- Si la ruta se publica en un medio multiacceso como Ethernet, Frame Relay, etc. El próximo salto corresponde a con la dirección IP de la interfaz del router que originó la ruta en este medio.

MULTI_EXIT_DISC **(código de tipo 4):** Es un atributo opcional intransitivo de cuatro bytes, que puede ser usado en el proceso de decisión de un portavoz BGP para discriminar múltiples salidas hacia un sistema autónomo es una métrica externa de una ruta, desde otra perspectiva es un indicio que se da a los vecinos externos de una ruta preferida para que se acceda a un SA que tiene múltiples puntos de entrada, el valor más bajo es el preferido.

Estos atributos se intercambian entre los SA, pero un atributo que es recibido por un SA tiene significado local para tomar decisiones dentro del SA por lo que la métrica no puede ser reenviada cuando esta actualización se pasa a otro SA se coloca el valor de cero por defecto a menos que se desee especificar un valor que no es correspondiente con el recibido de otro SA.

LOCAL_PREF **(código de tipo 5):** Es un atributo conocido discrecional de cuatro bytes que se incluye en todos los mensajes de *UPDATE* que se envían de un portavoz BGP a otro dentro del sistema autónomo, un router BGP calcula el grado de preferencia para cada ruta externa e incluye este grado de preferencia cuando pública esta ruta a otros routers IBGP, se prefiere la ruta con un valor más alto de LOCAL_PREF para seleccionar entra varias rutas hacia un mismo destino.

La preferencia local se usa para establecer un punto de salida de un SA para llegar a un cierto destino pues las actualizaciones pueden provenir de varios SAs. Un portavoz BGP no incluye este atributo en los mensajes de *UPDATE* que se envían a un EBGP de otro sistema autónomo, en caso de que se envié este atributo a otro SA este debe ser ignorado por el receptor del mensaje.

ATOMIC_AGGREGATE **(código del tipo 6):** Es un atributo discrecional conocido de longitud 0, se utiliza para especificar la pérdida de información que se da al

momento de hacer agregación de rutas, esto debido a que la información llega de diferentes orígenes por lo que tiene varios atributos diferentes que se pierden al momento de hacer la agregación, en caso de que un sistema propague una agregado de rutas debe adjuntar este parámetro, este parámetro no debe ser colocado cuando el agregado transporta alguna información adicional que indique de donde provenía este.

***AGGREGATOR* (código del tipo 7):** Es un atributo opcional transitivo de longitud 6 que se puede incluir en los mensajes de *UPDATE* cuando se realiza una agregación de ruta, este contiene el número del SA en dos octetos seguido de la dirección IP que identifica al router que realizó la agregación.

***COMMUNITY* (código del tipo 8):** Es un atributo opcional intransitivo de longitud variable y consta de un conjunto de valores de 4 bytes, una comunidad es un grupo de destinos que comparten algún tipo de propiedades en común no se limita a un sistema autónomo o grupo de redes por lo que no tiene límites físicos, este tipo de agrupaciones se utilizan para simplificar el uso de políticas de enrutamiento basándose en una propiedad lógica en lugar de un prefijo IP, se usa como un control para rutas que se aceptan, envían y prefieren de los vecinos BGP. Las comunidades de los rangos de 0x00000000 a 0x0000FFFF y de 0xFFFF0000 a 0xFFFFFFFF están reservadas y tienen un significado global como:

- NO_EXPORT (0xFFFFFF01). Si se agrega este valor en el atributo significa que no se debe publicar una ruta fuera del SA.
- NO_ADVERTISE (0xFFFFFF02). Si se envía recibe este valor la ruta recibida no se deberá transportar a ningún igual BGP.

Adicional a los valores de comunidad reservados lo valores de comunidad privada se pueden definir para usos especiales como los del RFC1998 que definen como las comunidades pueden ser utilizadas para manipular la selección de rutas en redes de proveedores de servicio.

Network Layer Reachability Information (NLRI)

Es un campo de longitud variable que contiene una lista de prefijos de direcciones IP, la longitud en bytes de este campo no se codifica de manera explícita pero se puede calcular de la siguiente manera:

Longitud del mensaje *UPDATE* - 23 - Longitud de las rutas inválidas – Longitud total del atributo de la ruta de acceso. La información de accesibilidad se codifica en una o más duplas de la forma <longitud, prefijo>, como se observa en la figura 1.36.

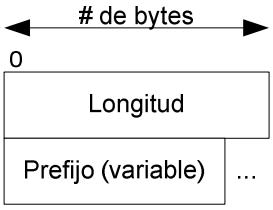


Figura 1.36: Campo NLRI [25]

El significado de los campos es:

Tamaño: Este campo indica el tamaño en bits del prefijo de dirección IP si su valor es 0 indica que coincide con todas la direcciones IP.

Prefijo: Este campo contiene el prefijo de la dirección IP seguido de un número suficiente de bits de manera que se complete un número entero de octetos.

Se usa para publicar a los sumo una ruta, la misma que puede ser descrita por varios atributos que se utilizan para detectar bucles y le da la flexibilidad para reforzar la políticas de enrutamiento local y global. Al usar el NLRI BGP versión 4 permite el uso de enrutamiento entre dominios sin clase (CIDR).

1.5.10.4 Máquina de estado finito de BGP [8] [9] [10]

Antes de establecer una sesión BGP la negociación transcurre por diferentes etapas en la máquina de estado finito, las mismas que se muestran en la figura 1.37.

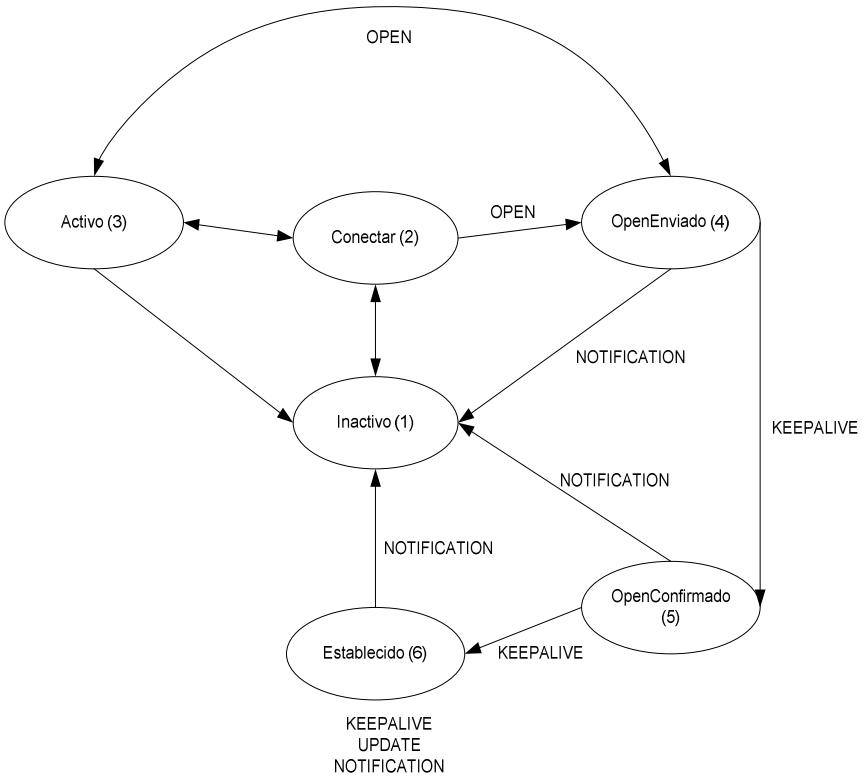


Figura 1.37: Máquina de estados finitos de BGP [8]

Inactivo: Es la primera etapa de la conexión, donde BGP espera una evento que se inicia por el administrador de la red, un evento se inicio se da cuando un administrador configura BGP en un router o reinicia una sesión, una vez que se produzca este evento se inicializan todos los recursos BGP, inicia el temporizador ReintentoConexión, inicia una conexión de transporte a otros iguales BGP, mientras escucha por conexiones que pueden ser inicializadas por iguales BGP remotos, finalmente pasa a un estado de conectado, en caso de que se produzca cualquier error regresa al estado inactivo, para salir de este estado necesita iniciar un evento.

Conectar: Es este estado BGP espera que la conexión de transporte se complete, si esta se establece con éxito se borra el temporizador ReintentoConexion, se completa la inicialización, se envía un mensaje OPEN y cambia al estado OpenEnviado. Si la conexión de transporte falla, se reinicia el temporizador ReintentoConexión, se continúa escuchando a conexiones que pueden ser inicializadas por un igual BGO remoto y se pasa al estado activo. Si expira el tiempo del temporizador ReintentoConexión, se reinicia el temporizador,

se inicia una conexión con otro igual BGP, se continúa escuchado a posibles conexiones y se mantiene el estado conectado. En caso de cualquier otro evento (iniciado por el sistema o un operador), se cambia el estado a inactivo.

Activo: En este estado BGP trata de adquirir un igual al iniciar una conexión de protocolo de transporte, si esta es exitosa el router BGP se borra el temporizador ReintentoConexion, completa la inicialización, fija el valor del temporizador de espera a una valor alto se recomienda de 4 minutos, envía un mensaje de OPEN al igual y pasa el esta OpenEnviado.

En caso de que el temporizador ReintentoConexion expire BGP reinicia este temporizador e inicia una conexión de transporte con otro igual BGP, continua escuchando por conexiones que pueden ser iniciadas por iguales BGP remotos y cambia al estado conectado. En caso de que el sistema local detecta que un igual está intentando establecer una conexión y la dirección IP de este no es la que se esperaba, el sistema reinicia el temporizador ReintentoConexion y rechaza el intento de conexión, mantiene el estado activo en la espera de conexiones de otro iguales BGP.

Cabe recalcar que la oscilación entre el estado conectar y activo da la pauta de que algo no está bien en la conexión de transporte TCP. En caso de cualquier otro evento (iniciado por el sistema o un operador), se cambia el estado a inactivo.

OpenEnviado: Al estar en este estado BGP está esperando un mensaje *OPEN* de su igual. Cuando este se recibe se comprueba que todos los campos estén correctos, si se detecta un error en cualquiera de estos se envía un mensaje de *NOTIFICATION* y vuelve al estado inactivo, si no existen errores inicia el envío de mensajes *KEEPALIVE* y se inicia el temporizador *KEEPALIVE*, en este punto se realiza la negociación del tiempo de espera tomado el valor más pequeño del los que se proponen por los dos iguales BGP, en caso de que el tiempo negociado sea de 0, los dos temporizadores no se reinician, al comparar los valores del SA si es el mismo que el del local se trata de un enlace interno (IBGP) si es diferente es externo (EBGP).

Si la capa de transporte genera una notificación de desconexión, el sistema local cierra la conexión BGP, reinicia el temporizador ReintentoConexion, se mantiene en escucha de conexiones de iguales BGP y pasa al estado activo. En caso de que se produzca cualquier otro error se envía un mensaje de NOTIFICATION con el código de error correspondiente y se pasa el estado inactivo liberando los diferentes recursos utilizados.

OpenConfirmado: En este estado BGP se encuentra esperando un mensaje de *KEEPALIVE* o uno de *NOTIFICATION*, si se recibe el primero el sistema pasa a un estado de establecido y la negociación con el vecino se completa, en cambio si recibe un mensaje de *NOTIFICATION* cambia al estado de inactivo.

En caso de que el temporizador de *KEEPALIVE* expire se envía un mensaje *KEEPALIVE* y se reinicia este temporizador, en caso de se produzca una notificación de desconexión de transporte se pasa a estado inactivo, al expirar el tiempo de espera o en respuesta a un evento de parada se envía un mensaje de NOTIFICATION con el código de error correspondiente y se pasa el estado inactivo liberando los diferentes recursos utilizados.

Establecido: Al pasar a este estado BGP puede intercambiar mensaje UPDATE, NOTIFICATION y KEEPALIVE con sus iguales, en caso de recibir un mensaje UPDATE o un NOTIFICATION se reinicia el temporizador de tiempo de espera siempre que este no tenga el valor de 0, en cambio si recibe un mensaje de NOTIFICATION cambia al estado inactivo. Si se envía un mensaje KEEPALIVE o UPDATE se reinicia el temporizador del KEEPALIVE.

Al recibir una notificación de desconexión de la capa transporte se cambia al estado inactivo, en caso de que se detecte un error en la manipulación de mensaje UPDATE, el tiempo de espera expire, o en respuesta a un evento de parada se envía un mensaje de NOTIFICATION con el mensaje de error correspondiente.

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO 1

LIBROS

[1] **BRUCE**, **DAVIE**, **FARREL**. "*MPLS: Next Steps*". Morgan Kaufmann. USA. 2008.

[2] **ALWAYN**, Vivek. "*Advanced MPLS design and Implementation*". Cisco Press. 2002.

[3] **MCDYSAN**, David; **DAVE**, Paw. "*ATM & MPLS Theory and Application: Foundations of Multi-Service Networking*". McGraw-Hill. Osborne. 2002.

[4] **GUICHARD**, Jim; **PEPELNJAK**, Ivan. "MPLS and VPN architectures". Cisco Press. 2000.

[5] **XIPENG**, Xiao; **NI**, Lionel M. "*Internet QoS: A Big Picture*". Michigan State University.

[6] **TANENBAUM**, Andrew. "*Redes de Computadoras*". 3ed. Capitulo 6, págs. 521-525.

[7] **ABE**, Martey. "*IS IS Network Design Solutions*". Cisco Press. Networking Technology. Febrero 2002

[8] **HALABI**, Sam; **MCPHERSON**, Danny. "*Internet Routing Architectures*". 2 ed. Cisco Press. Agosto 2000.

[9] **DOYLE**, Feff; **DEHAVEN**, Jennifer. "*Routing TCP/IP*". Volumen 2. Cisco Press. Abril 2001.

[10] **KHALID**, Raza; **MARK** Turner. "*Large-Scale IP Network Solutions*". Cisco Press. 2002.

[11] **RETANA**, Alvaro; **SLICE**, Don; RUSS, WHITE; "*Advanced IP Network design*". Cisco Press. Junio 1999.

[12] **SHAMIN**, Faraz; **AZIZ**, Zaheer; "*Troubleshooting IP routing protocols*". Cisco Press. Mayo 2002.

TESIS

[13] **NIETO**, Luisiana. "*Diseño y configuración de calidad de servicio en la tecnología MPLS para un proveedor de servicios de internet*". EPN. Mayo 2010.

[14] **CHAVEZ**, Diego; **MONTERO**, Silvana. "*Diseño para la migración de la red de SETEL hacia un carrier que utiliza tecnología MPLS, para proveer*

servicios de VoIP en todo el distrito metropolitano de Quito" EPN. Marzo 2008.

[15] **SANCHEZ**, Carlos. "*Análisis y propuesta de mejoramiento de la infraestructura de telecomunicaciones de la CNT Cañar*". UPS. Abril 2010.

PDF, RFC, PAPERS

[16] **ORAN**, David. "*RFC 1142: OSI IS-IS Intra-domain Routing Protocol*". Febrero 1990.

[17] **CANALIS**, María. "*MPLS Multiprotocol Label Switching: Una Arquitectura de Backbone para la internet del siglo XXI*".

[18] **ROSEN**, **VISWANATHAN**, **CALLON**. "*RFC: 3031: Multiprotocol Label Switching Architecture*". Enero 2001.

[19] **ANDERSSON**, **DOOLAN**, **FELDMAN.** "*RFC 3036: LDP (Label Distribution Protocol) Specification*". Enero 2001.

[20] **DOMÍNGUEZ**, Manuel. "*Servicio GoS sobre MPLS mediante técnicas activas*"
URL: http://www.manolodominguez.com/projects/opensimmpls/content/ common/pdf/documentation/gossobrempls.pdf

[21] **MORALES**, Luis. "*Investigación de Redes VPN con Tecnología MPLS*"
URL: http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/ capitulo2.pdf.

[22] **ANÓNIMO.** RFC 791. "IP (Internet protocol)". Septiembre 1981.

[23] **PINGARRÓN**, Raul. "*Arquitectura TCP/IP*".
URL: http://cfievalladolid2.net/tecno/recursos/c_redes_ciclos/archivos/ tcp-ip.pdf

[24] **ANÓNIMO**. "*Protocolo TCP/IP*".
URL: http://www.mcgraw-hill.es/bcv/guide/capitulo/8448199766.pdf

[25] **REKHTER**, **LI**, **HARES**. "*RFC: 4271: A Border Gateway Protocol 4*". Enero 2006.

[26] **PANTELIS**, Pablo; **MONTE DE OCA**, Victor; **GALLEGUILLO** Juan. "*BGP (Border Gateway Protocol) análisis y simulación*"
URL: http://ingenieria.unlam.edu.ar/ uea2010/trabajos/ uea2010_submission_15.pdf

INTERNET

[27] **SIENRA**, Luis G. "*Ofreciendo Calidad de servicio mediante MPLS: Fundamentos y aplicaciones a las redes de cable*".
URL: http://www.cinit.org.mx/articulo.php?idArticulo=14

[28] **ANÓNIMO**. "*The Role of BGP in MPLS networks*".
URL: http://www.networkers-online.com/blog/2010/04/ the-role-of-bgp-in-mpls-networks/.

[29] **ANÓNIMO**. "*Modelo TCP/IP*".
URL: http://www.alfinal.com/Temas/tcpip.php

[30] **ANÓNIMO**. "*Protocolo de control de transmisión (TCP)*".
URL: http://www.gestiopolis.com/recursos6/Docs/Ger/ sitemas-de-informacion-tcp.htm

[31] **ANÓNIMO**. "*Interior vs. Exterior Routing Protocols*".
URL: http://www.inetdaemon.com/tutorials/internet/ip/routing/ interior_vs_exterior.shtml

[32] **ANÓNIMO**. "*IS-IS for Spanish People*".
URL: http://anetworkerblog.com/2007/12/03/is-is-for-spanish-people/

[33] **ANÓNIMO**. "*Protocolos de enrutamiento de red IGRP, EIGRP, OSPF, ISIS, BGP*".
URL: http://www.compute-rs.com/es/consejos-2891289.htm

[34] **ANÓNIMO**. "*IS-IS*".
URL: http://www.worldlingo.com/ma/enwiki/es/IS-IS#History

[35] **WEHER**, Ariel. "*IS-IS Integrado: Conceptos básicos y configuración*".
URL: http://www.capaocho.net/2009/02/is-is-integrado-conceptos- basicos-y_10.html

[36] **ANONIMO**. "*Proyecto IS-IS version2*".
URL: www.redeschile.net/files/ccnp1/isis/proyecto_IS_IS2-VERSION2.doc

[37] **BARAJAS**, Saulo. "*Seguridad en BGP*".
URL: http://www.saulo.net/pub/inv/BGP-art.htm

[38] **ANÓNIMO**. "*Border Gateway Protocol*".
URL: http://www.aulafacil.com/cursosenviados/ bordergateway.htm

[39] **ANÓNIMO**.
URL: http://www.ccapitalia.net/netica/teleco/mpls-v3.pdf

[40] **ANÓNIMO**.
URL: http://cisco-press-traffic-engineering.org.ua/1587050315/ ch02lev1sec3.html

CAPÍTULO 2

RED IP/MPLS DE LA CNT E.P.

Este capítulo se enfoca en determinar las diferentes prestaciones que la red de la CNT E.P. ofrece con esta plataforma, realizando un estudio de la red para determinar los servicios y productos que actualmente se ofrecen. Además se determina las diferentes capacidades y servicios que pueden entregar los routers con los que dispone la CNT E.P para el desarrollo del laboratorio, en función de su ubicación jerárquica dentro de la red, core: cisco CRS-4, distribución: cisco ASR1006, cisco GSR12810, acceso: cisco 6524, cisco 2800, cisco 7600.

CAPÍTULO 2

RED IP/MPLS DE LA CNT E.P.

2.1 INTRODUCCIÓN:

Si bien CNT E.P. tradicionalmente ha sido una empresa de telefonía en la actualidad con los cambios que se han dado en el sector de las telecomunicaciones ha tenido que expandir los servicios que ofrece para satisfacer los requerimientos actuales de los clientes, esto debido a la gran demanda de servicios interactivos por parte de los clientes.

Otro de los factores que ha influido en cómo se ha desarrollado la empresa es la expansión de internet como un medio en el que se dispone de varias opciones como información, entretenimiento, ventas y demás servicios, adicionalmente las necesidades de clientes empresariales de interconectar sus redes privadas han llevado a que se producen una serie de cambios para satisfacer estos requerimientos.

Para satisfacer estas nuevas necesidades la empresa en los últimos años se ha visto en la necesidad de cambiar y migrar a tecnologías que permitan ofrecer servicios convergentes, una de las tecnologías que se ha desarrollado para esto es IP/MPLS, con la que CNT pretende tener una red de transporte de información adecuada para los cambios actuales y futuros.

El escoger este tipo de tecnología ha permitido que se integren bajo una misma plataforma un conjunto de tecnologías heredadas de sistemas de comunicación anteriores, permitiendo realizar una migración por etapas y reutilizado recursos como la gran infraestructura de par trenzado en última milla o la red de transmisión *Synchronous Digital Hierarchy (SDH)* e integrarla con tecnologías nuevas como *Dense Wavelength Division Multiplexing (DWDM).*

A continuación se realiza una descripción de los elementos que integran la red de la CNT, hay aspectos sobre los cuales no se hace mayor énfasis debido a que es información que la empresa se reserva y no puede ser presentada.

2.2 REDES DE ACCESO [8]

Es la parte que se encuentra ubicada entre el abonado y el primer nodo de la empresa proveedora de servicios y se la conoce como última milla es una de las partes más costosas y difíciles de implementar de la red, por lo que se han desarrollado varios alternativas tecnológicas que permitan una utilización adecuada de estos recursos.

Las aplicaciones multimedia que cada día tienen más demanda por parte de los usuarios, requieren una mayor velocidad de transmisión para satisfacer los requerimientos de estas, por esta razón se han desarrollado un conjunto de técnicas que permiten obtener grandes velocidades de trasferencia en los medios de transmisión convencionales.

La Corporación Nacional de Telecomunicaciones para satisfacer este tipo de servicios y basándose en la gran infraestructura de par de cobre instalado con la que dispone utiliza la tecnología *Digital Suscriber Line (DSL)* para su acceso de última milla de cobre, también dispone de una red WIMAX como acceso inalámbrico, y fibra óptica a las oficina en caso de que los clientes necesiten, llegando a ofrecer velocidades de acceso a la red de 1 Gbps Ethernet.

2.2.1 DSL *(DIGITAL SUSCRIBER LINE)* [8] [9] [41]

La línea digital de abonado es un conjunto de tecnologías que permiten transmitir datos sobre líneas telefónicas tradicionales, las velocidades de transmisión van desde los 100Kbps hasta los 100Mbps dependiendo de la tecnología, distancia entre el punto de presencia y el hogar del cliente y el calibre del par telefónico.

Dentro de las tecnologías DSL existen dos tipos: la asimétrica (ADSL) y la simétrica (SDSL) las mismas que abarcan un conjunto amplio de variantes que

permiten alcanzar diferentes velocidades y distancias de cobertura, está compuesta de varios componentes que se muestran a continuación:

Bucle de Abonado: es el par de cobre que se encuentra ubicado entre el punto de presencia del proveedor y el cliente.

***Splitter*:** Es un filtro que separa los servicios de datos de DSL y los de telefonía tradicional que se transmiten por un mismo par de cobre.

Modem DSL: Equipo ubicado en el lado del proveedor y el cliente encargado de modular y demodular las señal adaptándolas para enviarlas por el medio físico.

DSLAM: el multiplexor de acceso DSL es un equipo ubicado en un punto de presencia del proveedor que tiene varios módems DSL uno para cada abonado, se encarga de concentrar el tráfico de los diferentes clientes y enviarlo a la red WAN.

En la figura 2.1 se muestran los diferentes componentes que conforman una última milla DSL en la red de un proveedor de servicios.

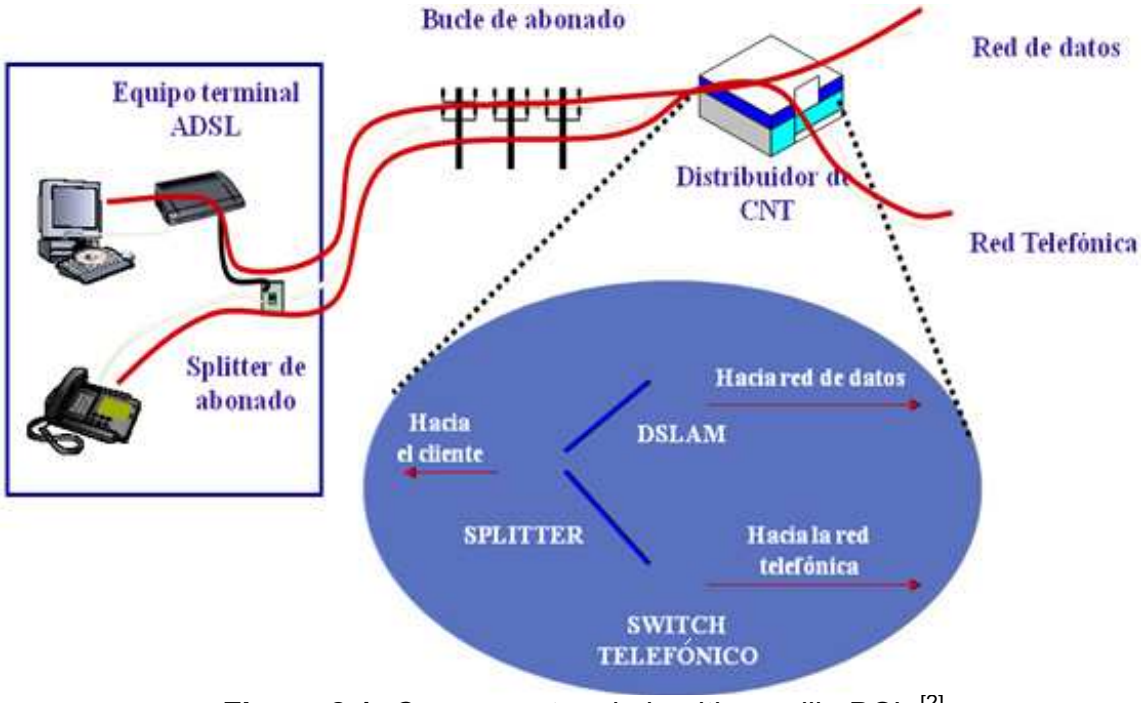


Figura 2.1: Componentes de la ultima milla DSL [2]

La tecnología DSL aprovecha el espectro no utilizado del par de cobre, partiendo de que la transmisión de voz se da entre los 330Hz a los 3KHz se considera un rango de 4KHz para la transmisión de voz por lo que se usa las frecuencias superiores a esta hasta 2,2Mhz para la transmisión de los datos.

2.2.1.1 ADSL (*Asymmetric* DSL)

Esta clasificación general hace referencia a enlaces en los que la velocidad de bajada es superior a las de subida, este esquema se usa para los clientes residenciales que acceden a internet, pues la tecnología se ajusta al comportamiento de estos. En la tabla 2.1 se describe las principales tecnologías ADSL existentes.

Tecnología DSL	ADSL	ADSL2	ADSL2+	G.Lite	VDSL	VDSL2
Velocidad de subida máxima	1Mbps	1Mbps	1,2Mbps	900Kbps	52Mbps	100Mbps
Velocidad de Bajada máxima	8Mbps	12Mbps	24Mbps	1,5Mbps	6Mbps	-
Distancia	2Km	2,5Km	2,5Km	2Km	1Km	500m
Estándar	ITU G.992.1 T1.413	ITU G.992.3/4	ITU G.992.5	ITU G.992.2	ITU G.993.1	ITU G.993.2
Número de pares de cobre	1	1	1	1	1,2 o 4	1,2 o 4

Tabla 2.1- Tecnologías asimétricas DSL [9]

2.2.1.2 SDSL (*Symmetric DSL*)

Este tipo de tecnología permite la misma velocidad de subida y bajada lo que permite satisfacer las necesidades de clientes corporativos facilitando la conexión entre varias intranet de la empresa ubicadas en diferentes locaciones,

a través de red de la corporación nacional de telecomunicaciones manteniendo el acceso por el par de cobre de la telefonía tradicional lo que abarata los costos en el acceso, a continuación en la tabla 2.2 se describen las tecnologías simétricas.

Tecnología DSL	HDSL	HDSL2	HDSL4	SDSL	VDSL	VDSL2
Velocidad de Tx	T1 1.544Mbps E1 2.048Mbps	T1 1.544Mbps E1 2.048Mbps	T1 1.544Mbps E1 2.048Mbps	2Mbps	26Mbps	50Mbps
Distancia	2700 m	2700 m	3300 m	3000m	1Km	500m
Estándar	ITU G994.1	-	-	ITU G.991.2	ITU G.993.1	ITU G.993.2
Número de pares de cobre	2	1	2	1	1,2 o 4	1,2 o 4

Tabla 2.2- Tecnologías simétricas DSL [9]

2.2.2 WIMAX [10] [16] [17]

WIMAX (Worldwide Interoperability for Microwave Access) se encarga de certificar la compatibilidad e interoperabilidad de equipos de varios fabricantes, para esto se creó el WIMAX fórum que certifica productos que operan en frecuencias alrededor de 2.3GHz, 2.5GHz, 3.5GHz y 5.8GHz, adicionalmente trabajo con el ETSI[1] para una mejor compatibilidad entre tecnologías.

Es una tecnología basada en el estándar inalámbrico IEEE 802.16 y brinda acceso de banda ancha con voz, video y datos a nivel metropolitano, es una alternativa para los accesos xDSL y de cable modem, por lo que brinda velocidades similares con una menor dificultad de implementación y menor costo.

[1] *European Telecommunications Standards Institute*

Dentro de las principales características de esta tecnología están las grandes velocidades de transmisión que pueden alcanzar hasta 75 Mbps, con una cobertura de 50 a 60 Km, movilidad de de hasta 50 o 60 Km/h y no necesita línea de vista entre el transmisor y el receptor, se utilizan dos estándares 802.16d fijo y 802.16e móvil.

En la tabla 2.3 se indica un cuadro comparativo con las principales características de los estándares de la IEEE disponibles actualmente.

Estándar	IEEE 802.16	IEEE 802.16d	IEEE 802.16e
Estatus	Completo en diciembre 2001	Completo en Julio 2004	Completo diciembre 2005
Frecuencias	10GHz - 66GHz	2GHz – 11Ghz	2GHz – 6Ghz (Móvil) 2GHz – 11Ghz (Fijo)
Línea de vista	Si	No	No
Tasa de Transmisión	32Mbps-134Mbps	1Mbps – 75 Mbps	1Mbps – 75 Mbps
Cobertura	6 – 10 Km	6 – 10 Km	5 – 8 Km
Movilidad	No aplica	No aplica	Hasta 60 Km/h

Tabla 2.3- Comparación de los diferentes estándares IEEE [10]

En el cuadro comparativo se observan las diferentes características que WIMAX brinda, siendo las tecnologías IEEE 802.16d y IEEE 802.16e las utilizadas por CNT dentro de su red.

La topología de la red WIMAX es la que se observa en la figura 2.2 donde se tienen varias estaciones base de transmisión (BTS) en las que acceden diferentes clientes tanto corporativos como residenciales a la red de transporte IP/MPLS que a su vez los conecta con otro proveedores o a internet.

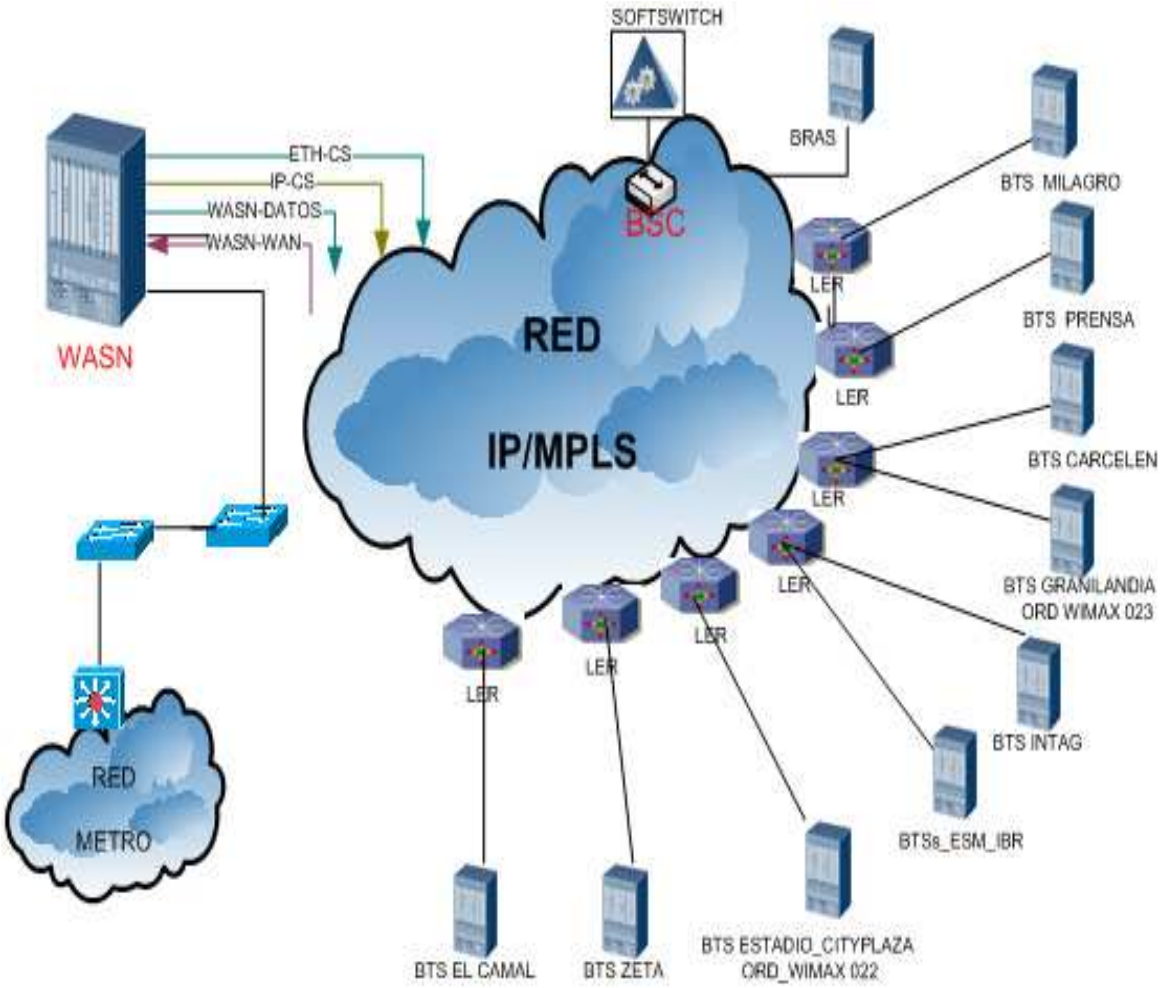


Figura 2.2: Diagrama de la red WIMAX de CNT E.P. [2]

2.3 RED DE TRANSPORTE [2]

La Corporación Nacional de Telecomunicaciones CNT EP en su afán de cubrir las necesidades del país, actualmente cuenta en su red de transporte con tecnologías como enlaces de radio, SDH, *next-generation SDH (NG-SDH),* DWDM y fibras ópticas directas.

El dimensionamiento de las capacidades no solo fue pensado en las necesidades actuales sino también pensando en los posibles crecimientos futuros de tal manera que estas redes proporcionen flexibilidad, alta confiabilidad y protección.

En la figura 2.3 se indica las diferentes plataformas tecnológicas de acceso, transmisión y conmutación de paquetes disponibles en la infraestructura de servicios de la CNT E.P.

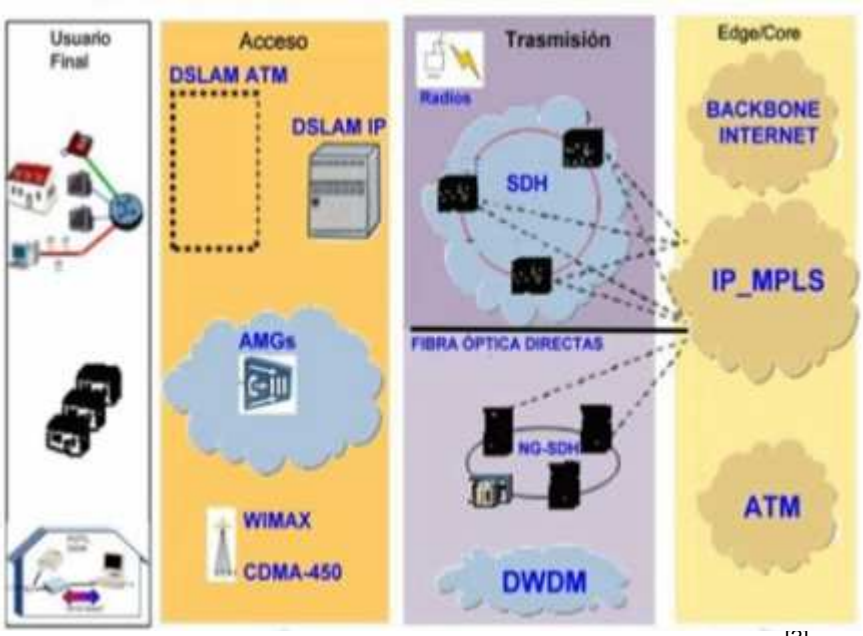


Figura 2.3: Plataformas Tecnológicas CNT E.P [2]

2.3.1 *RED SDH (SYNCHRONOUS DIGITAL HIERARCHY)* [2] [12]

En la tabla 2.4 se indican los diferentes anillos SDH con la capacidad de transmisión de cada uno de estos.

Red	Zona de concentración de tráfico	Capacidad Instalada
Norte	Noroccidente de la Provincia Pichincha	252 Mbps
Pichincha	Nororiental y Oriental *(valles de la ciudad de Quito)* de la Provincia de Pichincha	570 Mbps
Anillo Aeropuerto	Nororiental de Quito (valles nororientales como Cumbayá, Tumbaco, Pifo, Tababela, etc)	13,2 Gbps
Anillo Oriente	Provincia de Napo, Provincia de Orellana, suroriente de la Provincia de Pichincha, parte de la zona sur de la Provincia de Sucumbíos, *Central Ambato* en la Provincia de Tungurahua	903 Mbps
Anillo Oriente Huawei	Este anillo cubre las mismas zonas que el anillo oriente con nuevos nodos y repetidores.	1248 Mbps

Tabla 2.4- Resumen de los anillos SDH en la Region 2 de CNT. [2]

Un ejemplo de esto son las cinco redes SDH de la región 2: “Red Norte, Red Pichincha, Anillo Aeropuerto, Anillo Oriente, Anillo Oriente Huawei” todas estas redes se encuentran gestionadas desde la central de Quito Centro, muchas de

estas redes se enlazan mediante transmisiones de radio, algunas de estas se han ido remplazando mediante enlaces de fibra óptica, quedando de respaldo los enlaces de radio.

Pero debido a la gran demanda que ocasionarían los nuevos servicios que están por salir al mercado como lo son Video, IPTv, VoIP, Televisión codificada, entre otros. Se realizó la integración de la tecnología SDH con DWDM dando una solución a la al aumento de capacidad.

2.3.2 *DWDM (DENSE WAVELENGTH DIVISION MULTIPLEXING)* [2] [47]

"La red DWDM está compuesta por tres anillos principales que cubren la parte norte, centro y sur del país, que mediante la conexión con redes NG–SDH que conforman la Red Nacional de Transmisión, permiten transportar grandes cantidades de tráfico, utilizando, de forma eficiente, la red de fibra óptica de CNT S.A., y así ser la infraestructura de transporte de las redes de acceso y de la red IP/MPLS"[2]. En la figura 2.4 se observa un conjunto de tecnologías que se pueden encapsular y transmitir utilizando DWDM.

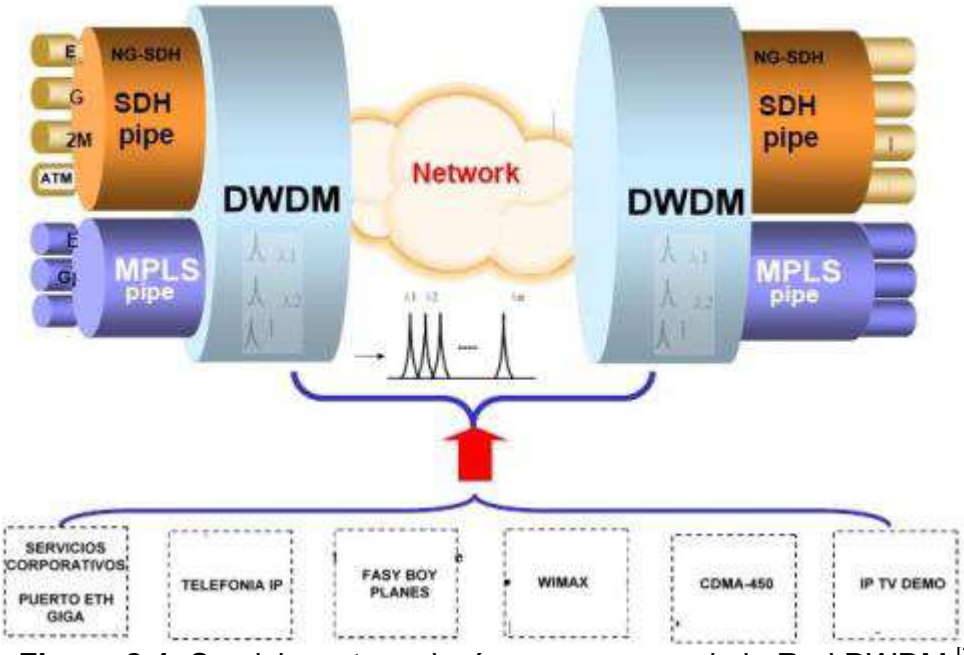


Figura 2.4: Servicios y tecnologías que encapsula la Red DWDM [2]

[2] Información tomada de: http://www.cronica.com.ec/index.php?option=com_content&view=article&id=8243:la-cnt-cumplio-en-el-ano-2009-con-el-pais&catid=38:nacionales&Itemid=53

La Red de Transporte Óptico de Larga Distancia mostrada en la figura 2.5 consiste de 2 anillos:

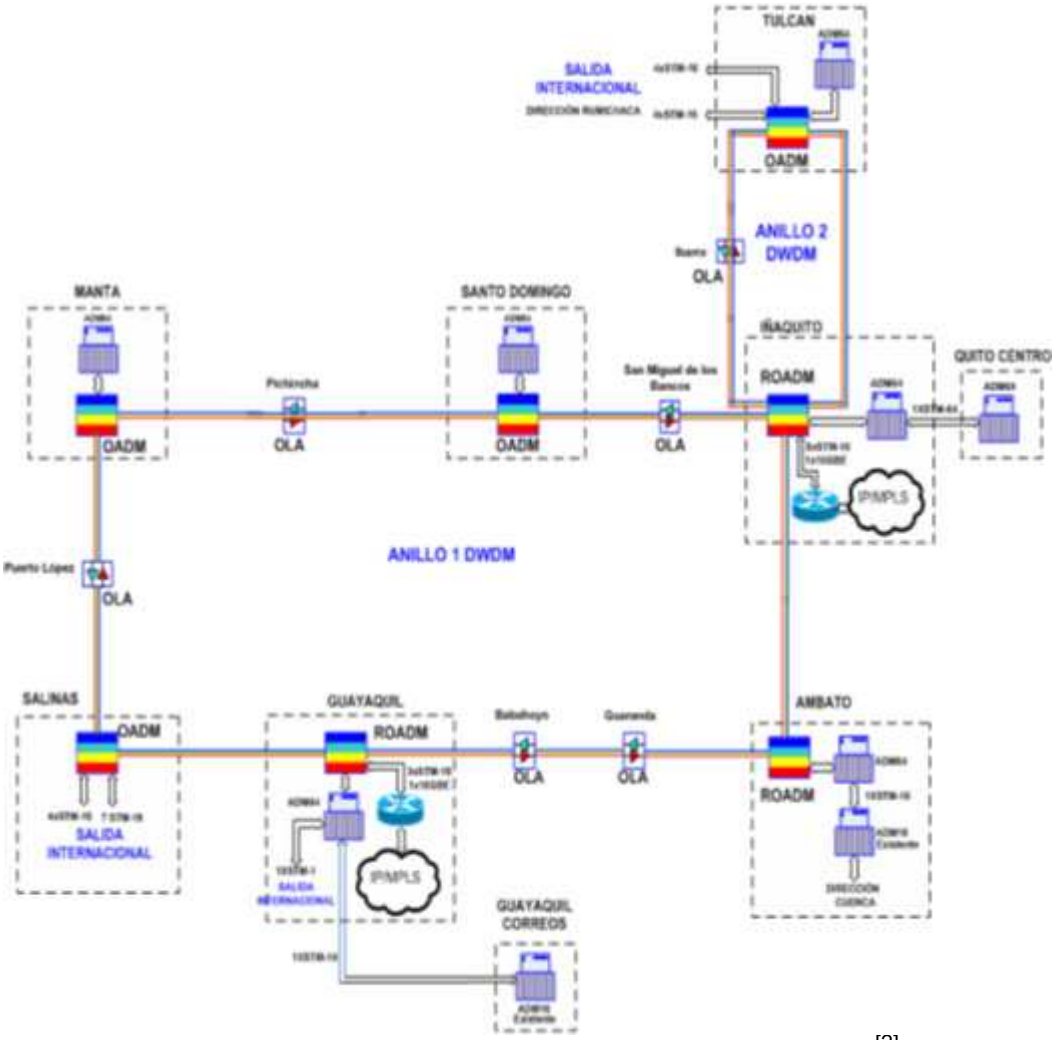


Figura 2.5: Topología de Red DWDN CNT E.P [2]

El anillo 1 consiste de 13 segmentos: Iñaquito, Latacunga, Ambato, Guaranda, Babahoyo, Guayaquil, Salinas, Puerto López, Manta, Pichincha, Quevedo, Santo Domingo, San Miguel, Iñaquito.

El anillo 2 consiste de 4 segmentos: Iñaquito, Tulcán, Ibarra, Cayambe, Iñaquito.

Las estaciones de Iñaquito, Ambato y Guayaquil son *ROADM*. Salinas, Manta, Santo Domingo y Tulcán son estaciones *Back-to-Back*. Latacunga, Guaranda, Babahoyo, Puerto López, Pichincha, Quevedo, San Miguel, Ibarra y Cayambe son estaciones OLA.

La capacidad diseñada de la red es de 96 longitudes de onda, 96*10Gbps. Inicialmente. En adición, se adoptado la topología de anillo doble, el cual permite el balanceo de carga de tráfico así como la protección de rutas de tráfico múltiples. Esto permitirá tener una red fiable y robusta.

2.3.3 NG-SDH [2]

De acuerdo con el tipo de servicio y el requerimiento de capacidad, el principal servicio es E1, DS3, STM-1, STM-16. En el nivel NG-SDH, el sistema accederá a todos los servicios y convergirá a STM-64. Dispone de 1 anillo STM-64 NG-SDH, por lo que usará 1 longitud de onda en el anillo DWDM, este se observa en la figura 2.6.

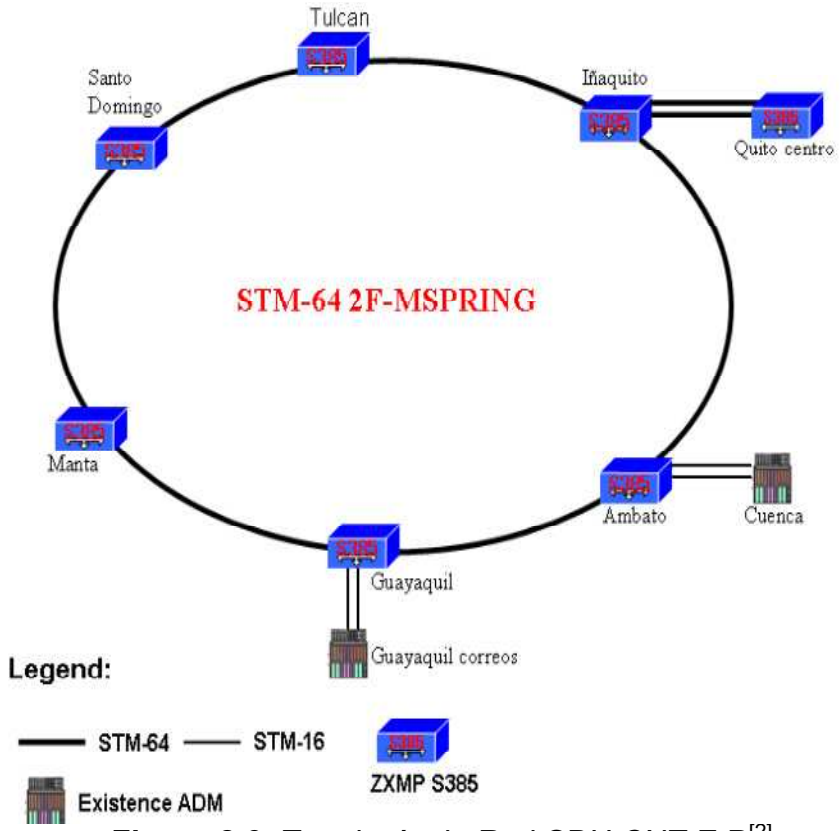


Figura 2.6: Topología de Red SDH CNT E.P[2]

El anillo SDH incluye estos sitios: Iñaquito, Quito Centro, Ambato, Guayaquil, Manta, Santo Domingo, Tulcán. Aquí se instalarán Multiplexores SDH (ADM64) para que se interconecten a los equipos DWDM y entregar interfaces de usuario para los diferentes servicios.

2.3.4 FIBRAS ÓPTICAS [2] [48]

El tendido de fibra óptica de los enlaces de la CNT S.A. es aéreo sujetado de los postes del tendido eléctrico y en algunos casos subterráneos, el cable de fibra óptica usado es totalmente dieléctrico y auto soportado (ADSS), es un cable de fibras monomodo de 12 hilos, indicado en la figura 2.7,

Figura 2.7: Fibra monomodo anillada [48]

La CNT describe de la siguiente manera su *backbone* de fibra:

"Somos propietarios de la red de fibra óptica más grande a nivel nacional, con más de 10.000 Km de fibra óptica instalada en todo el territorio Ecuatoriano." [3]

"La fibra óptica de mayor calidad del Ecuador." [3]

"Nuestra Fibra Monomodo y anillada, permite mayor calidad en la transmisión de datos y garantiza una alta disponibilidad en la red."[3]

"Nuestra fibra óptica incluye triple protección en el cable, chaquetas de seguridad, material anti-roedores y con alma de acero." [3]

"Implementación a través de canalización subterránea, brindando mayor seguridad para garantizar el servicio." [3]

"Implementación y operación conforme a estándares internacionales, tales como el 568B.3.1." [3]

En la figura 2.8 se indica la fibra óptica instalada de la que dispone la CNT.

[3] Información tomada de: http://www.cnt.com.ec/index.php?option=com_content&view=article&id=230&Itemid=23

Figura 2.8: Red Nacional de Transmisión CNT E.P. situación a fines de 2010 [2]

2.4 MODELO JERÁRQUICO DE RED [1] [2]

El modelo de red jerárquico de Cisco divide a una red en varias capas en las que cada una realiza funciones especificas, permitiendo que una red sea modular, facilitando la administración, la escalabilidad y el rendimiento con una rápida resolución de problemas, generalmente el modelo de 3 capas es el más utilizado y el que se utiliza en el *backbone* IP/MPLS de CNT.

El modelo de tres capas consta de acceso, distribución y núcleo que permiten la agregación y filtrado de tráfico en tres niveles de enrutamiento o *switching*, con este modelo adicionalmente se la implementa redundancia a nivel de núcleo como de distribución pues son equipos críticos y se incrementa la seguridad por puerto en el acceso.

2.4.1 CAPA DE CORE

La capa núcleo del diseño jerárquico es la *backbone* de alta velocidad de la *internetwork*. La capa núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo sea sumamente disponible y redundante. El área del núcleo también puede conectarse a los recursos de Internet. El núcleo agrega el tráfico de todos los dispositivos de la capa de distribución, por lo tanto debe poder reenviar grandes cantidades de datos rápidamente.

El *core* de la red MPLS está conformado por equipamiento Cisco CRS-1/8. A continuación se entregan detalles de la configuración física de estas plataformas.

El CRS-1 consta de un conjunto mecánico que contiene tarjetas modulares de servicio, o modular *service cards (MSCs),* y sus asociados módulos de interfaz de capa física, o *physical layer interface modules (PLIMs),* tarjetas de *switch fabric* y tarjetas procesadoras de ruteo, o *route processers (RPs).*

En el caso de C.N.T E.P corresponde al modelo *stand-alone* CRS-1 de 8 tarjetas de línea el cual dispone de un IOS del tipo XR, el cual posee 8 *slots* para MSCs,

cada una con una capacidad de conmutación de 40Gbps *full duplex*, por lo que la capacidad de conmutación agregada es de 640 Gbps.

Estos equipos poseen redundancia tanto de sus tarjetas procesadoras, de sus tarjetas de conexión al *switch fabric*, así como también de componentes físicos como fuentes de alimentación, unidades de distribución de energía y dispositivos de ventilación.

2.4.2 CAPA DE DISTRIBUCIÓN

Es un punto de demarcación entre las capas de acceso y distribución y cumple algunas funciones como controlar el acceso a los recursos para implementar seguridad, controla el tráfico que ingresa al *core* para mejorar el rendimiento, optimizar los protocolos de enrutamiento realizando la sumarizacion de rutas de la capa de acceso.

Dentro de la CNT esa capa se maneja con dos tipos de nodos denominados tipo a y tipos b, a continuación se detallan lo que los conforman:

2.4.2.1 Nodos Tipo A:

Los nodos de Distribución Tipo A son los 12000/10 y 12000/16 de la familia Cisco XR 12000 que disponen de un IOS del tipo XR .Los nodos de Distribución Tipo A /10 disponen de dos fuentes de alimentación DC. Estas fuentes de alimentación trabajan en redundancia 1:1 (si una de las fuentes sufre daños, la otra soporta toda la operación del nodo) y soportan la agregación de módulos adicionales, el /16 se dispone de cuatro fuentes de alimentación DC, las cuales funcionan con las mismas características de redundancia descritas anteriormente.

Dispone también de dos tarjetas de procesamiento “PRP-2” que trabajaran en redundancia 1:1, un conjunto de SFC “12810-SFC” “Cisco 12810 800Gbps *Switch Fabric Card*”, que trabajarán en redundancia 4:1, dos “12810-CSC” “12810 *Clock Scheduler Card*”, que trabajaran en redundancia 1:1, dependiendo del número de puertos WAN a 10 y a 1 Gbps (pueden ser LX o ZX) cada nodo dispondrá del número necesario de tarjetas y módulos.

2.4.2.2 Nodo de Distribución Tipo B

Todos los nodos de Distribución Tipo B corresponden al modelo 7609-S de la familia Cisco Routers 7600 que disponen de un IOS, dispone de dos fuentes de alimentación DC. Estas fuentes de alimentación trabajan en redundancia 1:1. Igualmente la capacidad de cada fuente soporta la agregación de módulos adicionales.

También dispone de dos tarjetas de procesamiento “RSP720-3CXL-GE” “Cisco 7600 *Route Switch Processor* 720 *Gbps fabric*, PFC3CXL, GE” que trabajaran en redundancia 1:1. Dependiendo del número de puertos WAN a 10 y 1 Gbps requeridos, cada nodo dispondrá del número necesario de tarjetas y módulos.

2.4.3 CAPA DE ACCESO

La capa de acceso se encarga de de concentrar las diferentes tecnologías de ultima milla tales como xDSL (*Digital Subscriber Line*), xPoN (*Passive Optical Networks*), HFC (*Hybrid Fiber Coaxial*), WiMax (*Worldwide Interoperability for Microwave Access*), Ethernet y redes Celulares 2G, 3G y 4G.

El principal objetivo de esta capa de acceso es la de conectar los diferentes clientes *(CPEs, Customer Premise Equipment)* a la red del *Carrier*. Pueden ser servicios Triple Play (Internet, Telefonia y Video) para usuarios residenciales, servicios de L2- VPN y L3-VPN para usuarios empresariales y servicios de transporte de Voz y Datos para la red Celular.

Esta capa de Acceso implementa mecanismos de conmutación y transporte de VLANs basados en 802.1Q y 802.1ad (QinQ), e incorpora protocolos de control y redundancia basados en *MST (Multiple Spanning Tree).* Dentro de la red de CNT se manejan dos tipos de nodos de acceso denominados tipo A, y tipo B cuyas características se detallan a continuación:

2.4.3.1 Nodos de Acceso Tipo A

Todos los nodos de Acceso Tipo A corresponden al modelo 7606-S de la familia Cisco Routers 7600, Disponen de un IOS dispone de dos fuentes de alimentación

DC de 2700 W. Estas fuentes de alimentación trabajan en redundancia 1:1, dispone de una tarjeta de procesamiento “RSP720-3C-GE” “Cisco 7600 *Route Switch Processor* 720Gbps *fabric*, PFC3C, GE”. Dependiendo del número de puertos WAN a 10 y 1 Gbps requeridos, cada nodo dispondrá del número necesario de tarjetas y módulos. En estos nodos en las interfaces LAN se colocan tarjetas de 48 puertos.

Esta capa se encuentra integrada por los equipos denominados como “Nodos de Acceso tipo A”, al estar basada en IP/MPLS, esta capa de agregación permite manipular la diversidad de servicios de manera eficiente, flexible y escalable, utilizando técnicas tales como *PWE3 (Pseudowire Emulation)* para transporte *Ethernet (*EoMPLS*, Ethernet over MPLS),* ATM (ATM *over* MPLS) y *TDM (SAToP, Structure-Aware Time Division Multiplexed y CESoPSN, Circuit Emulation Service over Packet Switched Network),* como así mismo permite implementar servicios de L2-VPN (E-Line y E-LAN por medio de *VPLS* (*Virtual Private LAN Service*).

Esta capa de agregación permite adicionalmente manipular en forma más eficiente los servicios basados en el uso de conmutación IP, tal como distribución de *Video Unicast (VoD)* y *Multicast (Video Broadcast).* Usa un plano de control basado en IP y conmutación basada en MPLS además cuenta con mecanismos rápidos y eficientes de recuperación y reparación de fallas que permiten asegurar una Alta Disponibilidad en la red *Carrier Ethernet.*

2.4.3.2 Nodos de Acceso Tipo B

Todos los nodos de Acceso Tipo B corresponden al modelo ME6524 disponen de un IOS, dispone de dos fuentes de alimentación DC. Estas fuentes de alimentación trabajan en redundancia 1:1, disponen de una tarjeta interna *PFC3C (Policy Feature Card 3D*) y una tarjeta hija MSFC2A, con capacidad de conmutación de 32 Gbps, un desempeño de hasta 15 Mpps. poseen 8 puertos de WAN, Y 24 Puertos LAN en los cuales pueden ser introducidos GLC.

Cada nodo dispondrá del número necesario módulos SFP GLC-LH-SM, GLC-ZX-SM, 1000BASE-ZX SFP, y 1000BASE-T SFP.

2.5 CARACTERÍSTICAS DE LOS EQUIPOS DE LA CNT E.P.

2.5.1 SISTEMA DE ENRUTAMIENTO CISCO CRS-1 DE 4-RANURAS [18]

El sistema de enrutamiento para *carrier* Cisco *CRS-1 (Carrier Routing System)* ofrece un sistema de operación continuo, flexibilidad de servicios, y longevidad del sistema. Utiliza el software Cisco IOS XR que operación 24/7, con una capacidad del sistema de hasta 92 Tbps. Utiliza el procesador de paquetes Cisco *Silicon Packet Processor*, un circuito integrado para aplicaciones específicas (ASIC) programable de 40 Gbps. El chasis de CRS-1 se indica en la figura 2.9.

Figura 2.9: Cisco CRS-1 4-Slot Single-Shelf System [18]

2.5.1.1 *Route Processors* (RP) [19]

En la figura 2.10 se indica un tarjeta procesadora (RP), para un sistema de enrutamiento CRS-1.

Figura 2.10: Tarjeta Route Processor [19]

Las tarjetas *route processor (RP)* son quienes realizan el procesamiento de ruteo en el CRS-1. Las mismas realizan todas las tareas del plano de control relacionadas con el procesamiento y la distribución de la información de ruteo y conmutación hacia las MSCs. La RP aporta un canal de control a cada MSC, realiza funciones de monitoreo del sistema y tiene un soporte físico en forma de disco rígido para almacenar configuraciones e información de *logging*[4].

Dispone de un Puerto de Consola (conector RJ-45), Puerto Auxiliar (conector RJ-45), Un Puerto Ethernet 10/100/1000 (conector RJ-45) y Dos puertos Ethernet 10/100/1000 (1000BASE-LX *Small Form-Factor Pluggable (SFP)* – Conector LC, 10 km) para conectividad del plano de control. La tarjeta RP es también la encargada de controlar el sistema en el CRS-1 las funcionalidades son las siguientes:

- Controladora del sistema
- Un multiprocesador simétrico de CPU dual realiza el procesamiento de ruteo. La CPU también sirve como procesador de servicio de las MSC, y monitorea la temperatura, voltaje márgenes de alimentación.
- Un puerto Ethernet de cobre 10/100/1000 provee conectividad para los sistemas de administración de red.
- Conexiones internas Fast Ethernet (FE) de 100 Mbps conectan cada MSC del chasis a ambas RPs.
- Un disco duro IDE es utilizado para almacenar información de *debugging*.[5]
- Slots de memoria flash PCMCIA proveen soporte para dos tarjetas de 2 GB cada una para almacenamiento flash.
- Controla los ventiladores, alarmas y fuentes de energía.

2.5.1.2 *Modular Services Card* (MSC) [31]

El módulo MSC (*modular services card*) es el motor de *forwarding* de nivel 3 del sistema CRS-1. Cada MSC se empareja con un módulo de interfaz de capa física o *physical layer* interface module (PLIM), a través del llamado *midplane*, que es

[4] Información de los cambios que el administrador realiza en los equipos.
[5] Información de los mensajes de depuración de operaciones del equipo.

un *backplane* pasivo que provee interconexión eléctrica. Estos módulos son los que finalmente contienen las interfaces físicas correspondientes.

Una MSC puede emparejarse con distintos tipos de PLIMs para proveer una amplia gama de interfaces tales como OC-768/STM-256 POS y 10-Gigabit Ethernet. Cada MSC y su PLIM asociada implementan los Niveles 1 a 3 del modelo OSI.

Cada MSC entrega un rendimiento a velocidad de línea de 40 Gbps de tráfico agregado. Servicios adicionales tales como procesamiento de QoS, replicación multicast, ingeniería de tráfico (TE) y recolección de estadísticas, son también provistos a 40 Gbps.

Las MSCs soportan diversos protocolos de *forwarding*, incluyendo IPV4, IPV6 y MPLS. La tarjeta *route processor* (RP) cumple las funciones de ruteo y distribución de tablas de ruteo, mientras que la MSC realiza el *forwarding* de los datos.

2.5.1.3 *Physical Layer Interface Modules* (PLIM)

El módulo de interfaz de capa física o *physical layer interface module (PLIM)* provee las interfaces físicas para el sistema de ruteo. Los módulos ópticos en la PLIM contienen puertos a los que se conectan los cables de fibra óptica. Los datos de usuario son recibidos y transmitidos a través de los ports de la PLIM, y convertidos de la señal óptica (usada en la red) a la señal eléctrica (usada por los componentes del chasis). En la figura 2.11 se indica una PLIM.

Figura 2.11: Tarjetas PLIM [31]

Las PLIM realizan principalmente funciones de capa 1 y capa 2, relegando las funciones de capa superior a la MSC, para lo cual cada PLIM se conecta con una

MSC a través del *midplane*. Actualmente están disponibles diferentes tipos de *Fixed-PLIMs*, tales como OC-768/STM-256 POS, y 10-Gigabit Ethernet.

2.5.1.4 Procesador de Interfaces SPA – 800 (SIP-800) para los Cisco CRS-1[20]

Las Port Adapter Inteface Processors (SIP) y adaptadores de puerto compartido o *Shared Port Adapters (SPAs),* se pueden instalar en vez de PLIMs. Una placa SIP es similar a una PLIM y se inserta en el mismo slot, para interconectarse con una MSC tal como las PLIMs. Al contrario de las PLIMs, las SIPs no contienen interfaces físicas pues se necesitan módulos para esto.

Una SPA es un tipo modular de adaptador de puerto que se inserta en un *subslot* de la tarjeta SIP para proveer conectividad de red e incrementar la densidad de interfaces. En la figura 2.12 se indica un tarjeta SIP y algunos SPAs de Cisco.

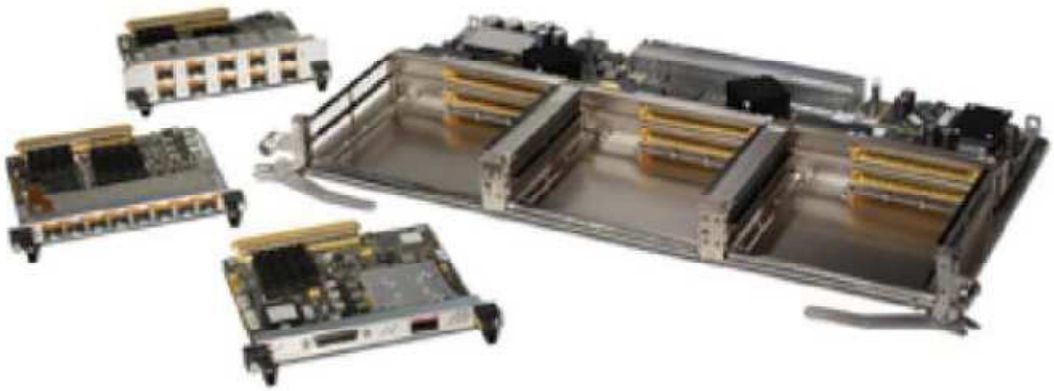


Figura 2.12: SIP-800 y SPAs para los Cisco CRS-1[20]

2.5.2 ROUTERS DE LA SERIE CISCO XR 12000 Y CISCO 12000 [21]

Los routers de esta serie están compuestos de un portafolio de soluciones inteligentes de enrutamiento que escalan su capacidad de 2.5 a n x 10 Gbps por ranura habilitando redes *carrier class*[6] IP/MPLS, permiten manejar una capacidad de conmutación de hasta 1,28 terabits por segundo con un desempeño de procesamiento *wire-speed*[7], escalabilidad y fácil actualización.

---

[6] Término utilizado para hacer referencia a sistemas que son altamente confiables orientados a proveedores de servicios.

[7] Indica que hay poca o ninguna sobrecarga de tiempo por software en la trasmisión por lo que se obtiene la velocidad física de la interfaz.

Este portafolio tiene una arquitectura de reenvió de paquetes completamente distribuida y una matriz de conmutación *(crossbar switch-fabric)*[8] de alta eficiencia. La combinación de un planificador centralizado y tecnología de encolamiento virtual de salida (VOQ) maximiza el uso del ancho de banda de la matriz de conmutación *switch-fabric*, minimizar la latencia, y ofrece un desempeño sin bloqueo. Se utilizan circuitos integrados para aplicaciones específicas de alto desempeño (ASIC) para proveer transmisión con velocidades iguales a las de línea manteniendo un estricto control del *jitter* y la latencia requeridos para servicios de tiempo real. Lo que permite brindar calidad de servicio (QoS), IP/MPLS, y alta disponibilidad. Los routers de las series Cisco 12000 mostrados en la figura 2.13 utilizan el software Cisco IOS XR y Cisco IOS.

Figura 2.13: Ruteadores de la serie 12000 [21]

2.5.2.1 Procesador de Enrutamiento "*Performance Route Processor-2*" para los Cisco 12000. [22]

El procesador de enrutamiento *Performance Route Processor-2 (PRP-2)* son quienes realizan el procesamiento de ruteo, las mismas realizan todas las tareas del plano de control relacionadas con el procesamiento y la distribución de la información de ruteo y conmutación para los Cisco 12000, ofrece hasta 4 GB de memoria, un Puerto de administración Gigabit Ethernet, y la opción de una unidad

[8] Una tecnología de conmutación que utiliza una matriz para conectar múltiples entradas con múltiples salidas.

de disco duro. Ofrece una interfaz BITS *(Building Integrated Timing Supply)*[9]. En la figura 2.14 se indica un tarjeta PRP-2.

Figura 2.14: Cisco XR 12000 y 12000 PRP-2 [22]

La PRP-2 realiza las siguientes funciones:

- Ejecución de pilas de protocolos de enrutamiento
- Realiza todas las comunicaciones de los protocolos con otros routers.
- Construir y distribuir información de reenvió a todas las tarjetas en línea.
- En el momento del encendido cargar las imágenes del software del sistema operativo a las tarjetas de línea instaladas.
- Proveer de puertos de consola, un auxiliar fuera de banda, y un Puerto Ethernet para mantenimiento y configuración del router.
- Monitorear y administrar la energía y la temperatura de los componentes del sistema como las tarjetas de línea, fuentes de poder, y ventiladores.

2.5.2.2 Procesador de Interfaz SPA (SIP) para los routers Cisco 12000 [23] [42]

En la figura 2.15 se muestra una tarjeta SIP y varios SPAs.

Figura 2.15: SIP para los routers Cisco 12000 con los SPAs. [23]

[9] Es un sistema de temporización centralizado para todos los equipos de telecomunicaciones dentro de un edificio.

El diseño de las interfaces I-Flex combina los SPAs *(shared port adaptors)* y los *SIPs (SPA interface processors),* haciéndolo escalable y facilitando la priorización de servicios de voz, video, y datos. La estructura de ranuras permite el intercambio de módulos entre las diferentes plataformas. El SIP (SIP 401, SIP 501, y SIP 601) para los routers Cisco XR 12000 y 12000 proveen:

- Un motor común de transmisión y encolamiento responsable de la clasificación, decisiones de transmisión, encolamiento, y registro de paquetes. Cada SIP tiene 2 motores de transmisión, una para ingreso y otro para egreso, permitiendo implementar políticas de calidad de servicio en el tráfico de entrada, independientemente de las aplicadas al de salida.
- Un módulo de interfaz de capaz física (PLIM) con sobre suscripción inteligente que alberga hasta cuatro SPAs. Cada SPA tiene una interfaz dedicada (2.5 a 10 Gbps) hacia el controlador SPA. Un algoritmo para asignación justa de ancho de banda comparte el ancho de banda disponible y en exceso entre los SPAs (los SPAs sobre suscritos no causan pérdida de paquetes sobre los SPAs no sobre suscritos, y cualquier ancho de banda no utilizado por un SPA es utilizado por el otro). El SIP soporta tres tipos de SPAs: SPAs de interfaz específica, SPAs de servicio específico y SPAs multiservicio.
    - SPAs de interfaz específica: Cada uno de estos SPAs está optimizado para un medio y una velocidad como Fast Ethernet, 1 Gbps, y 10 Gbps, Ethernet.
    - SPAs de servicio específico: Cada uno de estos SPAs ofrece procesamiento de servicios adicional al entregado por el motor principal para ofrecer servicios específicos como IP *Security* (IPsec).
- Un controlador de SPAs que realiza la adaptación del tráfico fluye entre las interfaces SPA y el motor de transmisión de capa 3[10]. El controlador de SPAs provee puede priorizar el tráfico desde el SPA hacia el motor, para ofrecer calidad de servicio (QoS) inclusive en configuraciones de sobre suscripción.

[10] Realiza las funciones de búsqueda, reescritura, almacenamiento de capa 3 en los paquetes.

2.5.2.3 SPA de 1 Puerto de 10 Gigabit Ethernet [24]

El Cisco 1-Port 10-GE SPA es utilizado en plataformas de enrutamiento de alto rendimiento. Las interfaces de 10 Gigabit Ethernet son comúnmente utilizadas para interconectar routers u otros dispositivos. El Cisco 1-Port 10-GE SPA mostrado en la figura 2.16 está basado en el estándar IEEE 802.3ae para compatibilidad e interoperabilidad.

Figura 2.16: Cisco 1-Port 10-GE SPA con XFP Ópticos [24]

2.5.2.4 SPAs Cisco de 2-, 5-, 8-, y 10-Puertos Gigabit Ethernet, Versión 2 [25]

El Cisco SPA/SIP permite el despliegue de diferentes interfaces (paquetes sobre SONET/SDH, ATM, Ethernet, etc.) en la misma interfaz del procesador. También proporciona una alta densidad de interfaces SFP con alta flexibilidad como se indica en la figura 2.17.

Figura 2.17: SPA Cisco de 10-Puertos Gigabit Ethernet [25]

2.5.3 CHASIS DEL ROUTER CISCO 7609-S [13] [36] [49]

El router Cisco 7609-S, se trata de un equipo de red de alto desempeño para ser implementado en el borde de una red, donde el rendimiento, servicios IP, redundancia, y recuperación frente a fallas son elementos críticos. Esto permite a los proveedores de servicios *Carrier* Ethernet implementar una infraestructura avanzada de red la cual soporte un amplio rango de aplicaciones de video IP y servicios triples (voz, video, y datos) tanto para mercados residenciales como de

negocios. El Cisco 7609-S cuyo chasis se indica en la figura 2.18 permite implementar soluciones de red avanzadas para entornos WAN y MAN en ambientes de alta demanda con tráfico elevado.

Figura 2.18: Chasis Cisco 7609-S [36]

El router Cisco 7609-S de 9 ranuras está diseñado para múltiples aplicaciones como: un agregador WAN de alta velocidad, un dispositivo para *peering*[11], un agregador para servicios residenciales de banda ancha, o como un dispositivo para agregación Metro Ethernet y manejo de *uplinks*, el Cisco 7609-S cumple con los requisitos de redundancia, alta disponibilidad y una alta densidad de *rack*. En el POP[12] (*point-of-presence*) del proveedor de Servicios o en el borde de la red metropolitana.

Posee una tasa de transmisión de hasta 400-Mbps distribuidos y un rendimiento total de 720-Gbps, proporciona desempeño y fiabilidad con opciones de procesadores de enrutamiento y fuentes de poder redundantes.

El chasis del router Cisco 7609-S entrega una numerosa cantidad de mejoras al diseño, que incluyen, mejoras a los mecanismos de recuperación de fallas en el

[11] Interconexión voluntaria entre dos redes en internet administrativamente independientes
[12] Es un punto de demarcación artificial o interfaz de punto entre las entidades de comunicación.

hardware, que vinculada a la adecuada imagen de *software* del Cisco IOS® puede alcanzar recuperación de fallas en 100 ms.

Cisco 7600 provee un amplio número de opciones para escalar la conectividad WAN desde DS-0 hasta OC-192 y la conectividad LAN desde Ethernet de 10 Mbps hasta conexiones de 10 Gigabit Ethernet.

El Cisco 7609-S incorpora muchos requerimientos de proveedores de servicios y empresas tipo *carrier*. Las tarjetas en línea son montadas de manera vertical para obtener un enfriamiento eficiente con un flujo de aire que va desde adelante hacia atrás. Lo referente a alta disponibilidad es una faceta inherente en la forma en la que los módulos de las fuentes de poder y los ventiladores han sido diseñados.

La flexibilidad del router Cisco 7609-S es ideal para direccionar aplicaciones que requieren un alto desempeño como son:

- Equipo Final de Clientes Locales (CPE)
- Líneas Dedicadas
- IP/Multiprotocol Label Switching (MPLS)
- Acceso Metro Ethernet
- Agregación WAN Empresarial
- Agregación de Redes de Acceso de Radio Móvil (RAN)
- Agregación de suscriptores residenciales.

2.5.3.1 Procesador de Enrutamiento/Conmutación 720 para la Serie Cisco 7600 [37]

El procesador de enrutamiento/conmutación 720 para los Cisco 7600 (RSP 720) está específicamente diseñado para entregar alta escalabilidad, desempeño, y una convergencia rápida requeridas para los servicios actuales y futuros de voz, video, datos y movilidad (servicios cuádruples). El RSP 720 para Cisco 7600 ofrece una verdadera convergencia de servicios sin añadir tiempos por demoras en el procesamiento por falta de CPU, dependiendo en gran medida de los tiempos de convergencia propios de los protocolos que esté utilizando el router, permitiendo manejar una amplia gama de aplicaciones sobre un rango de medios de acceso utilizando una única plataforma.

El RSP 720 para los Cisco 7600 utiliza la misma conmutación de fábrica de alto desempeño de 720-Gbps que utiliza la tarjeta supervisora 720 de los Cisco Catalyst 6500 y la combina con un nuevo y revisado motor de transmisión basado en un Circuito Integrado para Aplicaciones Específicas. En la figura 2.19 se indica la tarjeta procesadora de enrutamiento 720.

Figura 2.19: Procesador de Enrutamiento/Conmutación 720 para la Serie Cisco 7600 [37]

Este módulo entrega una capacidad de conmutación de 40 Gbps por ranura, soportando 4 puertos de 10 Gigabit Ethernet y tarjetas con una densidad de 48 puertos 10/100/1000. Con transmisiones habilitadas en hardware para IPv4, Unicast y Multicast de IPv6, y MPLS, el RSP 720 puede entregar transmisión centralizada de alta velocidad con gran variedad de características de procesamiento de paquetes como listas de control de acceso (ACLs), calidad de servicio (QoS), VPNs MPLS, y más. Combinando el RSP 720 para los Cisco 7600 con tarjetas de transmisión distribuida (DFCs), el desempeño del sistema total puede alcanzar hasta los 400 Mpps.

El RSP 720 para los Cisco 7600 ofrece una amplia gama de características para IP manejadas en hardware para aplicaciones como agregación de suscriptores, transmisión IP, VPNs MPLS de Capa 2 y Capa 3, y Ethernet sobre MPLS (EoMPLS) con calidad de servicio (QoS) y funcionalidades de seguridad.

El RSP 720 para los Cisco 7600 viene integrado con 2 nuevas tarjetas hijas:

Tarjeta para características de políticas (*Policy Feature Card* / PFC-3C o PFC-3CXL). Desempeña tareas de transmisión con un desempeño constante para capa 2 y capa 3, inclusive con características que requieren una alta carga de

procesamiento como ACLs, QoS, GRE *(Generic routing encapsulation)*, o NAT *(Network Address Translation)*; la PFC realiza las siguientes funciones:

- Realiza transmisión de capa 2 y capa 3
- Refuerza las funciones de ACLs
- Realiza políticas y marcado de QoS
- Recolecta estadística de NetFlow
- Ofrece Control Plane Policing (CoPP)

Tarjeta *Multilayer Switch Feature Card (MSFC4)*, corre protocolos de capa 2 y capa 3 o realiza todas las funciones de control de plano.

2.5.3.2 Tarjetas Ethernet Services Plus de 20 y 40 Gbps para la Serie Cisco 7600 [38]

Las tarjetas *Ethernet Services* Plus de 40 Gbps (ES+40) usan un diseño extensible que permite priorización de servicios para voz, video, datos y servicios de movilidad inalámbrica. Proveedores de servicios y clientes de empresas pueden beneficiarse de las mejoras económicas, de densidad, en las características avanzadas de *Carrier Ethernet*, y el alto desempeño de la tarjeta de configuración fija ES+40. Con la misma arquitectura y características, las tarjetas *Ethernet Services Plus* 20 Gbps (ES+20) para la Serie Cisco 7600 están diseñadas para redes que requieren una baja densidad de interfaces. En la figura 2.20 se indica una tarjeta ES+ con 20 puertos Ethernet de 1 Gbps.

Figura 2.20: Tarjeta de línea ES+ Series 20 puertos GE [38]

Los procesadores de interfaz programable de las tarjetas ES Plus para los Cisco 7600 protegen las inversiones de la red y reducen el costo total de propiedad (TCO). El diseño incrementa las opciones de conectividad y ofrece un superior

servicios de inteligencia a través de los procesadores de interfaz programable operando a velocidad de línea.

Diseñados para *Carrier Ethernet*, *IP/Multiprotocol Label Switching provider edge (MPLS PE)*, movilidad inalámbrica, y aplicaciones empresariales WAN y MAN, la tarjeta Ethernet *Services* Plus de 40 Gbps (7600-ES+40) para los Cisco 7600 soporta hasta 40 Gbps de ancho de banda con 40 puertos Gigabit Ethernet o 4 puertos de 10 Gigabit Ethernet. En la figura 2.21 se indica una tarjeta de línea ES+ que tiene dos puertos Ethernet de 10Gbps.

Figura 2.21: Tarjetas de línea ES+ Series 2-Port 10GE [38]

Con la misma arquitectura y características, la tarjeta Ethernet Services Plus 20 Gbps para los Cisco 7600 ofrecen 20 Gbps de ancho de banda con 20 puertos Gigabit Ethernet o 2 puertos de 10 Gigabit Ethernet. Las tarjetas ofrecen Calidad de Servicios (QoS) jerárquico, VLANs de significado local, aprendizaje de MACs distribuidas, y hasta 16000 instancias de servicios Ethernet por tarjeta.

Las tarjetas ES Plus para los Cisco 7600 proveen la habilidad única para combinar servicios tanto de capa 2 como de capa 3 en la misma tarjeta. La combinación de conmutación nativa de Ethernet capa 2, *bridging*, servicios de LANs privadas virtuales (VPLS), Ethernet sobre MPLS (EoMPLS), y enrutamiento de capa 3 para IP/MPLS.

La arquitectura innovadora de estos dispositivos líderes en la industria, las tarjetas *premium* ES Plus, se ha diseñado para entregar características de alto nivel a bajo costo, combinando tanto Circuitos Integrados para Aplicaciones Especificas

(ASIC) y tecnologías para procesadores de red para una combinación óptima de desempeño y flexibilidad.

La tarjeta ES Plus para el Cisco 7600 provee transmisión distribuida mediante el uso de tecnologías ASIC comprobadas en el proceso de transmisión (enrutamiento, conmutación, NetFlow y listas de control de acceso (ACL)), así como para funciones de encolamiento y moldeamiento para entregar el máximo desempeño para estas características fundacionales. Adicionalmente, 4 (para las tarjetas ES+40) o 2 (para las tarjetas ES+20) procesadores de red programables están incluidas en el plano de transmisión para facilitar flexibilidad y crecimiento a futuro.

2.5.4 ROUTERS PARA AGREGACIÓN DE SERVICIOS CISCO ASR 1000[26]

La Serie Cisco ASR 1000 *(Aggregation Services Ruteadores)* es una plataforma de nueva generación diseñada para ofrecer una gran variedad de servicios con un excelente desempeño (5 a 20 Gbps) y alta flexibilidad. Construida como una plataforma modular con una clara separación entre el Plano de Control y el Plano de *Forwarding*, posee una avanzada arquitectura de software (IOS-XE) que le otorga una alta escalabilidad y amplia variedad de servicios. La Serie ASR-1000 está constituida por:

2.5.4.1 Chasis de 2, 4 y 6 RUs (ASR1002, ASR1004 y ASR1006)

Que comparte la misma arquitectura y componentes funcionales. De manera similar, todos los chasis admiten Fuentes de Poder duales, ya sea AC o DC. En la figura 2.22 se indica los diferentes chasis para los routers Cisco ASR.

Figura 2.22: Familia de routers ASR [26]

2.5.4.2 *Route Processor* (RP) [27]

Disponible en dos versiones (RP1 y RP2, disponible para chasis de 4 y 6 slots) y donde reside una poderosa CPU con componentes de software tales como el IOS donde reside la inteligencia y control del equipo. El Chasis de 2 slots posee un RP1 integrado, en tanto el resto de los chasis posee slots especializados para alojar un único (ASR1004) o dual (ASR1006) RP1 o RP2. En la figura 2.23 se observa un *route procesor* para los sistemas ASR

Figura 2.23: *Route procesor* [27]

2.5.4.3 *Embedded Services Processor* (ESP) [28]

Disponible en versiones de 5, 10 y 20 Gbps, es donde reside un procesador especializado denominado QFP (*Quantum Flow Processor*) que implementa la totalidad de los servicios de *forwarding* de paquetes (*Data Plane*) y está encargado de realizar la inspección y disposición de la totalidad de los servicios IPv4 (unicast y multicast), IPv6 y MPLS en hardware a través de un arreglo procesadores que trabajan en paralelo. En la figura 2.24 se indica un ESP.

Figura 2.24: *Embedded Services Processor* ASR1000 [28]

En el ESP también reside un coprocesador de encriptación que permite realizar esta tarea con excelente desempeño (1.8 a 8 Gbps). Tanto el chasis ASR1002

(ESP5 o ESP10) como ASR1004 (ESP10 o ESP20) cuentan con un slot especializado para el ESP, en tanto el ASR1006 acepta ESPs duales (ESP10 o ESP20) para alta disponibilidad.

2.5.4.4 *SPA Interface Processor* (SIP) [29]

También llamado *Line Card*, es el responsable de alojar las diferentes variedades de interfaces en forma flexible en hasta 4 SPAs *(Service Port Adaptor)* por SIP (un SIP por slot). La actual generación de SIP es de 10 Gbps. El Chasis de ASR1002 posee un SIP (indicado en la figura 2.25) integrado que incorpora 4 interfaces GE y permite alojar hasta 3 SPAs, en tanto los chasis ASR1004 y ASR1006 permiten alojar hasta 2 y 3 SIPs, que permiten alojar hasta 8 y 12 SPAs respectivamente.

Figura 2.25: *SPA Interface Processor* ASR1000 [29]

La modularidad y uso de SPAs permite acomodar en la plataforma ASR-1000 un gran variedad de conectividad entre 64 Kbps a 10 Gbps, incluida Ethernet (4 u 8 port FE, 2, 5, 8 o 10 port GE y 1-port 10GE), y PoS (2, 4 o 8 port STM-1, 1, 2, 4 o 8 port STM-4 , 1, 2 o 4-port STM-16 y 1-port STM-64). En la figura 2.26 se indica un conjunto de SPAs con diferentes densidades de puertos.

Figura 2.26: SPA ASR 1000 [29]

2.5.5 CONMUTADOR ETHERNET DE LA SERIE CISCO ME 6500 [39]

El conmutador Ethernet de la serie Cisco® ME 6500 es un equipo de configuración fija de siguiente generación. Basado en la tecnología Cisco Catalyst 6500, el Cisco ME 6500 entrega de manera efectiva los requerimientos de desempeño, fiabilidad, y QoS que las implementaciones de borde WAN requieren.

El Cisco ME 6500 extiende las más avanzadas características de MPLS *(Multiprotocol Label Switching*), calidad de servicio (QoS), multicast, e IPv6 hacia el acceso Ethernet y las redes de agregación, habilitando el acceso Gigabit Ethernet con características de escalabilidad y amplios servicios tanto para implementaciones de fibra como de cobre.

El conmutador Ethernet de la Serie Cisco ME 6500 es un equipo de alto desempeño, lleno de características, y fiabilidad que viene equipado de manera estándar con las tarjetas PFC3C *(Policy Feature Card 3C) y MSFC2A (Multilayer Switch Feature Card 2A).*

El Cisco ME 6524 está disponible en dos configuraciones:

24 *Downlinks* tipo SFP *(Small Form-Factor Pluggable)* Gigabit Ethernet y 8 uplinks con SFPs Gigabit Ethernet, con Fuentes de poder redundantes (figura 2.27).

Figura 2.27: Cisco ME 6524 Puertos Ópticos [39]

24 *Downlinks* Ethernet 10/100/1000 y 8 uplinks SFP Gigabit Ethernet, con Fuentes de poder redundantes (figura 2.28).

Figura 2.28: Cisco ME 6524 Puertos Eléctricos [39]

El Cisco ME 6524 ofrece:

- Hasta 32 puertos Gigabit Ethernet, el Cisco ME 6524 puede agregar múltiples clientes que requieran conectividad Gigabit Ethernet. Las interfaces de uplink ofrecen opciones de conectividad flexible acomodando un amplio rango de SFPs ópticos, incluyendo CWDM *(coarse wavelength-division multiplexing)* y DWDM.
- Opciones de implementaciones flexibles de red: El conmutador presenta servicios altamente escalables de Capa 2 con características como túneles inteligentes 802.1Q, L2TP *(Layer 2 Protocol Tunneling)*, y translaciones de VLANs. La tarjeta PFC3C permite habilitar tecnologías MPLS en hardware para ofrecer VPNs MPLS y Ethernet sobre MPLS (EoMPLS). Para ofertas de servicios que se enfrenten a una creciente demanda de espacio de direcciones IP, protocolos habilitados en hardware para IPv6 proveen una entrega de servicios IP de alto desempeño y escalables de fin a fin.
- Ofrece un CPU de alto desempeño para la convergencia y estabilidad de protocolos de Capa 2 y Capa 3. El equipo presenta conmutación escalable de Capa 2, funcionalidades de MPLS y enrutamiento IP en hardware sin tener impacto en el desempeño.
- Disponibilidad de servicios incrementada: El Cisco ME 6524 ayuda a asegurar el tiempo que la red y servicios están arriba con su soporte de protocolos Cisco EtherChannel, protocolos de convergencia rápida como IEEE 802.1w/802.1s y Flexlink, y protocolos de balanceo de carga de Gateway.
- Seguridad Integrada: El Cisco ME 6524 ofrece un complete conjunto de características de seguridad para mitigar los ataques de negación de servicios (DoS), para restringir el acceso a la red, y para salvaguardar los recursos de la red. Mediante el uso de listas de control de acceso (ACLs) basadas en puertos y en VLANs se puede restringir tráfico no deseado basado tanto en los usuarios y en el tipo de tráfico; limitadores de tasa de CPU y políticas del plano de control (CoPP) limitan la cantidad de tráfico que entra a la red; la Seguridad de Puertos (*Port Security*) limita el número de direcciones MAC que pueden ser aprendidas; DHCP *Snooping* y la

inspección dinámica de ARPs previene de amenazas al servidor DHCP; las rutas por defecto; o ataques de suplantación de dirección. Estas características de seguridad integradas son habilitadas en hardware de tal manera que pueden ser habilitadas de forma concurrente sin afectar el desempeño del sistema mientras los niveles de tráfico aumentan.

- Las VPNs de Capa 2 pueden ser ofrecidas en una infraestructura puramente de capa 2. Mediante la habilitación de características como túneles 802.1Q, L2TP *(Layer 2 Protocol Tunneling)*, y traslación de VLANs, el Cisco ME 6524 permite al cliente segmentar y transportar de manera transparente el tráfico de los usuarios.
- De forma alternativa, las VPNs de Capa 2 pueden ser ofrecidas a través de una red Ethernet sobre MPLS. Esta tecnología ofrece un mecanismo de túneles de capa 2 sobre redes MPLS de capa 3, así usando los protocolos de convergencia de red de capa 3 se evita la necesidad de usar STP (Spanning Tree Protocol).
- Las VPNs de Capa 3, con frecuencia llamadas VPNs MPLS, son servicios multipunto de capa 3. La tarjeta compleja PFC3C en el Cisco ME 6524 habilita las funcionalidades de MPLS en hardware y provee capacidades de QoS y fiabilidad como marcado de bits MPLS EXP (MPLS Experimental), Ingeniería de Tráfico MPLS (MPLS TE), y Enrutamiento Rápido de MPLS (MPLS FRR).

2.5.6 CISCO 2800 [30]

Estos routers ofrecen una variedad de características entre las que incluye:

- Seguridad integrada, como firewall, cifrado y protección contra piratas informáticos.
- Conector de suministro de energía redundante integrado en la mayoría de los modelos para una mayor protección.
- Integración con Cisco *Unified Communications Manager Express* para soporte de procesamiento de llamadas de hasta 96 usuarios.
- Integración con Cisco *Survivable Remote Site Telephony (SRST)* para mantener los servicios de voz locales en caso de pérdida de la conexión.

- Mayor confiabilidad y flexibilidad que le permite dar prioridad al tráfico de voz o al intercambio de datos para que la entrega de información se adapte a las necesidades de su empresa.
- Soporte para conexiones de red privada virtual para conectar socio de negocios y oficinas remotas.
- Soporte para cobertura LAN inalámbrica en toda la oficina con una seguridad robusta y capacidades de acceso de invitado, que soportan todos los estándares inalámbricos IEEE 802.11a/b/g/n.
- Diferentes opciones de conectividad de banda ancha y red.
- Opciones de suministro de energía a los dispositivos de red a través de su conexión Ethernet *(Power Over Ethernet)* para reducir los costos de cableado.

2.6 CALIDAD DE SERVICIO QoS

2.6.1 SERVICIOS INTEGRADOS [3] [4] [11]

IntServ modifica el modelo básico de IP para ofrecer QoS extremo a extremo mediante una señalización extremo a extremo, mantenimiento de estado y un control de admisión en cada elemento de la red. Esta arquitectura fue desarrollada por la IETF y especifica un número de clases de servicios diseñados para cumplir con los requerimientos de diferentes tipos de aplicaciones, a pesar de especificar varios protocolos de señalización se utiliza el protocolo *resource reservation protocol (RSVP)* el cual reserva recursos para las diferentes peticiones de QoS. IntServ define un perfil de tráfico llamada Tspec, esta especifica el tipo de tráfico que ingresa en la red, en caso de que el tráfico no cumpla con esta especificación los paquetes se descartan.

Otras especificación definida es Rspec "*Request SPECification*" que se encarga de realizar una petición con los requerimientos de un nivel de QoS y reserva los recursos de la red, se verificar que existan los recursos de red necesarios para cumplir con la solicitud de QoS, caso contrario la petición es rechazada, para la implementación de esta arquitectura los elementos de red necesitan realizar una

clasificación de los paquetes de manera que se pueda conocer los diferentes niveles de QoS que requieren y dar el tratamiento adecuado a los paquetes.

2.6.1.1 Clases de Servicio de IntServ [6] [11]

Se definen tres clases de servicio para las diferentes aplicaciones:

Servicio garantizado: establece límites estrictos en el retardo extremo a extremo y asegura un ancho de banda para el tráfico que cumple con las especificaciones reservadas, este tipo de servicio requiere que cada flujo de datos use un encolamiento separado por lo que da como resultado una baja utilización de la red.

Carga controlada: este tipo de servicio provee un servicio superior al que se obtiene con el del mejor esfuerzo, traduciéndose en un bajo retardo en redes con carga moderada, es posible proporcionar una calidad de servicio adecuada para cada flujo de datos en la red siempre que se señale con RSVP y los recursos estén disponibles.

Servicio del mejor esfuerzo: este es el servicio tradicional utilizado por IP para transportar los datos sin ninguna garantía.

2.6.1.2 *Resource Reservation Protocol* (RSVP) [3] [6] [11]

Es un protocolo de señalización que permite a las aplicaciones informar los requerimientos de QoS a la red, la misma que responde con una respuesta de éxito o falla ante una petición. Este protocolo transporta información como la dirección IP de origen y el número de puerto que permiten identificar un flujo de datos, también transporta información adicional como el Tspec, Rspec y la clase de servicio deseado. Esta información se envía desde la aplicación de origen hasta el destino, pasando por cada elemento de la red.

RSVP utiliza dos tipos de mensajes para llevar la información: PATH y RESV. Los mensajes de PATH se envían desde el nodo origen que genera la petición, en el mensaje se incluye el Tspecs e información de clasificación provista por el origen.

Cuando se recibe un mensaje PATH se responde un mensaje RESV y se identifica la sesión para la cual se realizó la reservación.

Hay que tomar en cuenta que la reservación de RSVP es unidireccional, en caso de que se requiera un flujo bidireccional se debe enviar mensajes PATH y RESV del destino al origen de manera que se pueda establecer un flujo en la dirección contraria, el receptor pasa a ser el origen y viceversa como se observa en la figura 2.29.

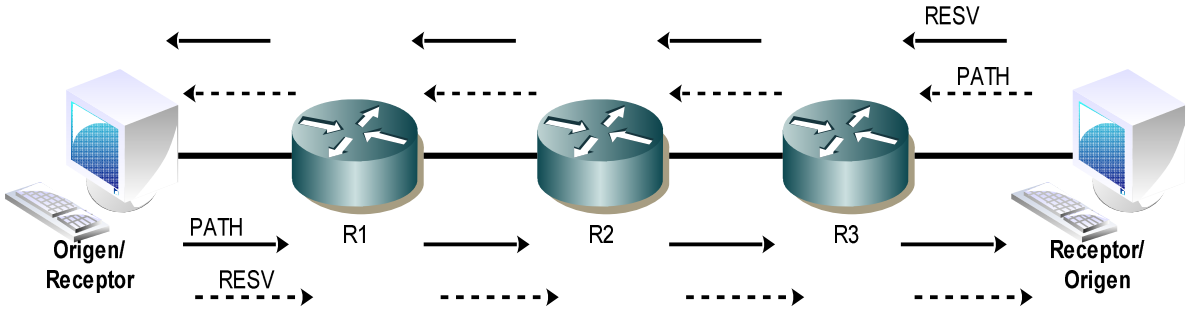


Figura 2.29: Gráfico establecimiento QoS IntServ bidireccional. [3]

Al establecerse una reservación los routers identifican los paquetes que son parte de esta basándose en cinco campos: IP de origen, IP de destino, puerto de origen, puerto de destino y el número de protocolo, al conjunto de paquetes identificados de esta manera se los llama reserva de flujo. Los paquetes en una reserva de flujo son vigilados para que no sobrepasen el perfil del Tspec.

Si bien RSVP fue diseñado para la reserva de micro flujos uno por cada aplicación, y en teoría se puede reservar QoS para cada una, en la práctica esto se ve limitado por los recursos disponibles y el hecho que la información de la reservación debe ser mantenida por cada elemento de la red, todo esto resulta en un problema de escalabilidad con cientos o miles de flujos en una red, aumentando la necesidad de memoria para soportar un mayor número de reservas.

2.6.1.3 Implementación de IntServ en MPLS [3] [4]

Considerando que RSVP puede hacer reservaciones para tráfico agregado, esta es la forma básica en la que MPLS implementa RSVP donde los paquetes que

pertenecen a un flujo de reserva pueden ser considerados parte de una FEC, está a su vez se asocian con las etiquetas y se distribuyen usado LDP o las extensiones de los protocolos, esta es la forma en que los LSR habilitan QoS dándose como resultado una asociación entre las etiquetas y los flujos RSVP.

Para establecer la sesión a través de una red MPLS se envía un mensaje RSVP PATH, el host que los recibe responde con un mensaje RSVP RESV, este mensaje se envía al LER que está conectado el host, este escoge una etiqueta del pool de etiquetas libres, la añade a la LFIB en el campo etiqueta entrante y envía un mensaje RESV con un objeto etiqueta y el valor previamente seleccionado al LSR dentro de la red MPLS.

Esto crea una entrada en la LFIB y coloca el valor que recibió en el campo etiqueta de salida, selecciona una etiqueta del pool de etiquetas libres, la asigna a la entrada LFIB como etiqueta de entrada y envía un mensaje RESV al siguiente LSR con el valor de esta etiqueta.

Cada LSR repetirá este proceso hasta que se alcance el LER al que está conectado el host que originó la petición, el LER usará el valor de la etiqueta que reciba del LSR para enviar los paquetes que procedan del host, con esto se establece un LSP a lo largo de la ruta RSVP y cada router puede asociar los recursos de QoS necesarios con el LSP, este procedimiento se observa en la figura 2.30.

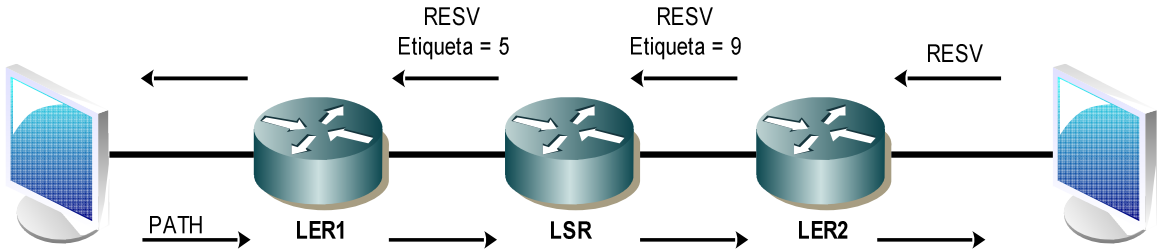


Figura 2.30: Asignación de etiquetas Int Serv. [3]

Cuando se usa RSVP en MPLS no es necesario que los LSR revisen los encabezados del paquete pues al recibirlo se realiza una búsqueda en su tabla LFIB y basándose en el valor de la etiqueta se reconocen todos los parámetros necesarios para dar el tratamiento adecuado de QoS.

2.6.1.3.1 *LSP de Ancho de Banda Garantizado*

Las extensiones de RSVP puede ser utilizadas para distribuir etiquetas como parte del proceso de reserva de recursos y de esta manera establecer un LSP con recursos reservados el cual es conocido como LSP de ancho de banda garantizado. Si se establece una reservación a lo largo de un camino entre el LER de ingreso y el de egreso el primero consulta su base de datos de estado de enlace y selecciona un camino que cumpla con las restricciones de ancho de banda en todos los enlaces, además debe tener un adecuado espacio de buffers de manera que permita admitir las ráfagas de tráfico. Para esto puede insertar un objeto de ruta explicita en el mensaje asegurando que el LSP se establezca a lo largo de la ruta seleccionada.

2.6.2 PRECEDENCIA IP [3] [5] [6]

La arquitectura IntServ que usa un RSVP por flujo no es escalable y es compleja de implementar. La precedencia IP definida por IETF ha simplificado la manera en que se da QoS a IP al definir un modelo agregado, en el se clasifican varios flujos en un conjunto agregado de clases, y se provee un QoS apropiado para los flujos clasificados.

Los paquetes se clasifican a su ingreso a la red (en los nodos de borde) en una de las 8 clases definidas. Para identificar las clases se usan tres bits del campo ToS (Tipo de servicio) de la cabecera IP, estos tres bits conocidos como de precedencia y se usan para clasificar los paquetes en el borde de la red en una de las ocho clases posibles. Además cada paquete puede ser marcado para recibir uno de los niveles de demora, rendimiento y fiabilidad. En la figura 2.31 se indica los campos definidos en precedencia IP.

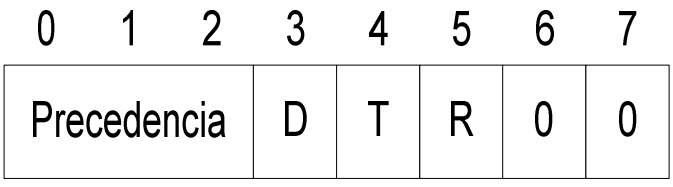


Figura 2.31: Definición campo ToS para precedencia IP

Los campos de la cabecera son:

- Bits 0-2: Prioridad.
- Bit 3 (D): 0 = Demora Normal; 1 = Demora Alta
- Bit 4 (T): 0 = Rendimiento Normal 1 = Alto Rendimineto
- Bit 5 (R): 0 = Fiabilidad Normal 1 = Alta Fiabilidad
- Bits 6-7: Reservados para uso futuro.

Los paquetes con una menor precedencia son descartados para favorecer a aquellos que tienen una mayor precedencia en caso de que se presente congestión en la red, una vez que los paquetes son marcados con los bits adecuados de pretendencia cualquier nodo a lo largo del camino del paquete conoce el nivel de prioridad y puede aplicar un envió preferencial para los paquetes que tienen una prioridad superior, la precedencia IP permite una especificación de prioridad relativa pues no da la opción de preferencia de descarte para paquetes de una misma clase.

Como se indica en la tabla 2.5, el uso de tres bits restringe el número de posibilidades a ocho, de estas dos se usan para el control de red y de encaminamiento, lo que reduce el número disponibles para producción a 6.

Número	Nombre
0	Rutina
1	Prioridad
2	Inmediato
3	Urgente
4	Muy urgente
5	Critico
6	Control De Encaminamiento
7	Control De Red

Tabla 2.5- Clases definidas por precedencia IP

2.6.3 MECANISMOS DE QOS [4] [32]

El modelo Intserv, Presedencia IP y DiffServ define únicamente el uso de campos y un tratamiento básico de los paquetes dentro de la red. Esto se debe a que

existen una variedad de colas, políticas, métricas y técnicas de catalogación de tráfico que pueden usarse para afectar y condicionar el tráfico, dentro de los algoritmos que se pueden poner en uso en la red de CNT se tiene:

2.6.3.1 *Traffic Policing* [4] [32] [43] [44]

Traffic policing es un mecanismo que permite controlar la tasa de envió o recepción en una interfaz para los diferentes niveles de servicio o SLAs que se tengan.

Committed Access Rate (CAR) se puede usar para condicionar el tráfico y proporcionar el comportamiento para las diferentes clases, se usa tanto en los límites como en el núcleo de la red.

Los paquetes son medidos y en base a esto se pueden tomar diferentes acciones dependiendo si el paquete está de acuerdo, viola o excede la tasa promedio configurada para esto se usa la ráfaga comprometida (committed burst Bc) y la ráfaga de exceso (excess burst Be).

Si el tráfico entregado al nodo se encuentra igual o por debajo del Bc se encuentra dentro de la tasa de acceso configurado, si el tráfico está entre Bc y Be es tráfico en exceso y caso de que el tráfico es más alto que Bc + Be este se descarta. Un paquete puede ser transmitido, descartado o remarcado.

2.6.3.1.1 *Committed Access Rate (CAR)* [44]

Este método implementa funciones que permiten limitar el tráfico entrante en un dispositivo, adicionalmente permite realizar un análisis de los paquetes para realizar una adecuada clasificación de los mismos.

Las características de limitación de tráfico de CAR se encargan vigilar el ancho de banda de acceso a la red, asegurando que el tráfico que se encuentra de dentro de los parámetros sea enviado, en cambio el tráfico que no cumpla con estos parámetros se descarta o se transmitirte con una prioridad más baja. Las funciones de limitación de CAR son las siguientes:

Permite controlar la máxima tasa de tráfico enviado o recibido por una red,

Permite realizar agregación o granularidad de capa 3 para limitar el ancho de banda de ingreso o egreso, también específica las políticas de manejo de tráfico en caso de que este cumpla o no los límites de velocidad especificados.

El limitador de ancho de banda agregado coincide con todos los paquetes en una interfaz o subinterfaz, en cambio el limitador de ancho de banda granular coincide con un tipo particular de tráfico para lo que se basa en la precedencia, la dirección MAC o cualquier otro parámetro. El método CAR a menudo se configura en los bordes de la red de manera que permita limitar el tráfico entrante y el saliente.

En su Funcionamiento CAR examina el tráfico recibido por un interfaz o un conjunto de criterios de selección de tráfico como la dirección IP, MAC, Precedencia IP, etc, luego compara la tasa de tráfico con lo configurado en *token bucket* y toma una acción basada en el resultado.

2.6.3.1.2 *Token Bucket* [43]

Es una definición de tasa de transferencia la cual tiene tres componentes: un tamaño de ráfaga *Bc (committed burst)*, una tasa de información media comprometida *CIR (committed information rate)* y un intervalo de tiempo Tc, la tasa media se expresa en bps y se relaciona con los otros dos parámetros de la siguiente forma:

$$CIR = \frac{Bc}{Tc}$$

Committed information rate (CIR): También conocido como tasa media especifica la cantidad de datos promedio que puede ser transmitido en una unidad de tiempo.

Committed burst (Cb): También conocida como tamaño de ráfaga, se especifica en bits o bytes y define el volumen de tráfico que puede ser enviado en una unidad de tiempo asegurando que no se creen problemas de administración.

Intervalo de tiempo (Tc): también llamado intervalo de medición, este especifica intervalo de tiempo en segundos para la ráfaga.

Para su funcionamiento los *tokens* son colocados en el colector de una capacidad específica a una tasa dada, en caso de llenar esta capacidad los *tokens* que lleguen serán descartados.

Cada *token* es un permiso para que la fuente envié una cierta cantidad de bits a la red, cuando un paquete es enviado el dispositivo regulador retira del colector un número de *tokens* que represente el tamaño del paquete. En caso de que no exista una cantidad adecuada de *tokens* para enviar un paquete se puede esperar hasta que exista un número adecuado de *tokens* o se puede descartar el paquete.

Adicionalmente se puede hacer extensivo este algoritmo para el Be con comportamiento igual al descrito, el Be será mayor al Bc y se tomaras ciertas medidas como el enviarlo a la red con una prioridad menor, el Be está definido para el mismo intervalo de tiempo Tc.

2.6.3.2 *Traffic Shaping* [4] [35]

Es un mecanismo que permite controlar el tráfico que sale de una interfaz con la finalidad de controlar su flujo de manera que coincida con la velocidad de la interfaz remota, así se asegura que el tráfico este conforme con las políticas contratadas.

Es por esta razón que el tráfico que cumple con un determinado perfil puede considerarse una forma de cumplir con los requerimientos del cliente, eliminando los cuellos de botella en topologías donde la tasa de transmisión sufre variaciones.

Una de las razones principales por la que se usa este método es para controlar el acceso al ancho de banda disponible, asegurando que el tráfico este de acuerdo con la políticas establecidas, también permite regular el flujo de tráfico para prevenir la formación de congestión por lo que previene la pérdida de paquetes.

2.6.3.2.1 *Generic Traffic Shaping (GTS)* [45]

Es un mecanismo que nos permite realizar *traffic shaping*, reduce el flujo del tráfico de salida previniendo un evento de congestión restringiendo la tasa de bits de salida para lo que usa *token bucket*. Se aplica a cada interfaz y puede usar una lista de acceso para controlar el tráfico en esta interfaz, puede trabajar sobre una variedad de tecnologías de cada enlace como ATM, Frame Relay, Ethernet, etc.

2.6.3.3 Mecanismo para el Manejo de Congestión [3] [6] [11] [32]

Las funcionalidades de manejo de la congestión controlan la congestión del tráfico cuanto esto ocurre en un link. Una manera de que los elementos de red puedan manejar un overflow de tráfico utilizando una buena técnica de encolado para luego poder priorizarlos en la salida del link.

2.6.3.3.1 *Low Latency Queuing (LLQ)*

El encolamiento de baja latencia es apropiado para el tráfico de VoIP y para video conferencia, consta de varias colas de prioridad personalizada basadas en los diferentes tipos de tráfico, se caracteriza por disponer de una cola que tiene prioridad absoluta sobre las demás.

La cola de prioridad absoluta será la primera en ser atendida, si esta cola no tiene paquetes se procede a atender a las demás colas basándose en su prioridad, para evitar que las demás colas no transmitan se define un limite de ancho de banda para la cola de mayor prioridad

2.6.3.3.2 *Class-Based Weighted Fair Queueing (CBWFQ)*

Es un método de encolamiento que permite la creación de clases que son definidas por el usuario, el tráfico perteneciente a las clases se pueden seleccionar en base a listas de acceso, el valor del campo DSCP o en base a la interfaz por al que ingresan los paquetes.

Se asigna una cola y una ancho de banda para cada tipo de tráfico, en base al criterio de selección es posible determinar el tipo de tratamiento que se dará a cada paquete, en el caso de que una clase no utilice una porción del ancho de banda asignado otras podrán usarlo, permite configurar el ancho de banda y el número máximo de paquetes en la cola.

2.6.3.4 Mecanismos para Evitar Congestión [3] [11] [32]

Las técnicas para evitar la congestión realiza un monitoreo de la carga de tráfico de manera proactiva, reaccionando para evitar posibles cuellos de botella. Estas técnicas están designadas para proveer diferentes tratamientos a las clases según la prioridad, tratando de maximizar el *throughput* y la capacidad y minimizando la pérdida de paquetes y el *delay*.

2.6.3.4.1 *Weighted Random Early Detect Distributed (WRED)*

Es una técnica de prevención de congestión, para ello vigila la carga de tráfico y descarta paquetes de manera que no se generen cuellos de botella es la evolución de *Random Early Detection* (RED).

RED es un método que consiste en descartar paquetes de manera aleatoria antes de que se produzca un evento de congestión para esto vigila el grado de ocupación de una cola, a medida que este se incrementa la probabilidad de descarte también aumenta, al producirse el descarte de un paquete se fuerza a que TCP reduzca la tasa de envió de datos evitando la congestión.

En cambio WRED define dos parámetros para determinar si un paquete se descarta define un umbral mínimo que especifica el número de paquetes que se pueden mantener en una cola antes de que se considere descartar paquetes y un umbral máximo que es un valor referencial máximo, antes de alcanzar este valor se descartan todos los paquetes que arriben a la cola para evitar congestión.

WRED descarta los paquetes basándose en la prioridad es decir los que tienen un alta prioridad tienen un menor probabilidad de descarte, para determinar en qué momento se descartan los paquetes se calcula la longitud media de la cola y se

compara este valor con los umbrales definidos, la probabilidad de descarte se incrementa cuando la longitud media se acerca al valor máximo.

2.6.4 CLASES DE SERVICIO DENTRO DE CNT [2]

Dentro de la red de la empresa se manejan diferentes tipos de clases de servicio y la forma en que se mapean entre los bits EXP MPLS y de precedencia IP se muestra en la tabla 2.6.

Aplicación	Clases
Enrutamiento	Control de la red
Gestión de red	
Voz	
Video Interactivo	VoIP
Señalización de voz	
Streaming de video	
Datos críticos	Datos Críticos
Datos Transaccionales	
Datos masivos	Datos no críticos
Mejor esfuerzo	
Por defecto	Default

Tabla 2.6- Clases Creadas por la CNT E.P.[2]

Las políticas que se implementan son:

- Manejo de Congestión en colas de salida
- Definición de la clase CM-VoIP como prioritaria
- Limitación del tráfico en la cola prioritaria al 10% del ancho de banda (BW)
- Asignación de anchos de banda mínimos garantizados al resto de las clases, según:
- Clase CM-Video: 30% BW
- Clase CM-Controlred: 3% BW

- Clase CM-Datoscriticos: 10% BW
- Clase CM-Datosnocriticos: 20% BW
- Clase Default: 15% BW
- Descarte de tráfico aleatorio mediante WRED en las clases Datoscriticos, Datosnocriticos y class-default
- Asignación de otros atributos como Queue-Limit[13] para las clases VoIP y Video.

2.7 *VIRTUAL PRIVATE NETWORKS* (VPN) [2] [14] [15] [34] [40]

Las redes privadas virtuales MPLS "MPLS VPN" son una de las aplicaciones más populares de la tecnología MPLS, que en la actualidad los proveedores de servicios han optado para la migración de sus tradicionales redes Frame Relay y ATM a redes MPLS VPN, y este es el caso de la Corporación Nacional de Telecomunicaciones "CNT EP" en la que se aplica esta aplicación tanto a nivel de capa 2 como capa 3.

La aplicación MPLS VPN sigue teniendo un gran interés que va en aumento dentro de las telecomunicaciones, donde los grandes *Service Provider* lo han empezado a usar como la siguiente innovación en el diseño de la red, con lo cual proporciona a los proveedores de servicios una alta escalabilidad y facilita el funcionamiento y administración de la red.

2.7.1 ELEMENTOS DE UNA VPN MPLS [15]

Una MPLS VPN está conformada por los siguientes elementos.

CE router: dispositivo de borde que pertenece a la red del cliente, es el dispositivo a través del cual el cliente/usuario final se conecta a la red del proveedor de servicios, conocido también como equipo local del cliente *(Customer Premises Equipment [CPE])*. Usualmente es un router y es a menudo referido a un CE router.

[13] Máximo número de paquetes que una cola puede mantener con un rango de 1 a 64.

PE router: dispositivo de borde que pertenece a la red del proveedor de servicios para el caso de CNT E.P. estos equipos son los Cisco 7600-S RSP720, el mismo que tiene una conexión directa con el dispositivo de borde del cliente CE router de capa 3. Este equipo tiene como funcionalidad la de separar las diferentes VPNs, corriendo protocolos de ruteo separados por CE (denominados *PE-CE connectivity protocols*), ademas de realizar el push o pop de etiquetas dependiendo de la dirección del flujo de datos.

P router: es un dispositivo que pertenece a la red del proveedor de servicios en el caso de CNT E.P. esta función la llevarán a cabo equipos CRS-1 y XR12000, los cuales no tienen conexiones directas con los routers del cliente y tampoco poseen conocimientos de la VPN. Estos equipos actúan como core de red transportando el tráfico desde el borde, sin hacer abstracción de los servicios mediante el *label stacking* de MPLS.

En la figura 2.32 se indican los diferentes elementos que conforman una MPLS VPN anteriormente explicados.

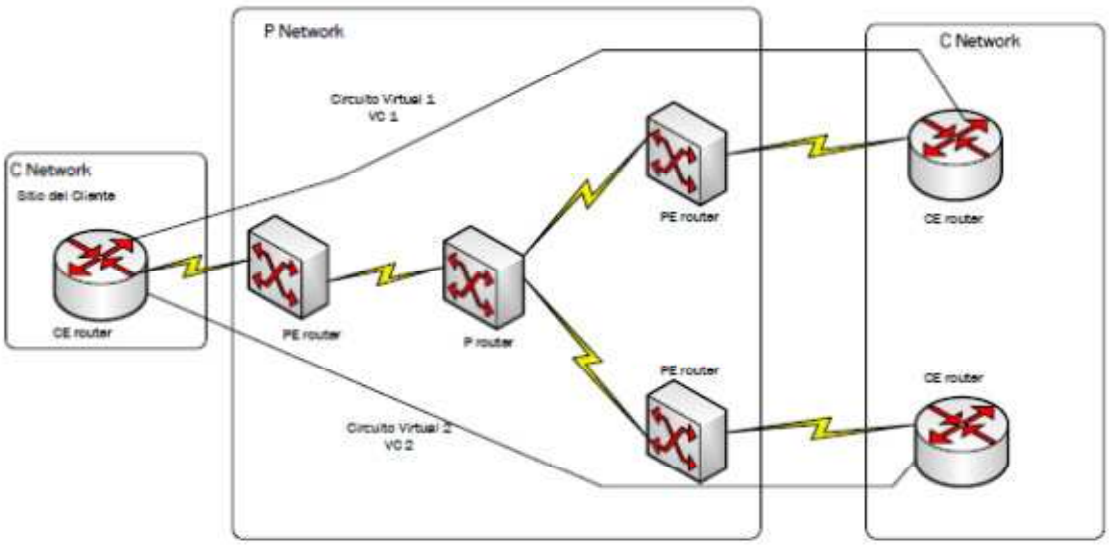


Figura 2.32: Elementos de una VPN [15]

Cuando se realiza una implementación MPLS VPN los routers P y PE deben correr MPLS de tal manera que puedan distribuir y enviar etiquetas entre ellos mientras que el CE router no necesita correr MPLS mas que en el caso de CNT E.P solo manejar IP puro, además entre los routers CE y PE interactúan a nivel de

capa 3 por tanto necesitan correr un protocolo de enrutamiento dinámico o estático entre ellos.

2.7.2 VPN MPLS CAPA 2 [7] [34] [46]

A pesar que se puede usar este tipo de soluciones en las redes actuales como MPLS no es un término nuevo, pues se hace referencia a este tipo de soluciones desde tecnologías anteriores como ATM y Frame Relay las mismas que fueron grandes infraestructuras de red de capa 2.

Una VPN de capa 2 permite ofrecer una solución conmutada que separa le red del proveedor de servicios de la del cliente, debido a que no existe un intercambio de enrutamiento entre los equipos de los dos involucrados reduciendo la complejidad de la implementación, el enrutamiento se debe configurar en los equipos de frontera de la red del cliente y es responsabilidad de este.

Estas VPN permiten emular servicios capaces de transportar tramas de capa 2 como Frame Relay, ATM, Ethernet sobre MPLS para lo que se utilizan *pseudowires*, con esto se mantiene un nivel de compatibilidad con las infraestructuras anteriores, la conectividad de un sitio con otro es transparente para los equipos del cliente que utilizan estas tecnologías.

Para enviar las VPN de capa 2 sobre una infraestructura IP/MPLS se utiliza *pseudowires* que es un enlace entre dos equipos PE de un proveedor que conecta dos emulaciones de servicios en los puntos finales, estos servicios se encargan de realizar un conjunto de funciones especificas que permiten adaptar las tramas de diferentes tecnologías y enviarlas sobre una red conmutada de paquetes, para establecer las *pseudowires* se utiliza mecanismos de señalización como LDP.

Cuando una trama llega al PE este encapsula la trama y la envía por un *pseudowire* para esto se usa un LSP. Se manejan dos tipos de modelos de conexión uno punto a punto y uno multipunto, que se los conoce como VPWS *(Virtual Private Wire Service)* y VPLS *(Virtual Private LAN Service)* respectivamente.

2.7.2.1 *Virtual Private Wire Service*

También se los conoce como *VLL (Virtual Leased line service)*, son servicios punto a punto que proveen conexión entre dos lugares distantes de un cliente a través de un backbone IP/MPLS de un proveedor de servicios.

Las VPWS pueden tener el mismo tipo de tecnología de transporte en cada en cada una de las terminaciones de la VPN o diferentes tipos en estas, en caso de que no sean similares los nodos PE deben realizan la traducción de un tipo de transporte a otro.

Para establecer una conexión entre dos nodos PE de un proveedor de servicios y brindar un servicio de capa 2 a un cliente se utiliza una conexión con una *pseudowire* como se observa en la figura 2.33, previo al establecimiento de esta se debe tener configurado correctamente MPLS, un IGP y un LDP, el IGP se encarga de establecer la ruta por la que se alcanzará un PE, una vez establecida esta LDP se encargará de asignar las etiquetas creando un LSP entre los dos PEs.

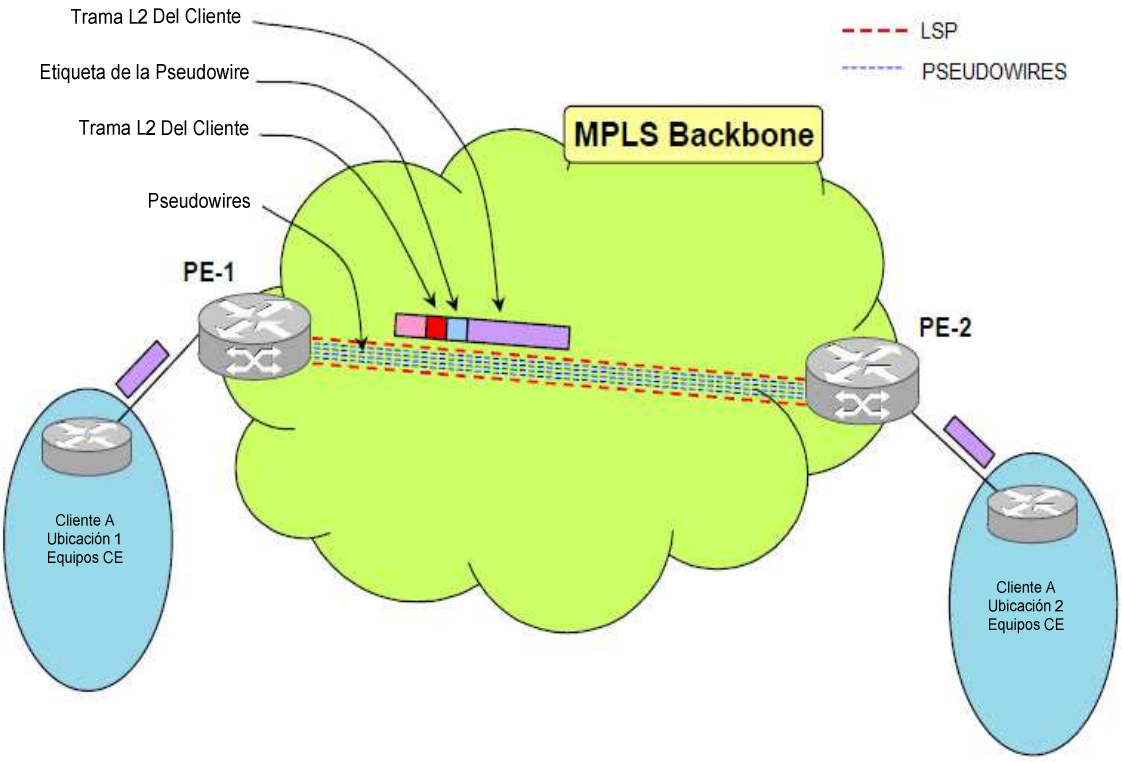


Figura 2.33: Conexión punto a punto VPWS. [46]

Considerando que un LSP es un camino unidireccional se deben tener 2 *pseudowires* para obtener una conexión dúplex, para establecer estas se utiliza un método de señalización como LDP, se intercambia el tipo de circuito virtual y otros parámetros que son parte del LDP *forwarding equivalence class (FEC)*, se asigna una etiqueta que identifica a *pseudowire*.

Cuando un PE recibe una trama se le retira el encabezado y se añade un campo de control de 4 bytes donde se lleva información del tamaño de la trama, las banderas y el número de secuencia (depende de la tecnología de capa 2), se le añade la etiqueta que identifica a la *pseudowire,* ésta se coloca en el fondo de la pila de etiquetas, sobre ésta se coloca otra etiqueta para enviarla por el LSP correspondiente y que se realice la conmutación en la red MPLS, solo el nodo destino leerán la segunda etiqueta reconstruirá la trama de capa 2 adecuada y la enviará al cliente correspondiente esto se observa en la figura 2.33.

Como se mencionó se pueden tener similares tecnologías en las dos terminaciones conocidas como igual a igual las tecnologías soportadas son: Ethernet, Frame Relay, PPP, HDLC, ATM. Adicionalmente se puede tener un modelo donde se tengan dos tecnologías diferentes en las terminaciones conocidas como cualquiera a cualquiera y se pueden tener las siguientes configuraciones:

- Interconexión Ethernet a Frame Relay.
- Interconexión Ethernet a ATM.
- Interconexión ATM a Frame Relay
- Interconexión Ethernet a PPP/HDLC
- Interconexión Frame Relay a PPP/HDLC.
- Interconexión ATM a PPP/HDLC.

2.7.2.2 *Virtual Private LAN Service*

Es un servicio Ethernet multipunto a multipunto que provee servicios de conmutación entre las diferentes ubicaciones del cliente que se encuentren unidos a la red, para dar este tipo de servicio se usa las *pseudowires* como base y se les

añade la capacidad de envió basada en MAC, este tipo de VPN ofrecen extensiones de la LAN y los dominios de *broadcast* en una WAN esto se observa en la figura 2.34.

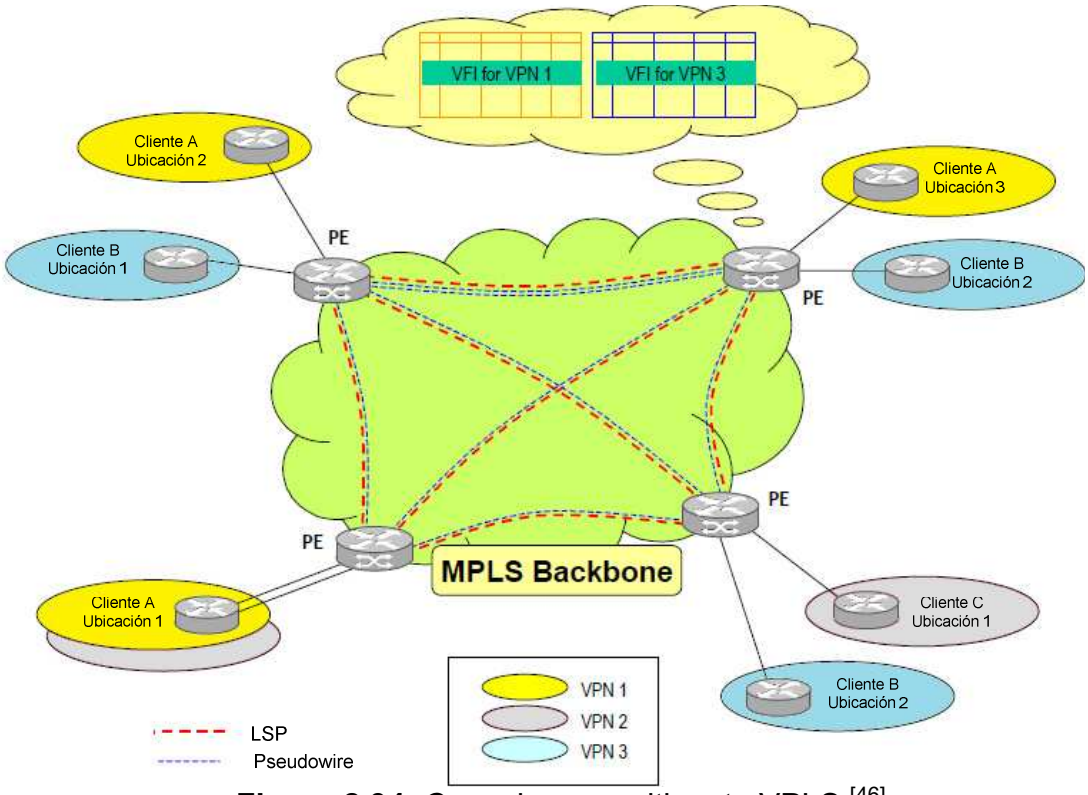


Figura 2.34: Conexiones multipunto VPLS [46]

Se establecen una topología full *mesh* entre los PE a los que se conecta el cliente que pertenece a una VPN para lo que se utiliza varias *pseudowires* entre los PEs para el establecimiento de estos se puede utilizar BGP como protocolo de señalización adicional a LDP.

Para VPLS se necesitan las *virtual switch instance (VSI)* en los PEs, estas son tablas de direcciones MAC que contienen la información correspondiente a los dispositivos del segmento LAN conectados al PE o de las localidades remotas que son parte del dominio VPLS en la figura se pueden ver los elementos que la conforman, se mantienen VSI diferentes para cada VPN que se transporta.

El envió de los paquetes en los PEs es similar al de los switch Ethernet, es decir se realiza un envio basado en MAC y se aplican todas las reglas del *switching*, adicionalmente se usa la regla del horizonte dividido para evitar los lazos en la

red, este escenario provee una conectividad simple y trabaja bien con un pequeño número de sitios a conectarse.

En la red IP/MPLS de CNT se usan las VPLS para transporte de datos de los clientes home ADSL o WIMAX de esta manera se permiten que los usuarios accedan a un servidor *BRAS (Broadband Remote Access Service),* que es el encargado de controlar el ancho de banda que se le asigna a cada usuario, se encarga de realizar la autorización, autenticación y la contabilización del consumo de recursos de los usuarios para una posterior facturación.

Una vez conectados al servidor y autenticados se les permite acceder a internet para eso se utiliza *PPPoE (Point to Point Protocol over Ethernet),* adicionalmente las VPLS se utilizan para ofrecer los servicios de última milla, a través de los que otros ISPs pueden ofrecer sus servicios utilizando la gran infraestructura de cobre de la que dispone CNT.

2.7.3 VPNs L3 "BGP-MPLS VPN" [2] [40] [15]

Una VPN basada en MPLS usa el modelo *peer-to-peer* y combina los beneficios de *overlay* (seguridad y características de segregación) y *peer-to-peer* VPN ("simplificación del enrutamiento del cliente"). En la figura 2.35 se observa el concepto de un VRF en un router físico.

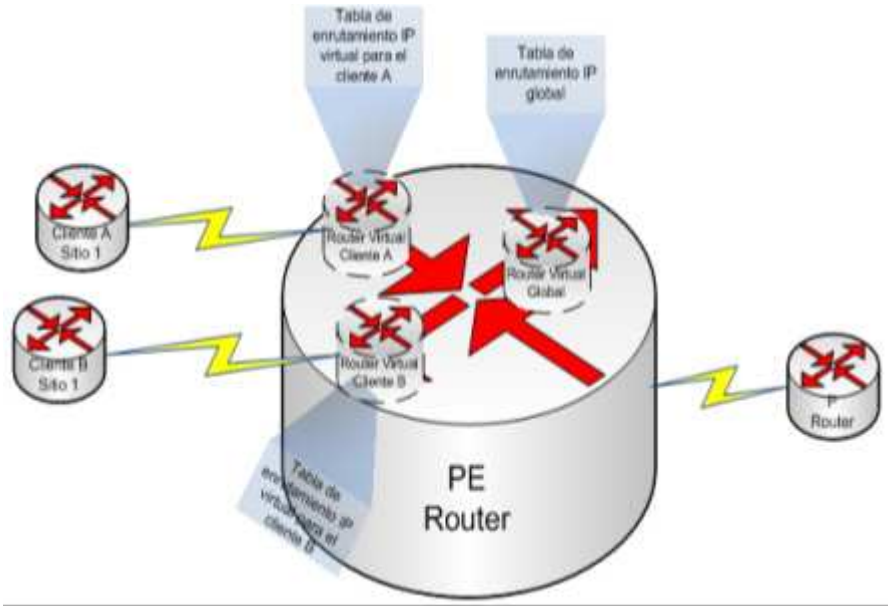


Figura 2.35: Conceptualización de una VRF dentro de un router físico [15]

La arquitectura de una MPLS/VPN se basa en el que cada cliente VPN tiene un router PE dedicado, el cual transporta únicamente sus propias rutas y crea las tablas de enrutamiento, únicamente con las rutas anunciadas por sus clientes VPN conectados a ellos, pero con la ayuda de MPLS el aislamiento entre los clientes VPN es por medio de routers virtuales levantados en el PE router a través de enrutamiento y envío virtual *(Virtual Routing and Forwarding "VRF")* los cuales pertenecen a diferentes clientes VPN, esto se indica en la figura 2.35.

2.7.3.1 Arquitectura MPLS VPN L3 [2] [15]

2.7.3.1.1 *VRF (Virtual Routing and Forwarding)*

Una VRF es el elemento básico para proveer servicios de VPN en una red MPLS. Con significancia local es el separador entre la routing Tabla global y la instancia propia virtual de ruteo (Virtual Router Forwarder). Las VRFs se configuraran en los PEs (Edge Ruteadores) que contengan servicios dentro de esas VPNs.

Cada VRF por definición incluye los siguientes componentes:

- Un nombre que identifica la VRF *(Case Sensitive)*
- Un *Route Disguisher* que identifica únicamente las redes IPv4 recibidas sobre la interface del cliente.
- Importa y exporta los *route-targets* definiendo los atributos para importar y exportar las mismas.
- *Route-maps* opcionales definiendo políticas de *export-import*

2.7.3.1.2 *Route Distinguisher*

El *route distinguisher* es un campo de 64 bits y puede ser representado por medio de dos formatos: ASN:nn***,*** donde ASN es el número de sistema autónomo que el *Internet Assigned Numbers Authority (IANA)* asigna al proveedor de servicios y el ***nn*** es el número que el proveedor de servicios asigna únicamente a una VRF. E IP-address:nn.

2.7.3.1.3 *Route Targets (RT)*

A través de la utilización de prefijos RD se identifica la pertenencia a una VPN pero la comunicación entre los sitios de diferentes VPNs no es posible. Siendo así, los *route targets* (RTs) fueron introducidos en la arquitectura MPLS con la finalidad de soportar complejas topologías de VPNs donde los sitios de los clientes pueden participar en más de una VPN. Los route targets son atributos adicionales añadidos a las rutas VPNv4 BGP con lo cual se indica pertenencia a una VPN. Para codificar dichos atributos se hace uso de comunidades extendidas de BGP las mismas que transportan los principales atributos.

Los RTs pueden trabajar de dos maneras:

- *Export RT*, identifican la pertenencia a una VPN y va adjunta a la ruta del cliente cuando ha sido convertida en una ruta VPNv4.
- *Import RT*, asociada con cada tabla de enrutamiento virtual y selecciona las rutas que van a ser insertadas en la VRF.

Tanto las *Export RTs* e *Import RTs* son el bloque central de las VPN debido a que la utilización de las mismas expresan las políticas que determinan la conectividad entre los sitios de los clientes.

2.7.3.2 Distribución de la Información de Ruteo para VPNs

Un servicio VPN L2/L3 requiere de un servicio de transporte de etiquetas, debido a que un LSP es requerido entre cualquier par de PEs involucrados en una aplicación VPN, en la red de CNT E.P. los LSP se derivarán de LDP para el caso de la distribución de los *labels* pertenecientes a los prefijos que se encuentran en el IGP, algunos de estos prefijos como por ejemplo las de la interfaces Loopbacks son utilizados como Next-Hop por MPBGP, LDP tiene que estar habilitado en todos los nodos de la red MPLS.

A su vez también habrá conexiones MP-BGP para señalizar los servicios de VPN de nivel 3, redes VPNv4. Por lo tanto todos los nodos PE deberán tener sesiones

MP-BGP contra los RRs (*Route Reflectors*) de la red. Las excepciones a MP-BGP son los nodos P, los cuales no tendrán conocimiento de redes BGP vpnv4.

Un router PE puede aprender prefijos IP de un router CE estáticamente o por medio de un protocolo de ruteo dinámico como BGP, RIP, EIGRP u OSPF entre el *Provider* y el *Customer*. Los prefijos IP son miembros de los *address-family* IPv4. Después de que el router PE aprende los prefijos IP, este lo convierte a prefijos VPNv4 combinando el prefijo IP aprendido, con los 8 Bytes de los *route-distinguisher* (RD), y el nuevo prefijo generado es ahora miembro del *address-family* VPNv4.

Esto sirve para identificar inequívocamente a las direcciones de clientes, aun si hay un *overlap*, ya que en una VPN, los clientes del proveedor de servicios VPN mantienen su propio esquema de direccionamiento, esto significa usar sus direcciones IP registradas, direcciones IP privadas ó también direcciones IP que están siendo usadas por otros clientes conectados al mismo proveedor de servicios (conocido como *overlapping IP addressing*).

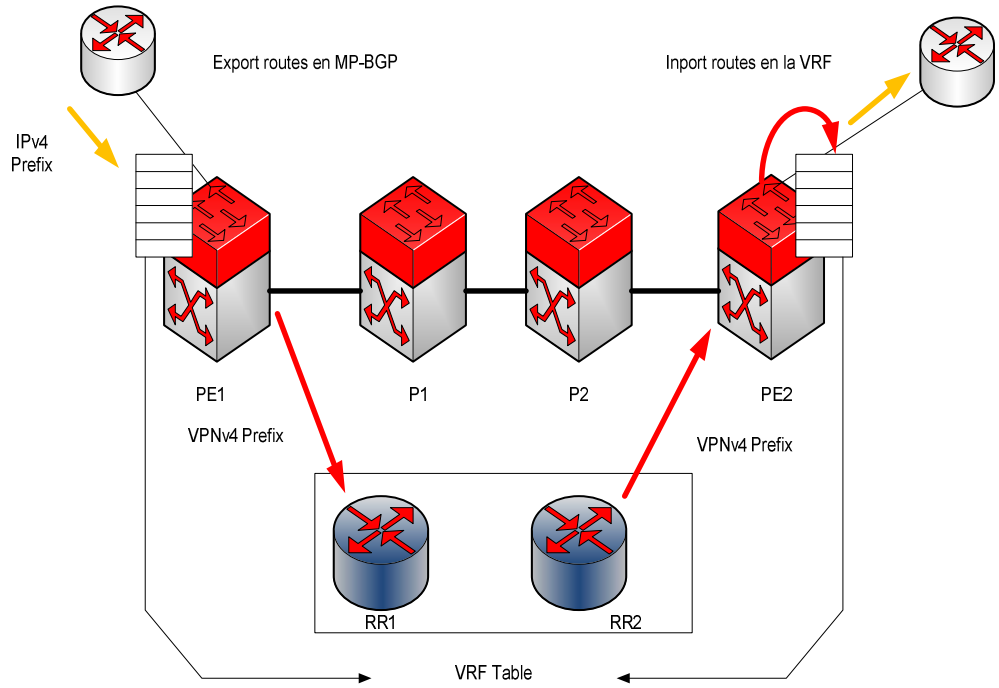


Figura 2.36: Intercambio de las tablas de enrutamiento virtuales entre PEs con MP-BGP [15]

BGP provee lo que se llama "*Multiprotocol Extensions*" (RFC2283, *Mutiprotocol Extension for* BGP-4), el cual define diferentes *addressfamilies* IPv4 y VPNv4 y permite la distribución de las redes VPNv4 en la red como se observa en la figura 2.36. Propaga la información VPNv4 a los otros PE.

La información de la VPN solo será propagada a aquellos routers que contengan la VPN en cuestión. Todos los miembros de la VPN aprenden las redes de otros routers que son miembros de la misma, habilitándolos para la comunicación entre ellos. La operación básica de la distribución de rutas VPNv4 es ilustrada en la figura 2.36. La comunicación a nivel de BGP sucede en dos niveles: dentro del sistema autónomo iBGP (*internal* BGP), o entre sistemas autónomos eBGP (*external* BGP).

El PE agrega una etiqueta a cada prefijo recibido del CE e incluye la misma dentro de la información que conocemos como "*Network Reachibility*" para informarla al resto de los PE.

Cuando un PE quiere hacer el *forwarding* de un paquete en una VRF hacia otro PE, le coloca la etiqueta antes mencionada que se relaciona con el router que genera ese prefijo para esa VPN. Cuando el router destino (*Destination* PE) recibe es paquete con el label, realiza una búsqueda en la correspondiente VRF y hace un pop del ultimo label para pasar el ahora paquete IPv4 al CE.

2.8 INGENIERÍA DE TRÁFICO [2] [3]

2.8.1 INTRODUCCIÓN

Debido a que Internet se ha transformado en un medio multiservicios en la que convergen voz, vídeo y comunicaciones de datos, su tráfico ha ido en crecimiento de forma agravada, siguiendo un crecimiento constante. Los grandes proveedores de servicios de Internet han respondido al reto del crecimiento de Internet mediante la implementación de tres iniciativas complementarias: arquitecturas escalables de red, la expansión de la capacidad, e ingeniería de tráfico (TE).

ISPs tienen cada vez más el reto de proporcionar la fiabilidad que los usuarios se han acostumbrado con redes PSTN y TDM. También hay una necesidad de establecer la diferenciación de servicios en las redes para que los ISP puedan proporcionar diferentes clases de servicio con tarifas diferenciadas.

Con el fin de proporcionar estas capacidades en la red, el prototipo básico de reenvío de tráfico de la Internet de hoy en día debe ser mejorado, para soportar la ingeniería de tráfico. La ingeniería de tráfico abarca muchos aspectos del rendimiento de la red, estos incluyen la provisión de una garantía de QoS, la mejora de la utilización de los recursos de la red con la distribución de tráfico de forma uniforme a través de los enlaces de la red, y por la recuperación rápida cuando un nodo o enlace falla.

La Internet puede ser modelada como una colección de sistemas autónomos que se comunican entre sí mediante un *Exterior Gateway Protocol (EGP)*, y un *Interior Gateway Protocol (IGP)* se ejecuta en el sistema autónomo para proporcionar cualquiera conexión. Protocolos de estado de enlace como Sistema Intermedio a Sistema Intermedio (IS-IS) y *Open Shortest Path First (OSPF)* suelen ofrecer la funcionalidad de IGP. El EGP actualmente en uso es BGP4, los protocolos de enrutamiento de estado del enlace IGP se utilizan para distribuir información acerca de todos los enlaces de la red.

En consecuencia, todos los routers IGP dentro del sistema autónomo, obtienen una imagen completa de todos los enlaces y los routers de la red. Cada router utiliza esta información para calcular la ruta más corta a cada subred de destino posible en la red utilizando un algoritmo de ruta más corta SPF. El router construye una tabla de reenvío, asociando un prefijo de dirección con el enlace del siguiente salto.

En una red con una topología extensa y densamente conectada, este enfoque podría causar una carga desproporcionada a la red. Los enlaces que no están en el árbol del camino más corto permanecen subutilizadas a pesar de la presencia de las cargas de tráfico pesado, esto conduce a la pérdida de ancho de banda y

subutilizados en las troncales del proveedor de servicios que de otro modo se podría poner a buen uso.

Este problema es actualmente direccionable en cierta medida, mediante la manipulación de la métrica del enlace, utilizada por los protocolos de enrutamiento y obligando al desigual costo de balanceo de carga a través de los enlaces. Sin embargo, estos métodos no proporcionan redundancia dinámica y no considerar las características del tráfico ofrecido y las limitaciones de capacidad de la red cuando se toman decisiones de enrutamiento, pero esto se ve solucionado con la Ingeniería de Tráfico.

2.8.2 MANIPULACIÓN DE MÉTRICAS DE LOS PROTOCOLOS DE ENRUTAMIENTO VS INGENIERÍA DE TRÁFICO MPLS [2] [3]

En redes IP se tiene una pobre eficiencia, debido a que el único mecanismo para redirigir el tráfico es cambiar la métrica de enlace presente en protocolos de estado de enlace IGP tal como OSPF. Sin embargo, el cambio de una métrica de enlace potencialmente puede cambiar la ruta de acceso de todos los paquetes que pasan por dicho enlace. Además, estos métodos no proporcionan redundancia dinámica y no considerar las características del tráfico ofrecido y las limitaciones de capacidad de la red cuando se toman decisiones de enrutamiento.

En una red MPLS con ingeniería de tráfico, cualquier *Label-Switched-Path (LSP)* puede ser cambiado dinámicamente desde una ruta congestionada a una ruta alternativa. Esto representa una mejora de la eficiencia en los métodos tradicionales de funcionamiento de las redes IP.

Además, los administradores de red pueden hacer uso de algoritmos de optimización global que proporcionan un mapeo de la demanda de tráfico a los enlaces físicos, de otro modo no se podría lograr usando sólo optimización local. El resultado neto es que un proveedor de servicios puede alcanzar un grado mucho más alto de utilización de los enlaces en toda la red, con la prestación de servicios a un costo menor.

Ingeniería de tráfico MPLS permite a los proveedores de servicios definir rutas de acceso explícito. Rutas explícitas redundantes se puede configurar, para proporcionar un mecanismo de reserva. Ingeniería de tráfico también se puede realizar mediante el *Cisco Express Forwarding (CEF)* basado en el costo desigual de balanceo de carga a través de túneles. Esta combinación de ajuste manual o automático ayuda a alcanzar los objetivos de la planificación de la capacidad y ayuda a optimizar la utilización de la red en el core.

2.8.3 VENTAJAS DE LA INGENIERÍA DE TRÁFICO MPLS [3]

Las características de Ingeniería de tráfico MPLS permiten a un backbone MPLS replicar y ampliar las capacidades de tráfico de la capa 2 de redes ATM y Frame Relay. Ingeniería de tráfico es esencial para los proveedores de servicios y backbones de Internet del proveedor de servicios.

Ambos backbones debe ser compatible con un alto uso de capacidad de transmisión y las redes deben ser muy flexibles para que puedan soportar fallos de enlace o nodo. Las siguientes son las ventajas de la ingeniería de tráfico MPLS:

- Con MPLS, las capacidades de ingeniería de tráfico están integradas en la Capa 3, permitiendo optimizar el enrutamiento de tráfico IP, dadas las limitaciones impuestas por la capacidad de backbones y la topología. En rutas IP el flujo de tráfico a través de una red basada en los recursos que el flujo de tráfico requiere y los recursos disponibles en la red.
- Utiliza *constraint-based routing*, en los que el camino para un flujo de tráfico es el camino más corto que responda a las necesidades de recursos o las limitaciones en términos de requisitos de ancho de banda, los requisitos de los medios de comunicación, y la prioridad del flujo de tráfico.
- Dinámicamente se recupera de errores de enlace o nodo, cambia la topología del backbone mediante la adaptación a una nueva serie de limitaciones, aunque varios caminos principales son calculados de antemano.

- Permite desigual participación en los costos de carga y permite el uso de otros caminos de las rutas aprendidas IGP.
- Representa enlaces por ancho de banda y por el tamaño del flujo de tráfico, cuando determinar rutas explícitas a través del backbone.
- Sustituye la necesidad de configurar manualmente los dispositivos de red para establecer rutas explícitas. En su lugar, se confía en la funcionalidad de ingeniería de tráfico MPLS para comprender la topología del backbone y el proceso automatizado de señalización.

2.8.4 ELEMENTOS DE INGENIERÍA DE TRÁFICO MPLS [3]

El modelo de superposición en la que IP se ejecuta sobre una red ATM o Frame Relay resulta en distintas capas de red, Capa 2 o Capa 3. La red IP funciona sobre una topología virtual en el que cada router es un salto de distancia. Esto causa dificultades y ocasiona respuestas lentas de la red para eventos tales como fallas de enlace o nodo.

MPLS permite a los elementos de ingeniería de tráfico estar completamente bajo el control de IP. Esto da lugar a una red de un nivel que puede ofrecer servicios IP, que ahora se puede lograr únicamente por la superposición de la red de Capa 3 en una red de capa 2. Esto proporciona una forma de lograr los beneficios de ingeniería de tráfico del modelo de superposición sin necesidad de ejecutar una red independiente y sin necesidad de una malla no escalable llena de routers interconectados.

Ingeniería de tráfico MPLS utiliza el Protocolo de reserva de recursos (RSVP) para establecer y mantener automáticamente un túnel a través del backbone. La ruta utilizada por un túnel dado, se determina en un instante de tiempo en base a los requerimientos de recursos del túnel y los recursos de red disponibles, tales como ancho de banda. La información disponible de los recursos se inunda a través de extensiones de estado de enlace basado en el IGP como OSPF o IS-IS.

Las rutas de los túneles se calculan en el inicio del túnel (router de origen o Head-End Router) basándose en el ajuste entre los recursos requeridos y los recursos

disponibles (basada en restricciones de enrutamiento). El IGP automáticamente enruta el tráfico dentro de estos túneles. Normalmente, un paquete cruza el backbone MPLS con Ingeniería de Tráfico, a través de un solo túnel que conecta el punto de entrada hasta el punto de salida.

2.8.4.1 Túneles LSP [2]

Túneles LSP proporcionan el mecanismo para el manejo de paquetes a través de la red MPLS. Se construyen utilizando un protocolo de señalización de servicios integrados tal como RSVP. Los túneles LSP comparten muchas de las características de los caminos virtuales de una red ATM, son explícitamente establecidos, ruteados y tiene un amplio conjunto de mecanismos de QoS.

El mensaje "RSVP PATH", lleva la ruta explícita a seguir y se utiliza en la asignación provisional de recursos a lo largo del camino, la respuesta al mensaje "RSVP PATH", es un mensaje de reserva "RSVP RESV", el cual establece las operaciones de la etiqueta y cambia la asignación provisional en una reserva permanente de recursos. Cuando se utiliza RSVP, la totalidad de ofertas de QoS de Servicios Integrados se ponen a disposición.

Túneles LSP son unidireccionales. El router de origen se conoce como la "*headend*", y el router de destino se conoce como *"tail end"*. Los caminos de ida y vuelta para un flujo IP son independientes, por lo tanto, la naturaleza unidireccional de túneles LSP encaja bien con la ingeniería de tráfico de tráfico IP.

2.8.4.2 Distribución de la Información de *Constraint-Based Routing* [3]

La distribución de la información *Constraint-Based Routing* se debe realizar a fin de encontrar caminos apropiados a través de la red. Túneles LSP con Ingeniería de Tráfico deben ser enrutados con un conocimiento de la carga de tráfico que necesitan para llevar. La restricción de la información debe ser distribuida a través de la red MPLS de forma coherente. El mecanismo utilizado por las inundaciones de protocolos de enrutamiento de estado de enlace como OSPF e IS-IS puede ayudar a crear una base de datos de reenvío y restricciones de tráfico integrado.

2.8.4.3 Asignación de Tráfico a Túneles [2] [3]

La función integrada de enrutamiento realiza la asignación automática de tráfico a los túneles utilizando una modificación del algoritmo SPF. El algoritmo convencional SPF se ejecuta de forma iterativa colocando caminos contendientes en una lista provisional, seleccionando la ruta más corta de esa lista, y añadió la ruta y nodo destino a su árbol de transmisión.

El nodo raíz se añade al árbol SPF y luego agrega las rutas de acceso de un salto a cada uno de sus vecinos directamente conectados a la lista provisional. En cada iteración, se agrega la ruta más corta presente a su árbol y luego extiende las rutas a través de los enlaces conectados al último nodo de la ruta. Las tablas de enrutamiento se derivan de este árbol del camino más corto, contienen conjuntos ordenados de destino y la información de primer salto.

Algoritmos de Ingeniería de Tráfico calculan rutas explícitas a uno o más nodos de la red. Estas rutas explícitas son vistas como interfaces lógicas por el router de origen, las rutas explícitas están representadas por el LSP y son llamados túneles de ingeniería de tráfico (túneles TE).

Un IGP de estado de enlace puede instalar rutas en la tabla de enrutamiento que apuntan a estos túneles TE, utilizan rutas explícitas, y el router que es *headend* del túnel controla el camino recorrido por un túnel TE, en el caso de CNT EP por defecto el LSP desde el *Head-end Router* hasta el *Tail-end Router* no serán anunciados por el protocolo de ruteo IS-IS, y cualquier prefijo de red anunciado por el *Tail-end Router* no serán visibles a través de estos caminos, para habilitar la instalación de rutas anunciadas por el *Tail-end Router* es necesario habilitar el *“AutoRoute Announce”*.

El tráfico también se puede asignar a los túneles LSP basados en el siguiente salto BGP o usando parámetros de clase de servicio (CoS). RSVP define la agregación sobrante de túneles, los túneles LSP puede ser utilizado de esta manera, con la ventaja añadida de que podrán ser ruteados a donde los recursos existen, si la ruta normal IP tiende insuficientes recursos para la solicitud.

Para la CNT E.P. para realizar *forwarding* en Túneles TE se realiza configurando explícitamente cuales prefijos o direcciones de red queremos alcanzar vía el túnel "rutas estáticas", y de esta manera se tiene un control más eficiente sobre el tráfico que seguirá un túnel en particular y cual tráfico seguirá otro camino, ya que no siempre se requiere que todo el tráfico dirigido hacia un *Tail-end Router* sea enviado por el túnel.

2.8.4.4 Cambio de Ruta [3]

Redes de Ingeniería de Tráfico debe ser capaz de responder a los cambios en la topología de la red y mantener la estabilidad. Cualquier falla de enlace o nodo no debe interrumpir los servicios de alta prioridad de la red, sobre todo las clases más altas de servicio. Rápidos cambios de ruta es un mecanismo que reduce al mínimo las interrupciones del servicio para el tráfico de los flujos afectados por una falla, y optimiza los flujos re-enrutados del tráfico re-optimizado afectados por un cambio en la topología.

2.8.4.5 Redireccionamiento Rápido "*Fast-Reroute FRR*" [2]

En MPLS, técnicas de corte/empalme y apilamiento se utilizan para permitir la reparación local de túneles LSP.

2.8.4.5.1 *Técnica de corte y empalme*

En esta técnica, una alternativa de túnel LSP es preestablecido desde el punto de la protección al destino a través de un camino de bypass por los elementos intermedios protegidos de red. Si se detecta una falla, la entrada de reenvío para la protección del túnel LSP se actualiza para utilizar la etiqueta y la interfaz del túnel de derivación LSP.

2.8.4.5.2 *Técnica de Apilamiento*

En esta técnica, una alternativa única de túnel LSP, actúa como reemplazo para el enlace fallido y estos bypass protegen el enlace. El router local mantiene una etiqueta que representa el túnel de bypass.

Cuando el enlace protegido falla, todos los túneles que usan el enlace se actualizan para utilizar el túnel de derivación. La información de la etiqueta de envió se actualiza para hacer su primer intercambio normal y obliga en la etiqueta para el túnel de derivación y envía el paquete por la interfaz para el túnel de derivación.

La etiqueta de la pila se extrae en el salto siguiente al último del túnel de derivación. Esto entrega las etiquetas de espera por el router al lado de la protección del túnel LSP.

Para la operación de FRR se requiere que la detección de fallas se dé rápidamente y que se anuncie que una falla se ha producido para que el FRR se active.

Existen diversos mecanismos para la detección de fallas de link, en el caso de links del tipo directos o fibra oscura, cuando se produce una falla se generará una caída de la interfaz mediante LoS, siendo este estado suficiente para que FRR actúe, por lo tanto el tiempo de convergencia estará dado por la rapidez en que una interfaz detecte la caída de un enlace y ponga la interfaz en el estado de *Link Down*.

Existen ocasiones en las que un router no es capaz de percibir una pérdida de comunicación en un link, esto ocurre normalmente cuando no se tienen conexiones *back-to-back* y no existen mecanismos de señalización *end-to-end* de la red de transporte.

De esta manera un router podría dejar de tener comunicación con su vecino pero no detectar la falla del enlace, para solucionar este problema se hace uso de un protocolo liviano orientado específicamente a la detección de fallas en el plano de *forwarding*, este protocolo es el BFD, el cual establece sesiones en cada enlace y permite ajustar los tiempos de convergencia, si una sesión BFD se pierde este informa a un punto de reparación para que este re-enrute el tráfico a través del túnel de *backup*.

2.8.5 SITUACIÓN ACTUAL DE INGENIERÍA DE TRÁFICO DE CNT E.P. [2]

Actualmente la red MPLS transporta servicios de datos y voz. Se ha llevado a cabo la implementación de túneles de tráfico para proteger el tráfico de señalización de VoIP. La situación operativa actual es la siguiente:

Se han implementado diversos túneles, principalmente para protección de tráfico VoIP. Estos túneles se han configurado en general entre los PE remotos y el PE donde se encuentra el softswitch para el servicio de VoIP.

En muchos túneles no se están cursando tráfico, debido a que no hay rutas estáticas o algún otro mecanismo de forwarding implementado.

Los requerimientos actuales del servicio de VoIP, en CNT E.P., señalan que la convergencia requerida es del orden de los 2 a 5 segundos, lo cual no hace necesario la configuración de FRR.

No existe un despliegue de ingeniería de tráfico para la optimización de recursos de red, ya sea en forma táctica o estratégica. Se implementa RSVP y Constrained ISIS, de tal forma de construir la base topológica de toda la red para MPLS TE.

2.9 *MULTICAST* [7] [50] [51]

2.9.1 INTRODUCCIÓN

Multicast es un servicio de red en el cual un único flujo de datos, proveniente de una determinada fuente, puede ser enviada simultáneamente para diversos destinatarios. *Multicast* está orientado hacia aplicaciones del tipo "uno a muchos" y "muchos a muchos", en estos casos, *multicast* presenta claras ventajas sobre los mecanismos de transmisión *unicast* y *broadcast*.

- En *unicast*, es necesario que la fuente replique varios flujos de datos idénticos con el objeto de transmitirlos a cada uno de los receptores, generando desperdicio de ancho de banda y recursos.
- En *broadcast* los datos se envían a toda la red de forma indiscriminada, dando como resultado el desperdicio de recursos, ya que esto implica el

transporte de datos para todas las estaciones de la red, aunque el número de receptores que deseen el contenido sea reducido.

- En *multicast*, la fuente de tránsito envía una única copia de los paquetes hacia una dirección de grupo *multicast*. La infraestructura de red replica estos paquetes de forma inteligente, encaminando los datos de acuerdo con la topología de receptores interesados en esa información.

En la figura 2.37 se observa los mecanismos de trasmisión descritos.

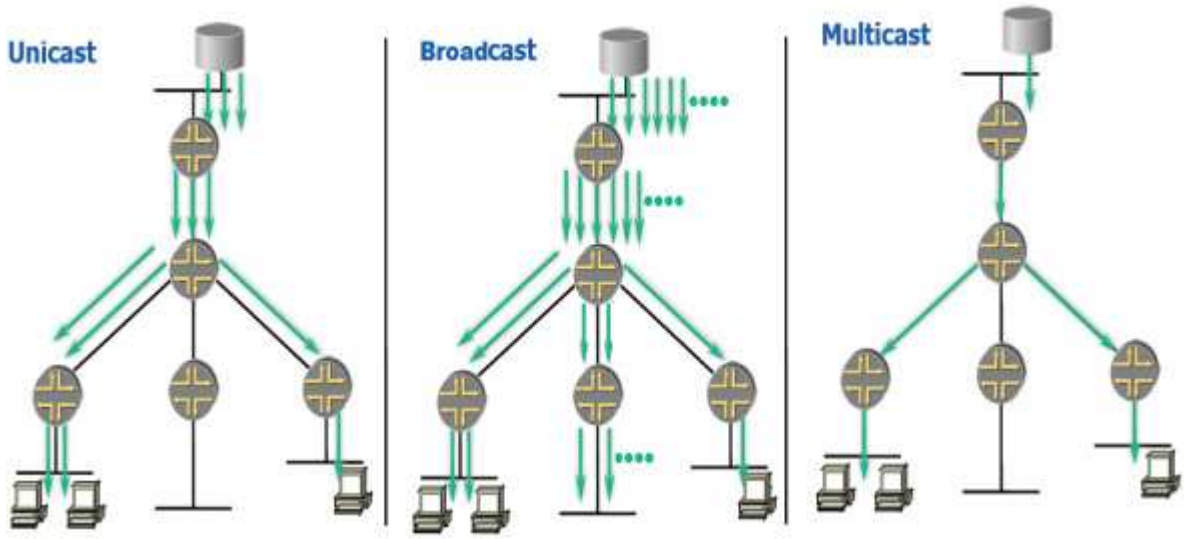


Figura 2.37: Mecanismos de transmisión

2.9.2 GRUPO MULTICAST [50] [51]

Un grupo *Multicast* define un grupo arbitrario de receptores, los cuales desean recibir un *stream* de datos en particular, todo host que requiera unirse a un grupo *multicast* debe hacerlo mediante mensajes IGMP *(Internet Group Management Protocol*). El IANA asignó un grupo de direcciones IP para *multicast* (clase D), donde cada IP simboliza un grupo *multicast*.

Existen una serie de rangos de direcciones dentro de la clase D que se han reservado para fines específicos y que no deberían ser utilizados de otro modo. El más singular de todos ellos es el 224.0.0/24 (que comprende desde la dirección 224.0.0.0 hasta la 224.0.0.255). Este rango está reservado para control en la red local y su ámbito está estrictamente restringido a la red local. Algunos de los rangos se muestran en la tabla 2.7.

Rango	Uso
224.0.0.0/24	Direcciones locales asignadas por la IANA. No propagadas por los routers.
224.0.1.0/24	Direcciones globales asignadas por la IANA. Propagadas por los routers.
224.0.2.0/24 - 224.0.255.0/24	Bloque para asignaciones ad-hoc
224.1.0.0/16	Grupos multicast para Stream Protocol
224.2.0.0/16	Bloque SAP/SDP (MBone)
232.0.0.0/8	Muticast especifico de la fuente (SSM)
233.0.0.0/8	Reservado
239.0.0.0/8	Multicast con ámbito limitado
255.255.255.255/32	Broadcast

Tabla 2.7- Direcciones *multicast* IPv4 reservadas o especiales

2.9.3 IGMP (*INTERNET GROUP MANAGEMENT PROTOCOL*) [50]

El protocolo IGMP se utiliza para mantener los grupos *multicast*, permite que los hosts notifiquen a los routers cuáles son los grupos *multicast* en los que están interesados. Gracias a la información recopilada mediante IGMP los routers mantienen una lista de los grupos *multicast* en los que están interesados los hosts que están conectados a sus interfaces.

Todos los mensajes IGMP se envían con un valor de TTL igual a 1, por lo que los mensajes IGMP solo pueden ser intercambiados entre equipos directamente conectados entre sí (normalmente entre hosts y routers conectados en una misma LAN).

Existen tres versiones de IGMP, v1, v2 y v3. IGMPv1 es un protocolo muy sencillo, puesto que solo implementa dos tipos de mensajes. Los mensajes "*Membership Query"* son emitidos por los routers, su objetivo es preguntar a los hosts en que grupos *multicast* están interesados. Los hosts responden con un mensaje "*Membership Report"*, en el cual informan a los routers de los grupos en los que están interesados. En IGMPv1 no existe un comando que permita a los hosts anunciar cuando abandonan un grupo *multicast*. El abandono es reconocido de forma implícita por los routers cuando el *Query* router ha enviado tres

mensajes '*Membership Query'* sin haber recibido un '*Membership Report'* como respuesta.

Con el ánimo de resolver los problemas que presentaba IGMP v1 se aprobó en 1997 el RFC 2236, que especifica IGMP v2. Las mejoras que presenta IGMP v2 son las siguientes:

- Existe un mensaje nuevo, el "*Leave Group"*, que permite a los hosts indicar de forma explícita cuando abandonan un determinado grupo multicast.
- El comando *Query* tiene ahora dos modalidades: el "*General Query"* (equivalente al Membership Query de IGMP v1) y el "*Group-Specific Query*", que permite a los routers lanzar una pregunta dirigida exclusivamente a los miembros de un grupo *multicast* determinado.

El protocolo IGMP v3 prevé como mejora fundamental la posibilidad de que los hosts indiquen a los routers no solo los grupos *multicast* en que están interesados sino las direcciones de origen de los datagramas que desean recibir.

Para permitir la suscripción selectiva a algunos emisores implementa el comando "*Membership Report"* de IGMP v3, además de indicar el grupo *multicast* en el que está interesado el receptor.

2.9.4 ÁRBOLES DE DISTRIBUCIÓN [51]

Los routers que soportan *multicast* crean "árboles de distribución", los cuales controlan el camino que toman los paquetes IP *multicast* a través de la red para entregar el tráfico a los receptores. Los dos tipos básicos de árboles de distribución IP *multicast* son:

- *Source Tree:* Es un árbol de distribución que tiene como raíz a la fuente emisora y como hojas a los receptores, utiliza el concepto del camino más corto por lo que también es conocido como *Shortest Path Tree (SPT).* La notación utilizada para especificar un host dentro de esta topología es (S,G), donde S indica la fuente y G el grupo, donde se puede decir que

existe un SPT, denotado por el par (S,G) para cada flujo Multicast entre la fuente y el grupo.

- *Shared Tree:* utiliza una única raíz, root denominada *Rendezvous Point* (RP) o *Core*, situada en algún punto de la red, Al utilizar esta topología de distribución, las fuentes envían el tráfico al RP definido por el protocolo IP *Multicast*, y este lo direcciona al grupo IP *Multicast* destino. Debido a que todas las fuentes utilizan la misma raíz, la notación utilizada es (*,G) para indicar un árbol compartido por varias fuentes (*) para el grupo G.

2.9.5 PIM (*PROTOCOL INDEPENDENT MULTICAST*) [50] [51]

El principal problema del *routing multicast* es el descubrimiento mutuo de emisores y receptores. Existen dos estrategias básicas para esto:

- El modo denso. Consiste en difundir los datagramas *multicast* por toda la red y esperar a que los routers que no los deseen lo indiquen explícitamente. Este proceso se conoce como 'podado' del árbol y se realiza mediante mensajes.
- El modo disperso. Consiste en difundir la información únicamente a los routers que previamente la han solicitado. Los routers que deseen adherirse al grupo deben indicarlo mediante una petición explícita (mensajes '*Join'*).

2.10 TRÁFICO EN LA RED MPLS CNT E.P [2]

2.10.1 CONSUMO INTERNET

En la figura 2.38 se puede observa el consumo de tráfico de las salidas internacionales a internet, este es el consumo total de los clientes de CNT E.P. se observa el gran crecimiento que ha tenido en el último año, donde hubo una triplicación en la cantidad de tráfico necesario para satisfacer a los clientes, una de las cosas a tomar en cuenta es que los proveedores de los enlaces han cambiado por eso las variaciones en los gráficos donde cada color representa un enlace.

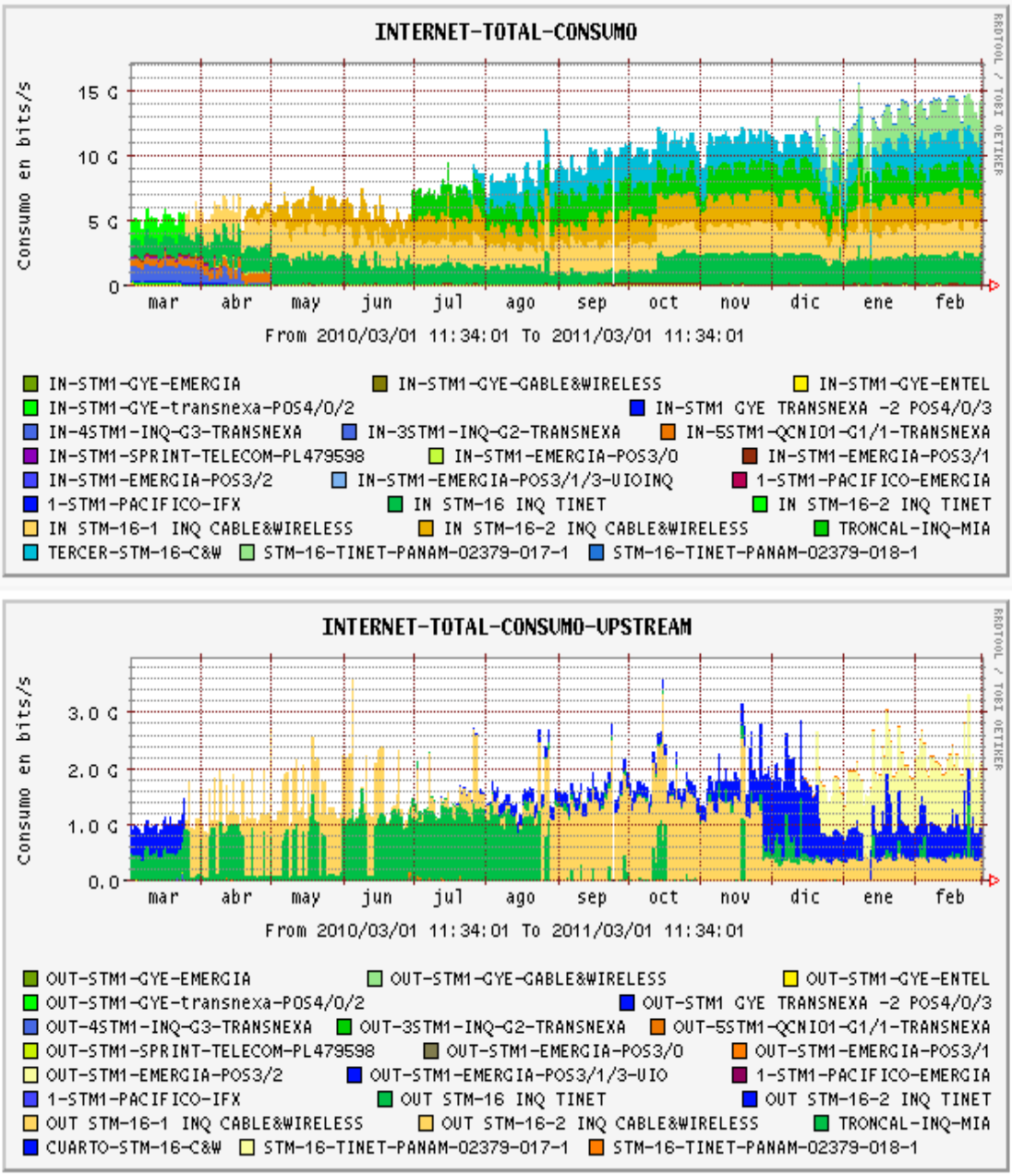


Figura 2.38: Tráfico del crecimiento del último año de las salidas internacionales de CNT E.P. [2]

La capacidad inicial de transmisión de la red fue de 6 Gbps de downstream y 1.5 Gbps de upstream, esta se ha incrementado gradualmente para satisfacer el crecimiento del mercado pues cada vez se tiene un mayor número de clientes que desean internet, cabe recalcar que este incremento ha sido posible gracias a la instalación de equipos de CNT en el NAP de las Américas y a la compra de capacidad de transmisión en los cables submarinos llegando en la actualidad a tener 16Gpbs de upstream y unos 3.6Gbps de downstream.

En la figura 2.39 se observa de manera más detallada el consumo de tráfico de internet de una semana, donde se puede observar que del lunes al jueves el pico de tráfico alcanzado es similar mientras que del viernes al domingo este disminuye, esto se debe al comportamiento de los clientes y a pesar que se puede generar un perfil puede haber días en los que los picos sean diferentes ya que depende del número de clientes conectados así como del tipo de uso que estos le den.

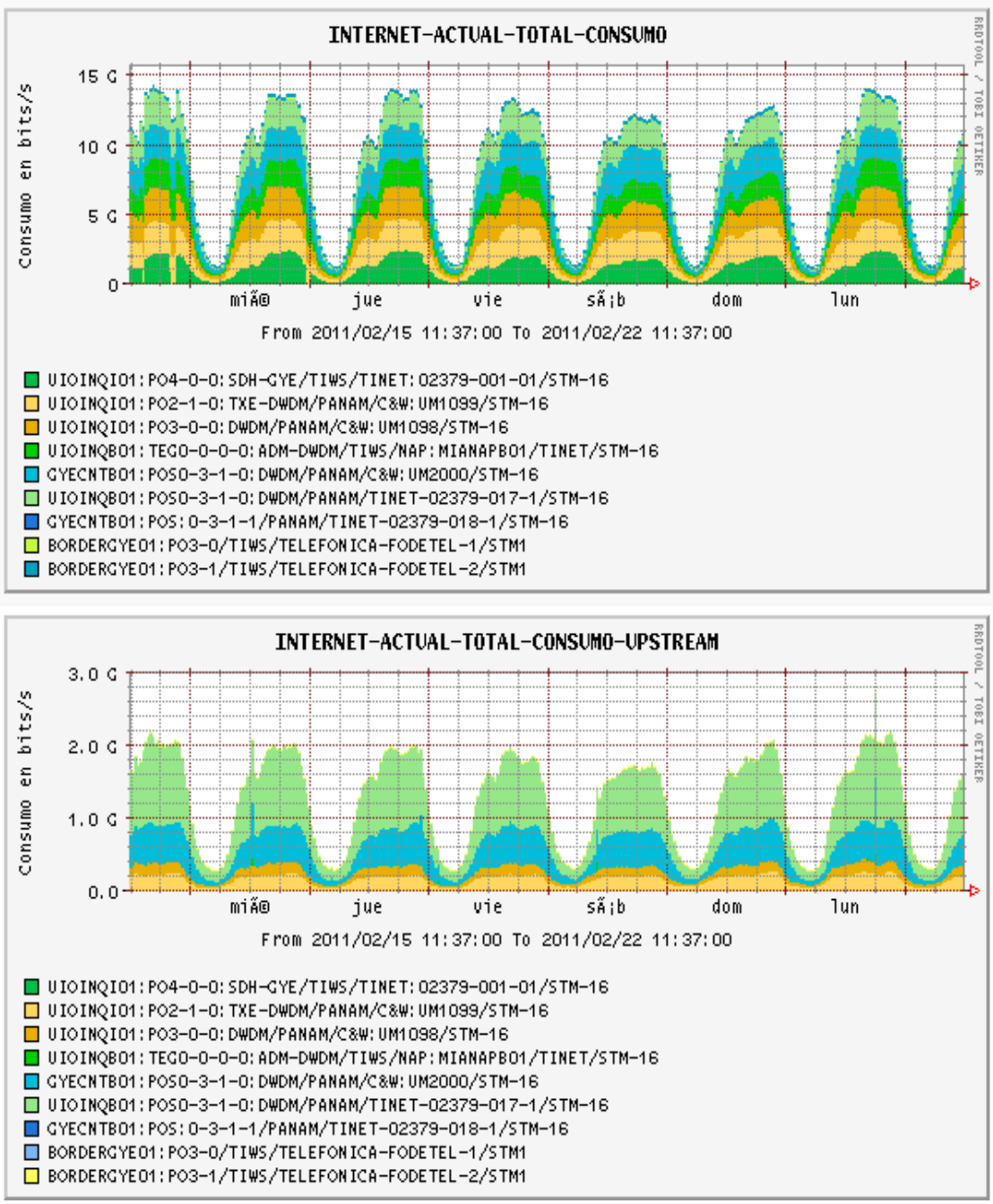


Figura 2.39: Consumo semanal de internet [2]

En la figura 2.40 se observa el tráfico tomado en dos días de la semana, específicamente los días lunes y martes donde se observa que los picos son de los más altos de la semana, se observa las horas de mayo uso que es entre las 11:00 y las 23:00 donde se puede visualizar que los volúmenes de tráfico alcanzan los picos máximos en cambio se observa que las horas de menor consumo son entre las 3:00 y las 7:00, en las otras horas se observa que el nivel de ocupación se incrementa o disminuye según se observa.

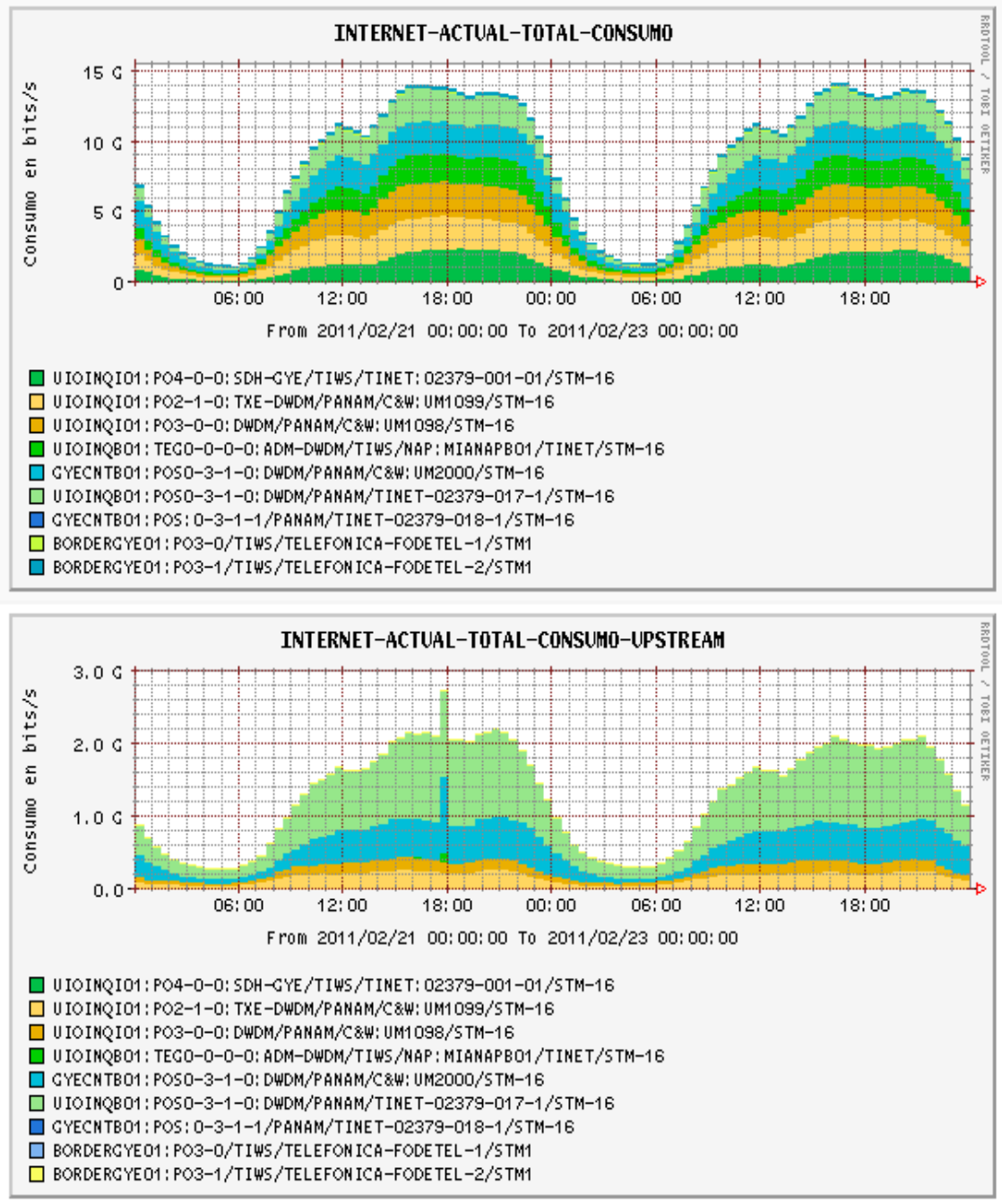


Figura 2.40: Tráfico de los días lunes y martes [2]

En la figura 2.41 en cambio se toman los días sábado y domingo donde se observa una disminución en los picos de tráfico pero que las horas de mayor y menor uso se mantienen similares a las expuestas en lo anterior, la baja en el consumo se debe a que es fin de semana y muchas empresas no realizan actividades.

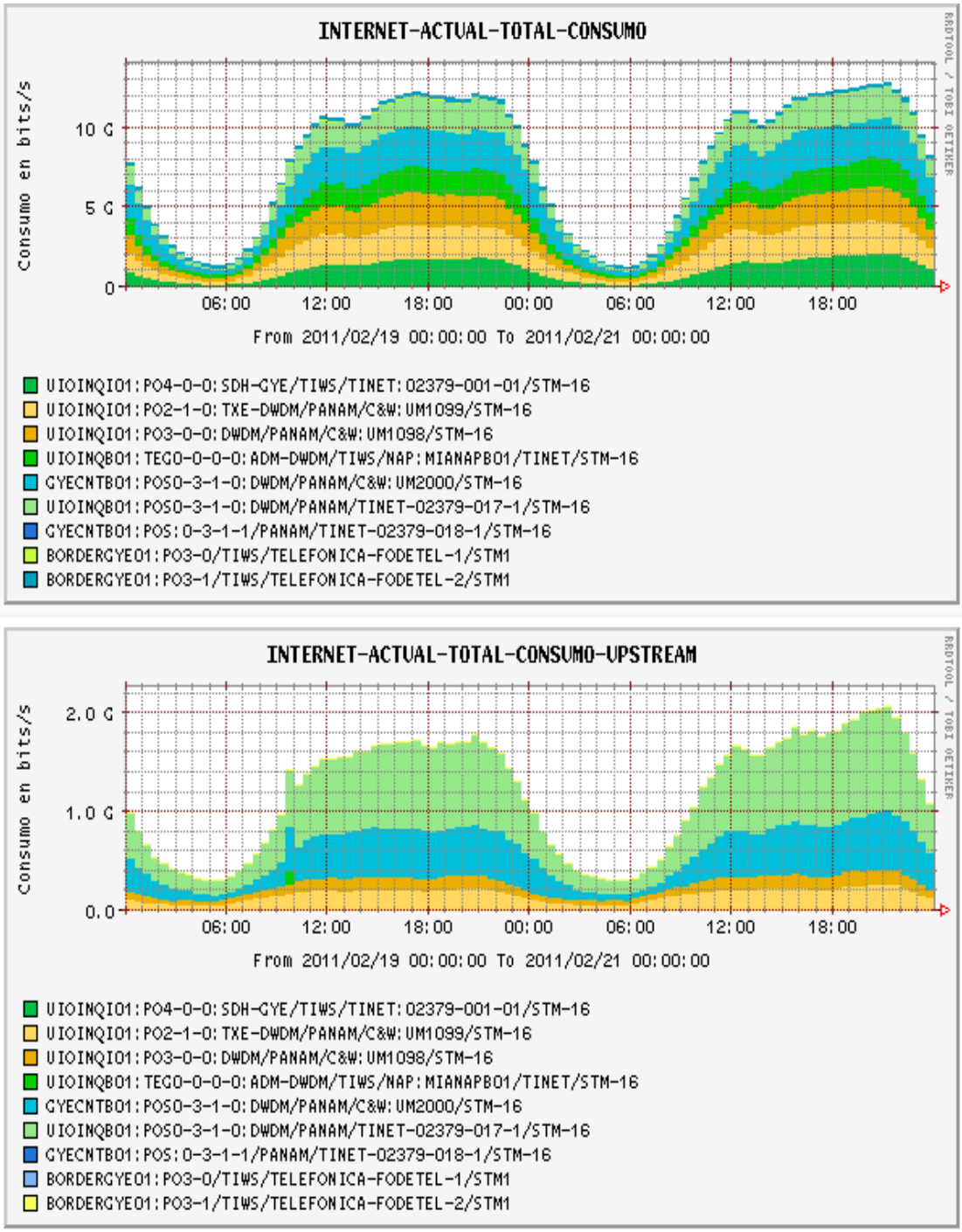


Figura 2.41: Tráfico del fin de semana [2]

2.10.2 DSLAMs

En la figura 2.42 se observan algunos ejemplos de los enlaces que conectan los DSLAM que es la parte de acceso con la red de transporte MPLS, generalmente se usan para ofrecer acceso a clientes residenciales por lo que los picos de transmisión son bastante fluctuantes.

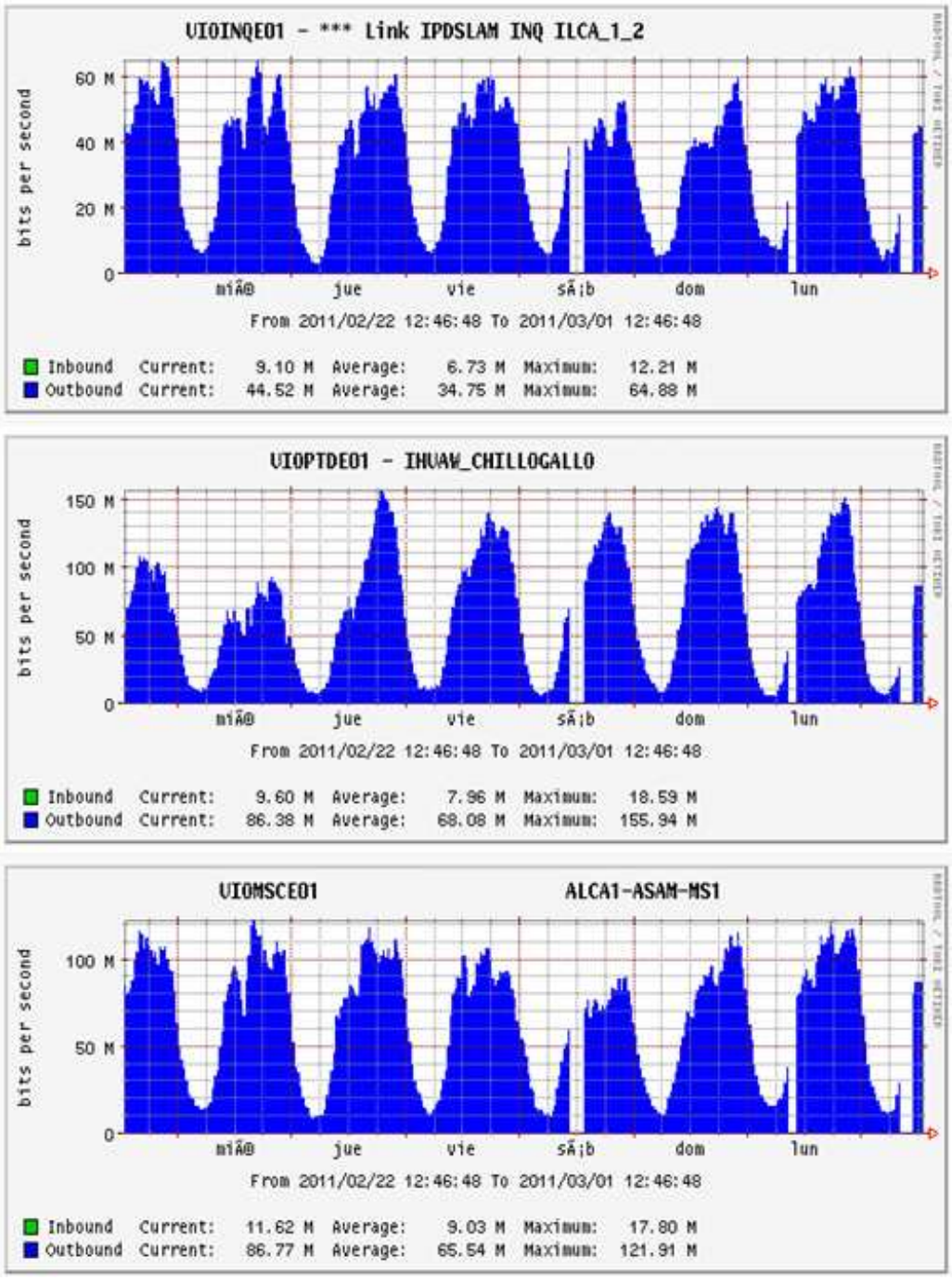


Figura 2.42: Tráfico en los DSLAM [2]

2.10.3 WIMAX

En la figura 2.43 se observa la utilización de los accesos por la tecnología WIMAX se ha tomado de 3 BTS y se monitorea el tráfico entre la BTS y el equipos MPLS al que esta se conecta.

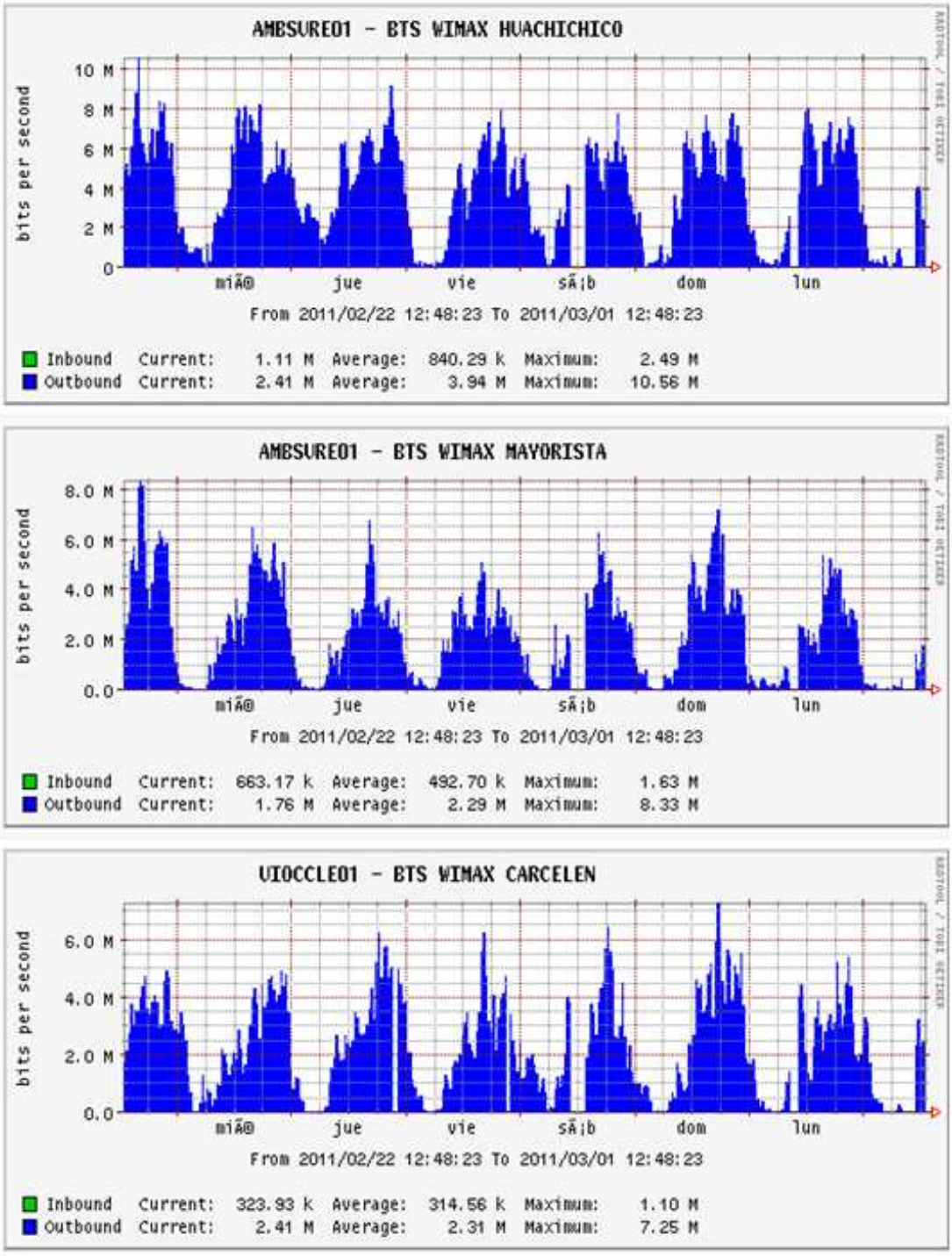
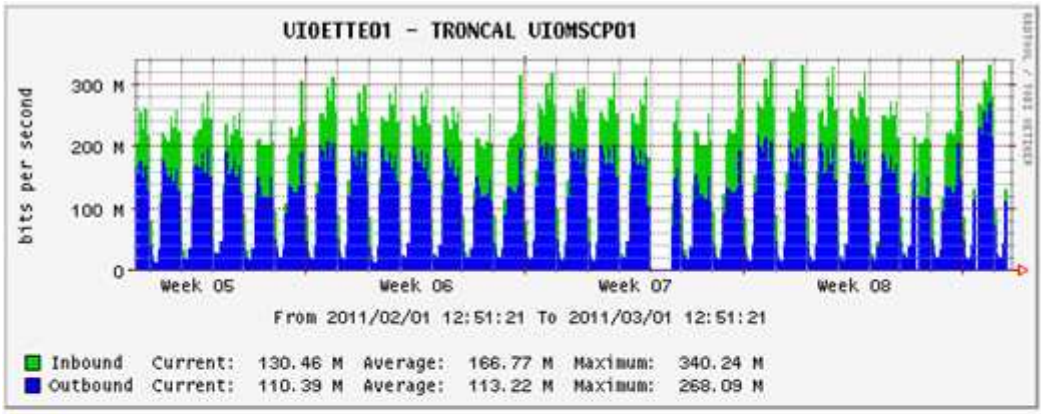
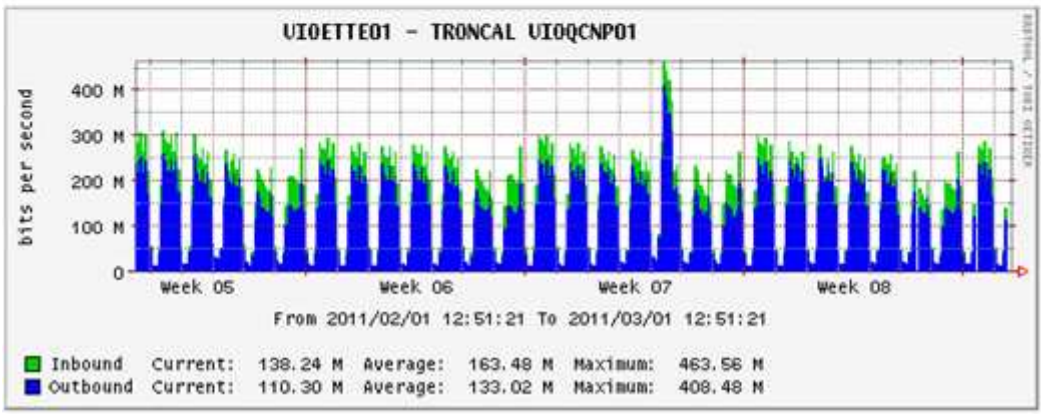


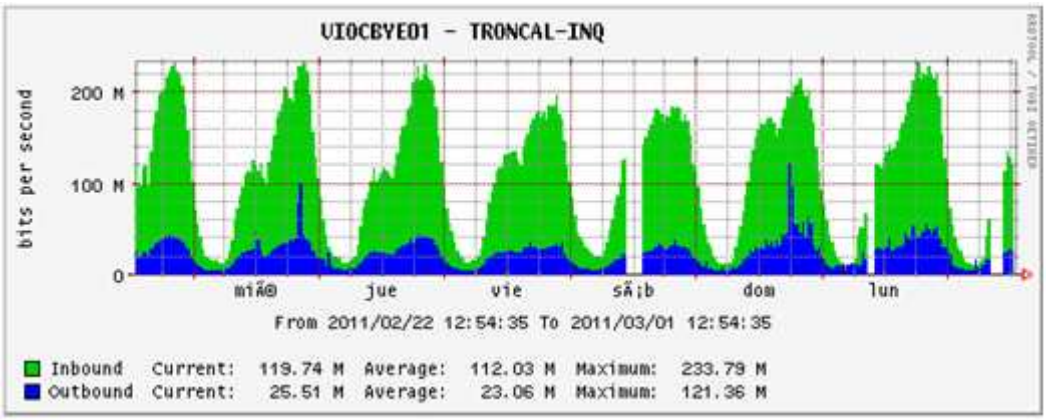
Figura 2.43: Tráfico en las BTS [2]

2.10.4 TRONCALES

En la figura 2.44 se observa la utilización de los enlaces que unen diferentes routers de la red MPLS, los diferentes espacios en blanco en los gráficos son momentos en que los enlaces no se encuentran disponibles pero no implica que estas localidades se quedaron sin servicio pues la red cuenta con alta redundancia, estas fallas pueden ser roturas de las fibras, fallas en las interfaces, fallas de energía y demás inconvenientes que producen fallas.







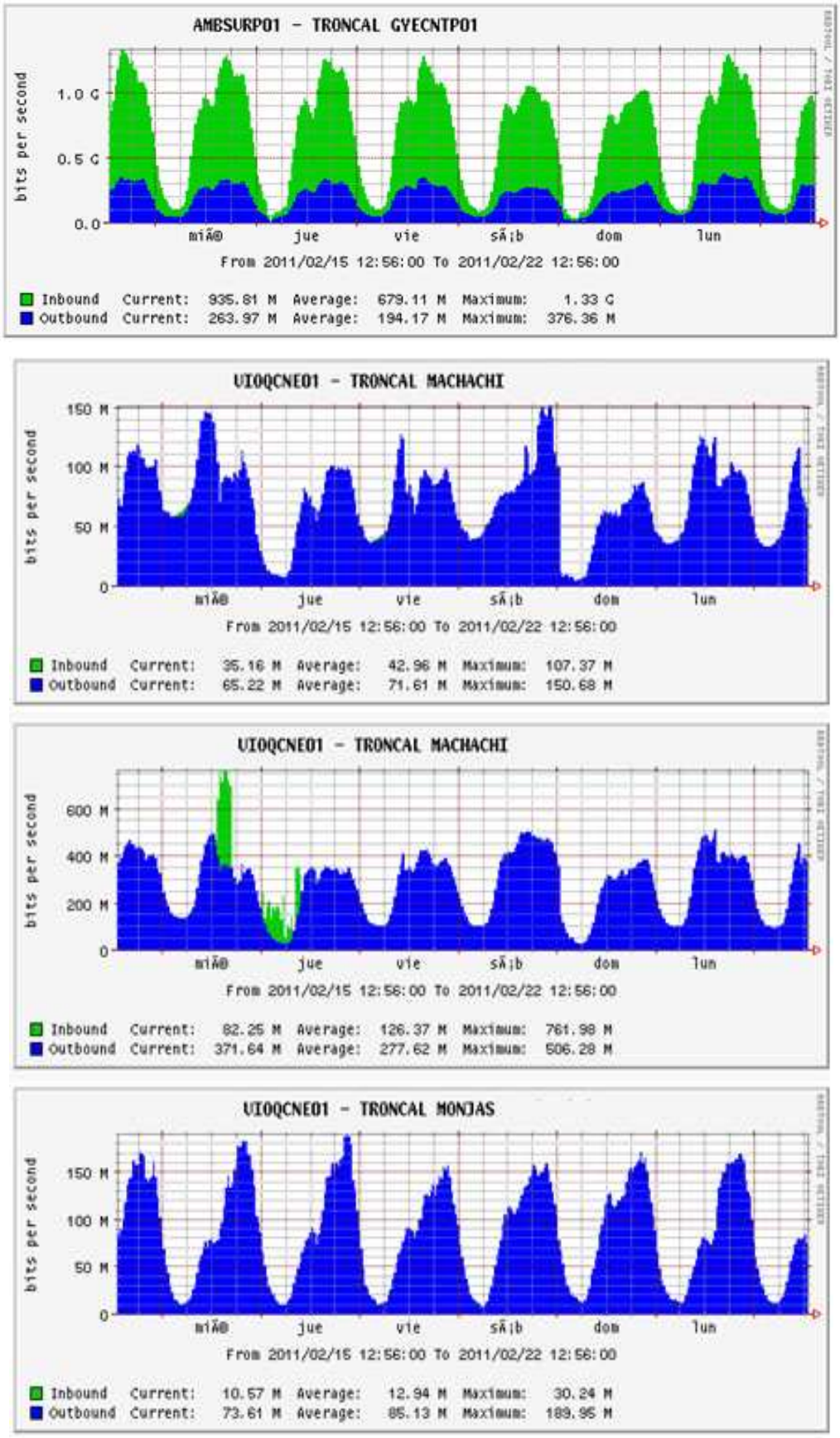


Figura 2.44: Tráfico de las troncales [2]

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO 2

LIBROS

[1] **OPPENHEIMER**, Priscilla. "*Top-Down Network Design*" Cisco Press. 2004.

[2] Información proporcionado por CNT E.P. Gestión ATM-IP/MPLS.

[3] **ALWAYN**, Vivek. "Advanced MPLS design and Implementation". Cisco Press. 2002.

[4] **ALVAREZ**, Santiago. "*QoS for IP/MPLS Networks*". Cisco Press. Junio 2002.

[5] **EVANS**, John; **FILSFIL**, Clarence. "*Deploying IP and MPLS QoS for Multiservice Network*". Morgan Kaufmann. San Francisco. 2007.

[6] **FARREL**; ASH; DAVIE; EVANS. "*Network Quality of Service*". Morgan Kaufmann. Burlington. 2009.

[7] **MORROW**, Monique; **SAYEED**, Azhar. "*MPLS and Next-Generation Networks: Foundations for NGN and Enterprise Virtualization*" Cisco Press, Noviembre 2006.

TESIS

[8] ***LEÓN***, Alejandro. "*Modelado y simulación de transmisión de datos en un ADSL transceiver utilizando LabVIEW*". Universidad de las Américas Puebla. Mayo 2005.

[9] **MENDIETA**, Viviana; **DUARTE**, Sabrina. "*Estudio sobre tecnologías xDSL Digital Subscriber Line*". Universidad Católica "Nuestra Señora de la Asunción" Asunción 2002.

[10] **PROAÑO**, Enrique; **RODRIGUEZ**, Ernesto. "*Análisis comparativo del servicio de internet móvil brindado a través de 3G (UMTS) versus la opción brindada por el anexo "e" del estándar IEEE 802.16 (WiMAX móvil)*" EPN. Marzo 2007.

[11] **NIETO**, Luisiana. "*Diseño y configuración de calidad de servicio en la tecnología MPLS para un proveedor de servicios de internet*". EPN. Mayo 2010.

[12] **CÁRDENAS**, Gonzalo. "*Estudio y diseño de la red que permita la integración de la tecnología de multiplexación DWDM con la técnica de transmisión SDH, para prestar servicios de voz, datos y video, en la Región 2 (enlaces Pichincha – Napo – Orellana) de la Corporación Nacional de Telecomunicaciones CNT S.A*.". EPN. Noviembre 2010.

[13] **FERRO**, Martha. "*Diseño de una Red de Datos Corporativa Basada en Servicios de Telecomunicaciones*". Universidad Pontificia Comillas. Madrid Junio 2007.

[14] **MORALES**, Luis. "*Investigación de Redes VPN con Tecnología MPLS*". Universidad de las Américas Puebla. Mayo 2006.

[15] **SEGARRA**, Ana. "*Estudio de Redes Privadas Virtuales Basadas en la Tecnología MPLS*". ESPE. Diciembre 2009.

PDF, RFC, PAPERS

[16] **BELMONTE**, Pedro. "*La tecnología WIMAX*"
URL: http://www.pedrocores.com/wimax.pdf

[17] **ANÓNIMO**. "*WiMAX y Tecnologías de Acceso BA Inalámbrico (WBA)*"
URL: http://www.robertoares.com.ar/wp-content/uploads/2010/06/
White-Paper-Completo-2008.pdf

[18] **ANÓNIMO**. "*Cisco CRS-1 4-Slot Single-Shelf System*". Cisco System. 2009.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps5763/
product_data_sheet0900aecd804ff54e.pdf

[19] **ANÓNIMO**. "*Cisco CRS 8-Slot Line-Card Chassis Route Processor*". Cisco System. 2009-2010.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps5763/ps6112/
product_data_sheet0900aecd801d53aa.pdf

[20] **ANÓNIMO**. "*Cisco CRS SPA Interface Processor-800*". Cisco System. 2009-2010.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps5763/
product_data_sheet0900aecd80280a68.pdf

[21] **ANÓNIMO**. "*Cisco Cisco XR 12000 Series and Cisco 12000 Series Ruteadores*". Cisco System. 2006.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps167/
product_data_sheet0900aecd800f414a.pdf

[22] **ANÓNIMO**. "*Cisco XR 12000 and 12000 Series Performance Route Processor-2*". Cisco System. 2008.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps167/
product_data_sheet0900aecd800f414a.pdf

[23] **ANÓNIMO**. "*Cisco XR 12000 and 12000 series SPA Interface processor-600*". Cisco System. 2005.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps167/
product_data_sheet0900aecd8028085a.pdf

[24] **ANÓNIMO**. "*Cisco Cisco 1-Port 10 Gigabit Ethernet Shared Port Adapter, Version 2*". Cisco System 2009 - 2010.
URL: http://www.Cisco.com/en/US/prod/collateral/modules/ps6267/ product_data_sheet0900aecd804dc62d.pdf

[25] **ANÓNIMO**. "*Cisco Cisco 2-, 5-, 8-, and 10-Port Gigabit Ethernet Shared Port Adapters, Version 2*". Cisco System 2010.
URL: http://www.Cisco.com/en/US/prod/ collateral/modules/ps6267/ product_data_sheet0900aecd804d884d.pdf

[26] **ANÓNIMO**. "*Cisco ASR 1000 Series Aggregation Services Ruteadores*". Cisco System 2010.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps9343/ data_sheet_c78-447652.pdf

[27] **ANÓNIMO**. "*Cisco ASR 1000 Series Aggregation Services Router Route Processor*". Cisco System 2008 – 2009.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps9343/ data_sheet_c78-441072.pdf

[28] **ANÓNIMO**. "*Cisco ASR 1000 Series Embedded Services Processor*". Cisco System 2010.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps9343/ data_sheet_c78-450070.pdf

[29] **ANÓNIMO**. "*Cisco ASR 1000 Series Shared Port Adapter Support*". Cisco System. 2010.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps9343/ data_sheet_ c78-443175.pdf

[30] **ANÓNIMO**. "*Cisco 2800 Series Integrated Services Ruteadores*". Cisco System. 2010.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps5854/ps5882/ product_data_sheet0900aecd8016fa68.pdf

[31] **ANÓNIMO**. "*Cisco CRS Modular Services Card (LC)*". Cisco System. 2010.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps5763/ps5862/ product_data_sheet09186a008022d5ee.pdf

[32] **ANÓNIMO**. "*Internet Protocol - DARPA Internet Program Protocol Specification*," RFC 791. USC/Information Sciences Institute, September 1981.

[33] **VARIOS AUTORES**. "*RFC 2475: An Architecture for Differentiated Services*". December. 1998.

[34] **ANDERSON, MADSEN**. "*RFC 4026: Provider Provisioned Virtual Private Network (VPN) Terminology*" Marzo 2005.

[35] **DELFINO**, Adrian; **RIVERO**, Sebastian. "*DiffServ: Servicios Diferenciados*".
URL: http://iie.fing.edu.uy/ense/asign/perfredes/trabajos/trabajos_2003/diffserv/Trabajo%20Final.pdf

[36] **ANÓNIMO**. "*Cisco 7609 Chassis". Cisco System 2009*.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps368/ps367/product_data_sheet09186a0080169ead.pdf

[37] **ANÓNIMO**. "*Cisco 7600 Series Ethernet Services Plus 20- and 40-Gbps Line Cards*". Cisco System. 2010.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps368/product_data_sheet0900aecd8057f3b6.pdf

[38] **ANÓNIMO**. "*Cisco 7600 Series Ethernet Services Plus 20- and 40-Gbps Line Cards*". Cisco System. 2010.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps368/data_sheet_c78-49152.pdf

[39] **ANÓNIMO**. "*Cisco ME 6524 Ethernet Switch*". Cisco System 2009.
URL: http://www.Cisco.com/en/US/prod/collateral/switches/ps6568/ps6845/product_at_a_glance0900aecd806c4cc2.pdf

[40] **AHMED**, Abdelhalim. "*IP/MPLS-Based VPNs Layer-3 vs. Layer-2*". Foundry Networks, Inc. 2002

INTERNET

[41] **ANÓNIMO**. "*DSL*".
URL: http://www.bandaancha.es/Informacion/Tecnologias/TecnologiasCableadas/Paginas/ADSL.aspx

[42] **ANÓNIMO**. "*Cisco XR 12000 and 12000 series SPA Interface processor-600*". Cisco System. 2005.
URL: http://www.Cisco.com/en/US/prod/collateral/routers/ps167/product_data_sheet0900aecd8028085a_ps6342_Products_Data_Sheet.html

[43] **ANÓNIMO**. "*Policing and Shaping Overview*".
URL: http://www.Cisco.com/en/US /docs/ios/12_2/qos/configuration/guide/qcfpolsh.html#wpxref26748

[44] **ANÓNIMO**. "*Committed Access Rate*".
URL: http://www.Cisco.com/en/US/docs/ios/ 11_1/feature/guide/CAR.html

[45] **ANÓNIMO**. "*Configuring Generic Traffic Shaping*".
URL: http://www.Cisco.com/en/US/ docs/ios/12_2/qos/configuration/guide/qcfgts.html#wpxref8056012

[46] **ABDELHALI**, Abdelhali. "*IP/MPLS-Based VPNs*" Foundry Networks. 2002.
URL: http://www.brocade.com/downloads/documents/white_papers/wp-ip-mpls-based-vpns.

[47] **ANÓNIMO**, "*Ampliación y Mejoramiento de los Anillos de fibra óptica DWDM*"
URL: http://www.cronica.com.ec/index.php?option=com_content&view=article&id=8243:la-cnt-cumplio-en-el-ano-2009-con-el-pais&catid=38:nacionales&Itemid=53

[48] **ANÓNIMO**, "*CNT Nuestra Tecnología*". Portal CNT E.P 2011.
URL: http://www.cnt.com.ec/index.php?option=com_content&view=article&id=230&Itemid=23

[49] **ANÓNIMO**. "*Cisco 7600 Router*". Cisco System. 2009
URL: http://www.Cisco.com/en/US/products/hw/routers/ps368/index.html

[50] **MONTAÑANA,** Rogelio. "*Multicast*". Departamento de Informática Universidad de Valencia. 2010
URL: http://www.securisite.org/biblioteca/seguridad/Ingenieria%20Telematica-curso/TELE_17-Multicast/amplif_4.pdf

[51] **CICILEO,** Guillermo. "*Multicast Conceptos Básicos*". Walc. 2010
URL: http://www.eslared.net/walcs/walc2010/material/track4/multicast-walc.pdf

CAPÍTULO 3

DISEÑO DEL LABORATORIO DE SERVICIOS IP/MPLS

En este capítulo se define el diseño del sistema de cableado estructurado el mismo que debe ser flexible permitiendo una topología física reconfigurable, para los diferentes esquemas de red. Se realiza los diferentes diseños de esquemas de red, que permitan probar las funcionalidades de los equipos a nivel de enrutamiento, servicios MPLS capa2 y capa3, pruebas de *Multicast*, LDP, IGP, BGP, QoS, *Traffic Engineering*, redistribución de protocolos, pruebas de stress, etc.

CAPÍTULO 3

DISEÑO DEL LABORATORIO DE SERVICIOS IP/MPLS

En este capítulo se procede a realizar los diseños de las distintas topologías, que permitan mostrar los diferentes servicios que se pueden brindar a través de una red IP/MPLS. Se da una explicación de cada uno de los pasos que permiten habilitar los protocolos y funcionalidades, requeridas en cada una de las pruebas.

3.1 SISTEMA DE CABLEADO ESTRUCTURADO [22]

3.1.1 INTRODUCCIÓN

En la actual área de la gestión IP/MPLS ubicada en las instalaciones de “CNT E.P edificio Mariscal” en la que se implementó el Laboratorio de Pruebas, no contaba con un adecuado sistema de cableado estructurado, de acuerdo a las necesidades y requerimientos de los equipos instalados. Por lo cual en esta sección se describe un diseño de la infraestructura de cableado estructurado acorde a dichas necesidades y a posibles cambios o nuevas implementaciones que se den en el cuarto de telecomunicaciones, así como también su fácil administración.

3.1.2 DISEÑO DEL CABLEADO ESTRUCTURADO [22] [8]

El diseño y pruebas del cableado estructurado del laboratorio están ajustados a las normas:

- TIA/EIA-568-C de Cableado de Telecomunicaciones para Edificios Comerciales ("*Commercial Building Wiring Standard*"), incluyendo todas sus partes y *addendums*.
- Estándar TIA/EIA-569 de Rutas y Espacios de Telecomunicaciones para Edificios Comerciales.

- Estándar TIA/EIA-606 de Administración para la Infraestructura de Telecomunicaciones en Edificios Comerciales.
- Estándar TIA/EIA-607 de Requerimientos de Puesta a Tierra y Punteado de Telecomunicaciones para Edificios Comerciales.
- Boletín TIA/EIA TSB-67 de Sistemas Técnicos, Especificaciones de Rendimiento de Transmisión para la Prueba en el Campo de Sistemas de Cableado de Par Trenzado sin Blindaje.
- Boletín TIA/EIA TSB-72 Guía de Cableado de Fibra Óptica.

3.1.2.1 Cableado Horizontal [22]

El cableado horizontal que se contempla es aquel que se extenderá en toda el área del laboratorio, donde el cableado se utilizará para las interconexiones entre los gabinetes de telecomunicaciones, emulado conexiones LAN y WAN, se utilizará *Patch cord* ya sea para fibra óptica mono modo o cable UTP categoría 6A según los requerimientos de conexión de cada equipo.

Las rutas y espacios horizontales que serán utilizados para distribuir el cableado horizontal, utilizarán dos tipos de sistemas, uno para el cableado horizontal que permita el transporte de fibra óptica, el cual se instalará en un ducto plástico amarillo conocido con el nombre de "*fiber runner*" de 4x4", que permite el manejo adecuado de la fibra óptica, dicha instalación contempla todos los accesorios (uniones, curvas planas, TEEs, tapas finales y cobertores) necesarios para completar la ruta. Adicionalmente se requiere de ductos corrugados plásticos para el ingreso de las fibras hacia cada uno de los organizadores verticales, de los gabinetes y racks, de manera que no quede expuesto ningún enlace, el *fiber runner* será instalado de manera aérea colocada con soportes hacia el techo o en su defecto soportes hacia la pared, dependiendo de la ruta elegida, cuya separación del techo al *fiber runner* podría variar entre 30 y 40 cm.

Para el transporte del cableado UTP se utilizará el sistema de escalerillas metálicas, para el caso del laboratorio serán escalerillas modulares de 30 cm de ancho y 2" de alto, su estructura cuenta con protección contra la corrosión y la oxidación, además de quedar integradas al sistema de puesta a tierra regidos, por

la norma ANSI/TIA/EIA-607, todos los soportes quedarán debidamente anclados y nivelados.

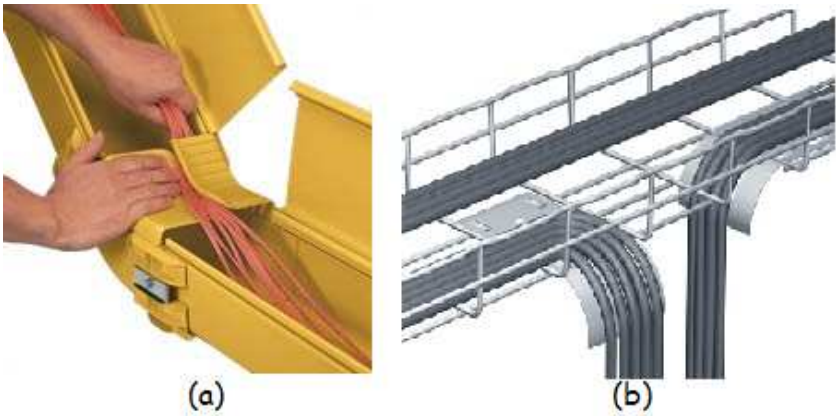


Figura 3.1: a) Fiber Runner, b) Escalerilla metálica. [36] [37]

En los enlaces de fibra óptica se debe contar con un remanente de fibra, de aproximadamente 30 cm, para que se puedan dar cambios sin afectar la longitud y trayectoria de la fibra.

En el caso de los enlaces de cable UTP todas las partes del cableado UTP (incluyendo cables, conectores, terminales, patch-cords, etc.) deben ser Categoría 6A certificada como mínimo, es decir que cumpla con la norma ANSI/TIA/EIA-568-C.2-10, también se recomienda que para sujetar los enlaces de cable se utilizarán amarras tipo *velcro*, ya que este material tiene la capacidad de reutilizarse las veces que sea necesario, la distancia entre cada amarra será de un intervalo de 30 cm en tramos verticales y en horizontales de 100 cm, de igual manera deben de contar con un remanente de cable, de aproximadamente 30 cm, para no afectar su longitud y trayectoria en el caso de que se requiera hacer alguna modificación.

Los *Patch Cord* de fibra óptica serán del tipo mono modo dúplex con terminaciones LC, mientras que los Patch Cord de cobre serán de categoría 6A con terminaciones RJ45 machos, teniendo compatibilidad con las interfaces disponibles en los equipos Cisco

Los recorridos de los *patch cord* dentro de un gabinete de telecomunicaciones serán por medio de los respectivos organizadores horizontales y verticales, y si

éste necesita salir del gabinete deberá utilizar las respectivas canalizaciones de manera que los enlaces no queden expuestos a posibles daños.

3.1.2.2 Cableado Vertical [22] [8]

El propósito del cableado vertical es proporcionar interconexiones entre facilidades de entrada de edificio, cuartos de equipo y cuartos de telecomunicaciones. El cableado del *backbone* incluye la conexión vertical entre pisos en edificios de varios pisos. También incluye medios de transmisión, puntos principales e intermedios de conexión cruzada y terminaciones mecánicas.

Para el caso del cableado vertical del laboratorio, se tiene un enlace de fibra óptica hacia el cuarto de telecomunicaciones principal del edificio, donde se encuentra los equipos de conexión a la nube MPLS de CNT E.P, este enlace fue necesario para realizar la integración del laboratorio a la red MPLS de CNT E.P, el enlace de fibra es mediante un cable de fibra óptica de 24 hilos que a sus extremos en cada uno de los cuartos de telecomunicaciones, su terminación es un ODF (Organizador de Fibras).

3.1.2.3 Cuarto de Telecomunicaciones. [22] [8]

Un cuarto de telecomunicaciones es el área en un edificio utilizada para el uso exclusivo de equipos asociados con el sistema de cableado de telecomunicaciones.

En el caso del laboratorio, el área destinada para su implementación, en un inicio tenía como único propósito ser un área de trabajo, destinada al desarrollo de nuevas configuraciones para optimizar la red IP/MPLS de CNT. Por el limitado espacio físico disponible en el MUX[1] de Mariscal y la necesidad de CNT de instalar nuevos equipos que permitan aumentar la capacidad de su red, se cambio el propósito del área del laboratorio, transformándolo en un cuarto de equipos secundario, del cual forma parte el laboratorio de pruebas. Con lo cual en este

[1] Nombre con el que le conoce al cuarto de telecomunicaciones principal de un punto de presencia de CNT.

espacio no se superarán las distancias máximas a los puestos de trabajo como lo establece la norma EIA/TIA 568-C.

3.1.2.3.1 *Dimensionamiento de Racks*

Para el caso de los Racks para los equipos activos, se utilizarán Racks cerrados, más conocidos como gabinetes los cuales combinan la estética, la seguridad y proporciona una accesibilidad superior para el enrutamiento de cable, un ejemplo del gabinete se muestra en la figura 3.2

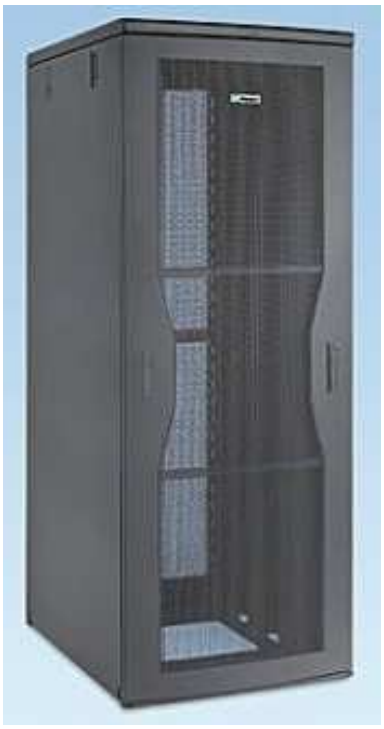


Figura 3.2: Gabinete Panduit. [35]

Cada gabinete está integrado al sistema de puesta a tierra, del cuarto de telecomunicaciones, contará con sus respectivos anclajes de piso, se instalará diferentes accesorios para la protección de los cables y control de los radios de curvatura, de manera que ningún enlace esté desprotegido, además de los organizadores verticales para ordenar los cables eléctricos de las fuentes de poder.

Para organizar los diferentes equipos de prueba, se han establecido la ubicación de tres gabinetes, la distribución del primer gabinete se muestra en las figuras 3.3.

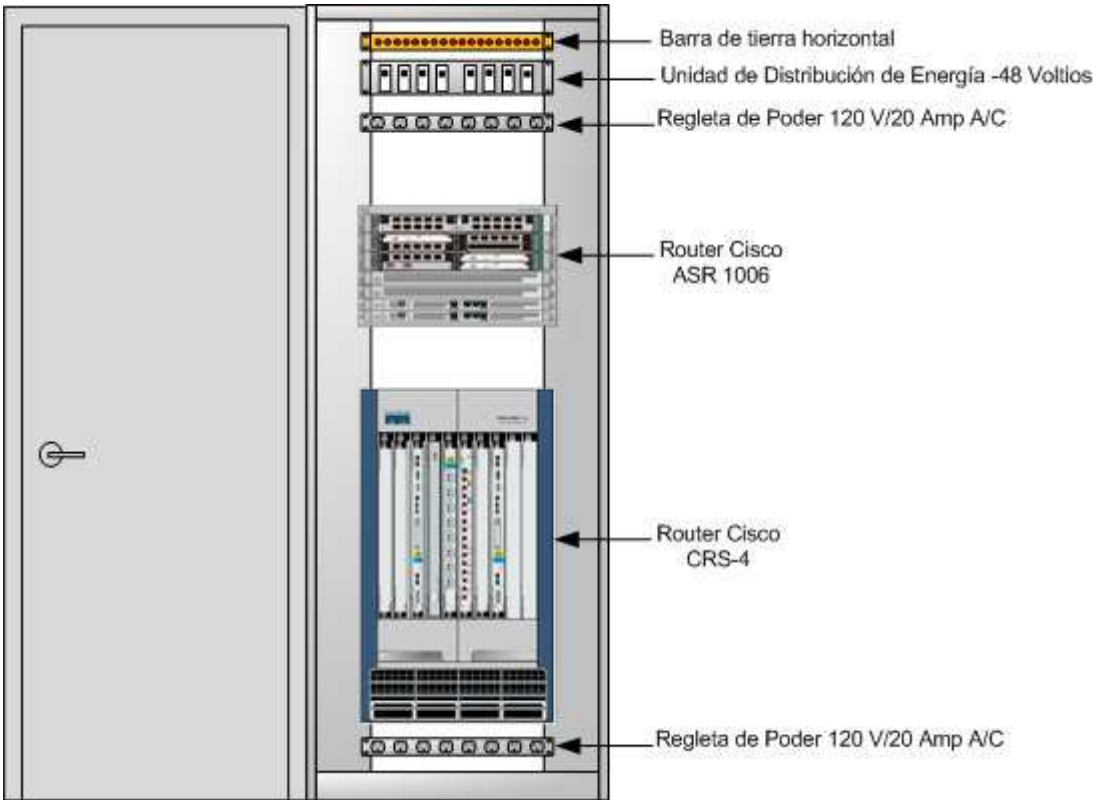


Figura 3.3: Distribución de Equipos en el Gabinete Nº 1

Dentro del gabinete N° 1 tenemos dos equipos un Router Cisco CRS-4 y un ASR1006 los elementos que integran cada uno de estos se detallan a continuación. En la tabla 3.1 se detallan los elementos de ARS1006.

Parte	Descripción	Cantidad
ASR 1006	Cisco ASR1006 Chassis, Dual P/S	1
ASR1000-SPA	SPA for ASR1000; No Physical Part; For Tracking Only	1
ASR1000-RP2	Cisco ASR1000 Route Processor 2, 8GB DRAM	1
ASR1000-SIP10	Cisco ASR1000 SPA Interface Processor 10	1
M-ASR1K-RP2-8GB	Cisco ASR1000 RP2 8GB DRAM	1
M-ASR1K-HDD-80GB	Cisco ASR1000 RP2 80GB HDD	1
ASR1006-PWR-DC	Cisco ASR1006 DC Power Supply	2
SFP-GE-L	1000BASE-LX/LH SFP (DOM)	1
ASR1000-ESP20	Cisco ASR1000 Embedded Services Processor, 20G,Crypto	1
SPA-2X1GE-V2	Cisco 2-Port Gigabit Ethernet Shared Port Adapter	1
SASR1R2-AISK9-23SR	Cisco ASR 1000 Series RP2 ADVANCED IP SERVICES	1

Tabla 3.1- Elementos del ASR1006.

En la tabla 3.2 Se detallan los elementos que conforman el equipo de core Cisco CRS-4 ubicado en el gabinete N° 1.

Parte	Descripción	Cantidad
CRS-4/S	Cisco CRS-1 Series 4 Slots Carrier Routing System	1
GLC-LH-SM	GE SFP, LC connector LX/LH transceiver	4
CRS-4-DC-PIM	Cisco CRS-1 Series 4 Slot DC Power Input Module	1
CRS-4-DC-INPUT	Cisco CRS-1 Series 4 Slot DC Input Shelf	1
CRS-4-DC-SUPPLY	Cisco CRS-1 Series DC Supply for CRS-4	1
CRS-4-FAN-TR	Cisco CRS-1 Series Fan Tray for CRS-4	1
CRS-4-FC	Cisco CRS-1 Series Fabric Card for CRS-4	4
CRS-4-CH	Cisco CRS-1 Series 4 Slots Chassis	1
CRS-4-DOOR-KIT	CRS-1 4 Slot System Door Kit	1
XC-RP-03.08	Cisco IOS XR IP/MPLS Core Software	1
CRS-FLASH-DISK-2G	CRS-1 2GB Flash Disk	1
CRS-4-DC-KIT	CRS-1 4 Slot System DC Kit	1
CRS-8-RP	Cisco CRS-1 Series 8 Slots Route Processor	1
4-10GE=	Cisco CRS-1 Series 4X10GE Interface Module	1
CRS-MSC-40G-B=	Cisco CRS-1 Series Modular Services Card revision B 40G	1
CRS-MSC-B	Cisco CRS-1 Modular Services Card Rev B	2
XENPAK-10GB-LR+	GBASE-LR XENPAK Module with DOM support	2
20-1GE-FLEX=	Cisco CRS-1 Series 20X1GE Flexible Interface Module	1
XC-LC40G	Cisco CRS-1 Series MSC 40G license	2
SFP-GE-L	1000BASE-LX/LH SFP (DOM)	6

Tabla 3.2- Elementos del Cisco CRS-4

En la figura 3.4 se muestra la distribución del los diferentes elementos que conforman el gabinete N° 2, donde se encuentra el Router Cisco 12000.

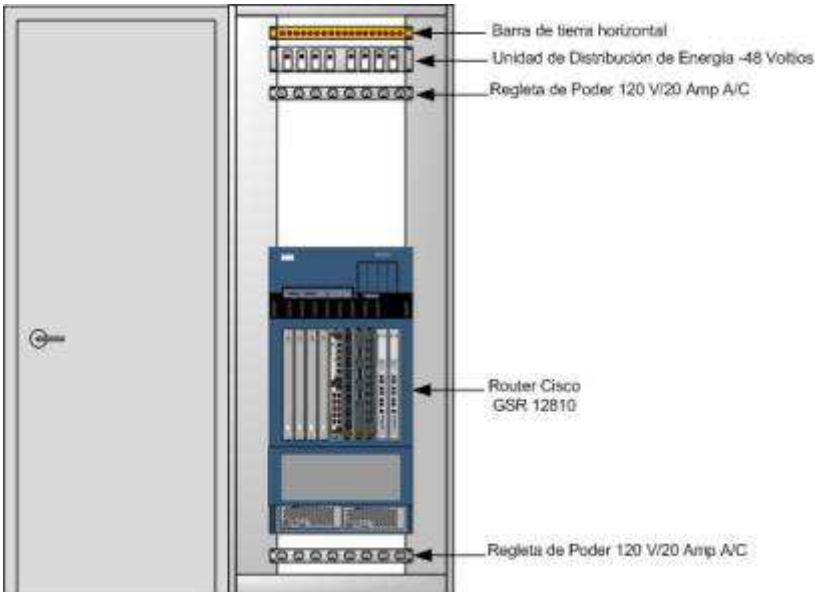


Figura 3.4: Distribución de Equipos en el Gabinete Nº 2

En la tabla 3.3 Se detallan los elementos que conforman el equipo de Distribución tipo A Cisco 12000 ubicado en el gabinete Nº 2.

Parte	Descripción	Cantidad
12000/10-DC	Cisco 12000 10-slot; 2Alarm, Blower, 2DC	1
XR-MEN-PRP2-2G	Cisco XR 12000 PRP-2 2Gig DRAM Option	1
12810E-CSC	12810 800Gbps Enhanced Clock Scheduler Card	2
FLASH-2G	Cisco 2GB Flash Memory Option	1
12000-SPA	SPA for Cisco 12000; No Physical Part; For Tracking Only	1
MEM-PRP2-2G	2GB Memory - (1x2GB DIMM) Configuration	1
MEM-FD2G	Cisco 2GB PC ATA Flash Disk	1
12000/10-BEZEL	Cisco 12000 10-slot Enhanced Bezel	1
PRP-2	Cisco 12000 Performance Router Processor 2 (PRP-2)	1
12000-SIP-601	Multirate 10G IP Services Engines (Modular)	3
SPA-10X1GE-V2	Cisco 10-Port Gigabit Ethernet Shared Port Adapter	1
SPA-1X10GE-L-V2	Cisco 1-Port 10GE LAN-PHY Shared Port Adapter	4
XR-XR12KK9-03.06	Cisco IOS XR IP/MPLS Core Software 3DES	1
SFP-GE-L	1000BASE-LX/LH SFP (DOM)	5
XFP-10GLR-OC192SR	Multirate XFP module for 10GBASE-LR and OC192 SR-1	4

Tabla 3.3- Elementos del Cisco 12000.

En la figura 3.5 se muestra la distribución del los diferentes elementos que conforman el gabinete N° 3.

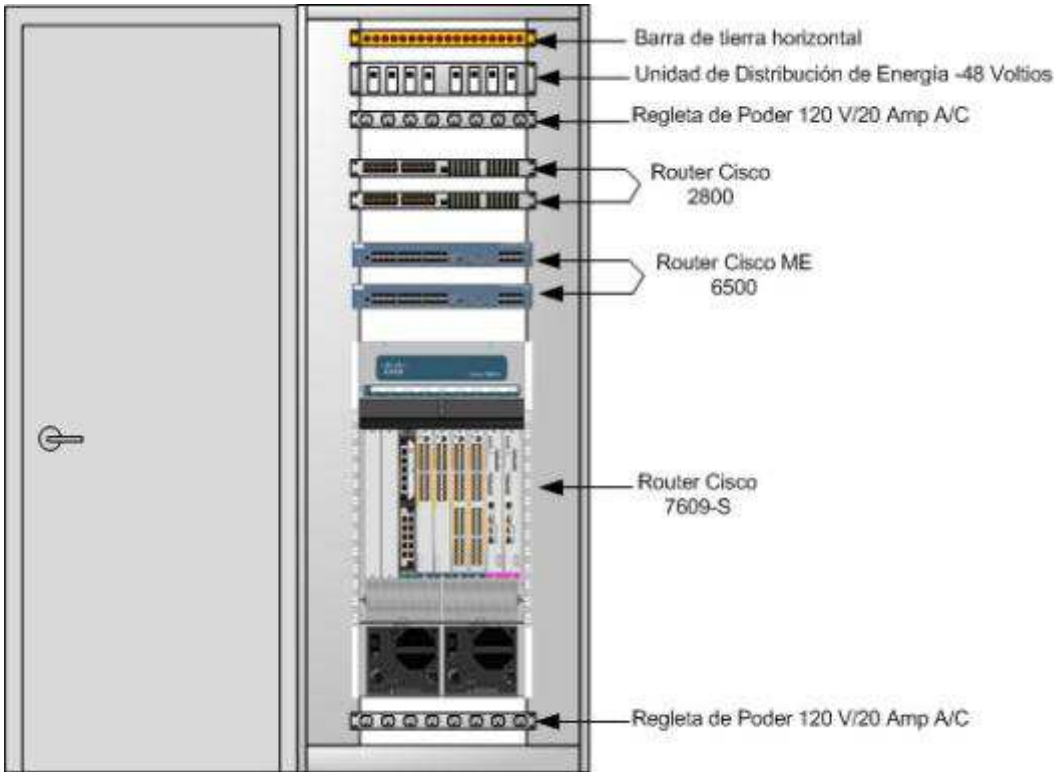


Figura 3.5: Distribución de Equipos en el Gabinete Nº 3

En la tabla 3.4 Se detallan los elementos que conforman el equipo de acceso tipo C Cisco Me 6500 ubicado en el gabinete N° 3.

Parte	Descripción	Cantidad
ME-C6524GS-8S	Cisco ME6524 Switch - 24 GE SFP + 8GE SFP, Fan tray	1
MEM-C6K-CPTFL512M	Catalyst 6500 Sup720/Sup32 Compact Flash Mem 512MB	1
GLC-LH-SM=	GE SFP,LC connector LX/LH transceiver	12
GLC-T=	1000 BASE-T SFP	10
S523AIK9N-12233SXI	Cisco ME 6524 IOS ADV IP SERV SSH LAN ONLY (MODULAR)	1
MEM-MSFC3-1GB	1GB Mem for Sup720, Sup720-3B and MSFC2A	1
PWR-400W-DC	400W DC PS for Cisco ME6524 Switches	1

Tabla 3.4- Elementos del Cisco Me 6500.

En la tabla 3.5 Se detallan los elementos que conforman el equipo de Distribución tipo B Cisco 7600 ubicado en el gabinete N° 3.

Parte	Descripción	Cantidad
CISCO7609-S	Cisco 7609-S Chassis including fans	1
MEM-XCEF720-1GB	Catalyst 6500 1GB DDR, xCEF720 (67xx interface, DFC3BXL)	1
PWR-6000-DC	6000W DC Power Suply for Cisco7609/7609S/7613	1
RSP720-3CXL-GE	Cisco 7600 Route Switch Processor 720Gbps fabric,PFC3CXL, GE	1
MEM-RSP720-CF256M	C7600 RSP720 Compact Flash Memory	2
S764AIK9-12233SRD	Cisco 7600-RSP720 IOS ADVANCED IP SERVICES SSH	1
7600-ES+20G3CXL	7600 ES+ Line Card, 20xGE SFP with DFC 3CXL	2
SFP-GE-L	1000BASE-LX/LH SFP (DOM)	24
7600-ES+2TG3CXL	7600 ES+ Line Card, 2x10GE XFP with DFC 3CXL	1
XFP-10GLR-OC192SR	Multirate XFP module for 10GBASE-LR and OC192 SR-1	1
76-ES+ADVIP-20G	ES+ 20G Adv License, with MVPN, IPv6, 6vPE, L3 IP/MPLS VPN	3
WS-X6748-GE-TX	Cat6500 48-port 10/100/1000 GE Mod: fabric enabled, RJ-45	1
WS-F6700-DFC3CXL	Catalyst 6500 Dist Fwd Card- 3CXL, for WS-X67xx	1

Tabla 3.5- Elementos del Cisco 7600.

En la tabla 3.6 Se detallan los elementos que conforman el equipo de acceso tipo B Cisco Me 6500 ubicado en el gabinete N° 3. Este equipo a pesar de tener similares características que el acceso tipo C, el tipo de puertos eléctricos con el que cuenta los diferencia.

Parte	Descripción	Cantidad
ME-C6524GT-8S	Cisco ME6524 Switch - 24 10/100/1000 + 8GE SFP, Fan tray	1
MEM-C6K-CPTFL512M	Catalyst 6500 Sup720/Sup32 Compact Flash Mem 512MB	1
MEM-MSFC2-512MB	Catalyst 6500 512MB DRAM on the MSFC2 or SUP720 MSFC3	1
GLC-LH-SM=	GE SFP,LC connector LX/LH transceiver	2
S523AIK9N-12233SXI	Cisco ME 6524 IOS ADV IP SERV SSH LAN ONLY (MODULAR)	1
PWR-400W-DC	400W DC PS for Cisco ME6524 Switches	1

Tabla 3.6- Elementos del Cisco Me 6500 con puertos eléctricos.

En la tabla 3.7 Se detallan los elementos que conforman los equipos que simularan las localices del cliente ubicados en el gabinete N° 3.

Parte	Descripción	Cantidad
CISCO2811-ADSL2/K9	2811 bundle, HWIC-1ADSL, SP Svcs, 64FL/256DR	2
S28NSPSK9-12415T	Cisco 2800 SP SERVICES	2
MEM2800-64CF-INC	64MB CF default for Cisco 2800 Series	2
PWR-2811-AC	Cisco 2811 AC power supply	2
ROUTER-SDM-CD	CD for SDM software	2
ACS-2811-STAN	Cisco 2811 Standard Accessory Kit	2
HWIC-1ADSL	1-port ADSLoPOTS HWIC	2
CAB-SS-V35MT	V.35 Cable, DTE Male to Smart Serial, 10 Feet	8
WIC-2T	2-Port Serial WAN Interface Card	2
WIC-2T	2-Port Serial WAN Interface Card	2
PVDM2-16	16-Channel Packet Voice/Fax DSP Module	2
HWIC-1ADSL	1-port ADSLoPOTS HWIC	2

Tabla 3.7- Elementos del Cisco 2800.

A continuación en la figura 3.6 se muestra la distribución de las áreas y racks que se encuentran en la sala de equipos, conjuntamente con el sistema de cableado estructurado existente.

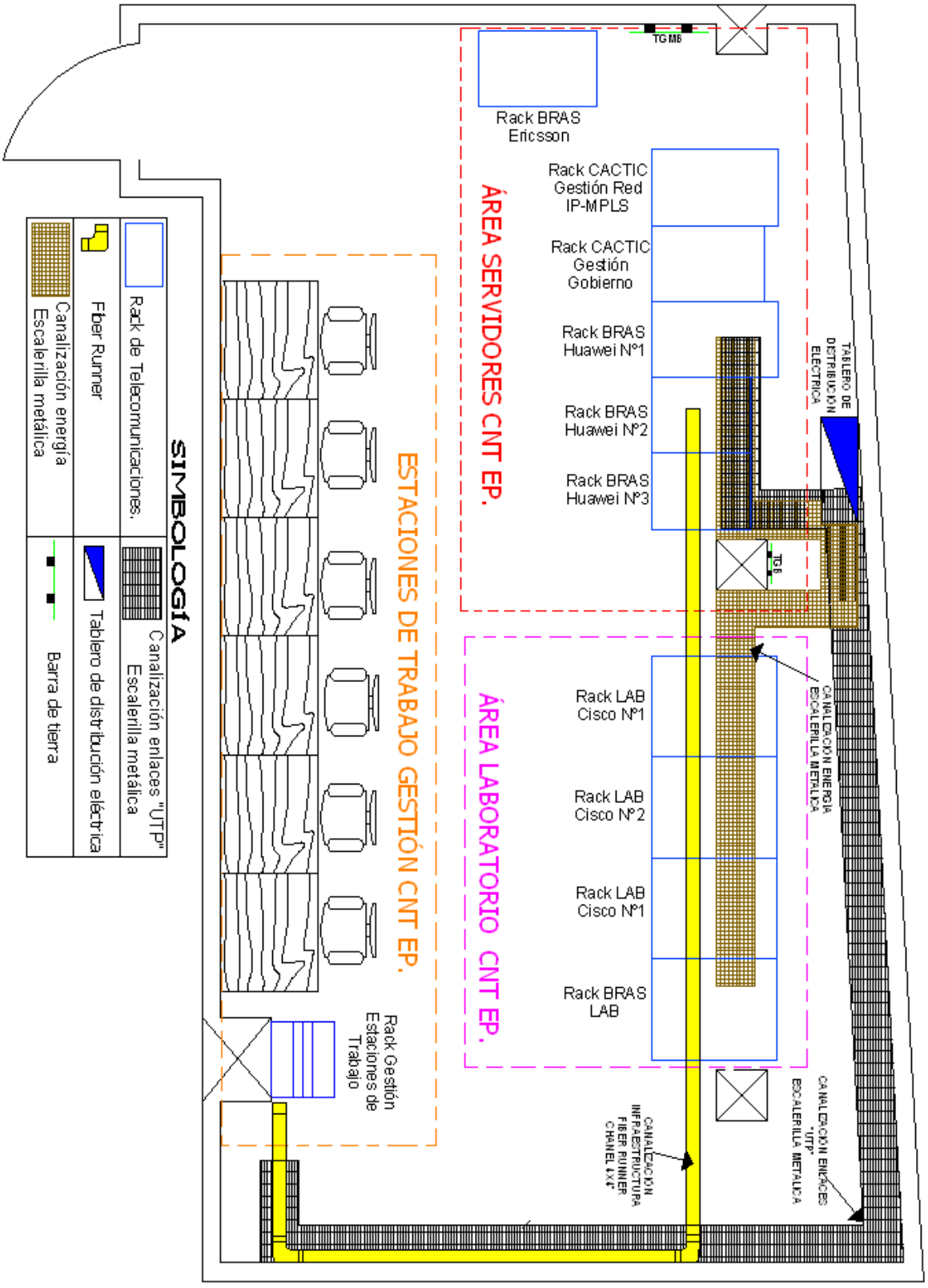


Figura 3.6: Diagrama de distribución de los Equipos

3.1.2.4 Sistema Eléctrico [22] [8]

3.1.2.4.1 *Cableado de Energía*

El sistema eléctrico es el que suministrará la energía a los equipos activos mediante un voltaje de -48 voltios DC (corriente directa), el montaje de las acometidas se realizará en una caja eléctrica contra corto circuitos, con las debidas protecciones en el gabinete para equipos activos.

Los colores para identificar cada una de las líneas de energía son los siguientes colores:

- ROJO para (+) positivo.
- NEGRO O AZUL para (-) negativo.
- VERDE / AMARILLO para la tierra.

Todas las acometidas cuentan con su respectiva canalización de manera que el cable no sea afectado por un agente externo, ni afecte este a los enlaces de telecomunicaciones, el cableado eléctrico también irá montado sobre una escalerilla metálica similar a la de cable UTP, todos los cables serán agrupados y sujetados de manera que estén fijos a la escalerilla, evitando el movimiento.

Las acometidas eléctricas estarán a una distancia mínima de 30 cm de las canalizaciones de cable de cobre UTP para evitar la interferencia electromagnética.

Se instala un circuito de 20 amperios con una salida de toma corriente doble polarizado, para la conexión de la regleta de poder (120 voltios, 20 amperios) que se ubicará en el gabinete de equipo activo, se establece esta capacidad de corriente debido a que en esta regleta se prevee la conexión de equipos de gestión y prueba como los generadores de trafico IXIA y laptops para la configuración de los equipos.

Considerando que tanto los IXIAs como las laptops son PCs que tienen un consumo de potencia de 250 watts promedio por cada y asumiendo una situación crítica, en la cual se ocupen todas las tomas de la regleta el consumo total sería

2000 watts lo que demandaría que la corriente soportada por el circuito sea de 16,67 A con un voltaje de 120 V. Por lo que para asegurar esta corriente y tener un margen de demanda de corriente se estableció un circuito de 20 amperios.

3.1.2.4.2 *Puesta a Tierra*

El sistema de puesta a tierra integra todo el sistema de infraestructura:

- Canalizaciones de infraestructura cable UTP.
- Canalización eléctrica.
- Gabinetes de telecomunicaciones.
- Fuentes de poder para los equipos activos.
- Chasis de los equipos activos

Se instala una barra de tierra tipo TGB[2] en los gabinetes para la ampliación de la conectividad a tierra, y estas se integrarán a la barra de tierras TMGB[3] del edificio, las mediciones en el sistema de tierras entregado debe ser menor al valor de los 5 Ω (ohmios).

En el anexo 2 se realiza un estudio de la situación actual de la sala de equipos, en la que se encuentra el laboratorio. Luego del cual se establecerán unas recomendaciones para mejorar el ambiente del cuarto de telecomunicaciones.

3.2 DISEÑOS Y CONFIGURACIONES DE LOS ESQUEMAS DE RED PARA PROBAR PROTOCOLOS Y SERVICIOS UTILIZADOS EN UNA RED IP-MPLS

En esta parte se procede a describir los escenarios que se crearon para probar los diferentes protocolos y servicios, necesarios para el adecuado funcionamiento de una red de transporte MPLS, de un proveedor de servicios, utilizando los equipos disponibles en el laboratorio descritos en el capítulo 2, se detallan los

[2] *Telecommunications grounding Busbar* Es la barra de puesta a tierra para telecomunicaciones donde se conectan los diferentes equipos.
[3] *Telecommunications* main *grounding Busbar.* Barra colectora principal para aterrizaje de telecomunicaciones a esta se conectan las TGB.

pasos a seguir para una adecuada configuración, sintaxis y semántica de los diferentes comandos.

3.2.1 SIMULACIÓN DE UN BACKBONE MPLS [9] [10]

La creciente necesidad de reducir costos, aumentar la productividad, soportar más aplicaciones y elevar la seguridad hace de MPLS (*Multi-Protocol Label Switching*) una alternativa de mayor alcance dentro de un ambiente WAN.

La capacidad de MPLS para integrar voz, vídeo y datos en una plataforma común con garantías de calidad de servicio (QoS), sumado a las mejoras del rendimiento y la disponibilidad que se obtienen con esta tecnología, así como su soporte de una amplia y escalable gama de servicios (VPNs, Multicast, etc) y la ingeniería de tráfico con la precisión e inteligencia del encaminamiento basado en MPLS, permiten empaquetar más datos en el ancho de banda disponible y reducir los requerimientos de procesamiento a nivel de router. Se trata, pues, de una tecnología de red efectiva en costos, rápida y altamente escalable.

Por lo que a continuación se procede al diseño de un esquema de prueba que permita simular los principales componentes de una red de transporte MPLS de un ISP.

3.2.1.1 Objetivo

En la prueba se desea poner en funcionamiento un backbone MPLS básico, para verificar el establecimiento de los LSP, la asignación, distribución, operación y manipulación de las etiquetas.

Se realiza una explicación de cómo habilitar un backbone MPLS, en un escenario de prueba, partiendo de una red IP genérica utilizando ISIS como IGP y LDP como el protocolo de distribución de etiquetas, para de esta forma tener preparado el backbone de red y poder empezar a configurar servicios utilizados en la red de un proveedor de servicios.

3.2.1.2 Esquema de Red para la Simulación de un Backbone MPLS [1] [2] [14] [15] [9] [10]

3.2.1.2.1 *Consideraciones del escenario de Pruebas*

El esquema de prueba que se diseña debe cumplir con las siguientes consideraciones:

- Se han dispuesto de cuatro routers “PE1, P1, P2 y PE2”, los cuales forman una topología común de un *backbone* de infraestructura MPLS
- Cada PE router se interconectará con un router de core “P”, además se interconectará los routers P, todos con un enlace GigabitEthernet.
- Habilitar el reenvío MPLS sobre las interfaces que interconectan PE routers con P routers y entre P routers.
- Se utiliza como protocolo de enrutamiento interno (IGP) IS-IS para la distribución de rutas.
- Se utiliza LDP como el protocolo de distribución de etiquetas.

En la topología de prueba, se utilizan dos elementos fundamentales que son parte del *backbone* MPLS en una red de *Service Provider,* en donde los routers “P1 y P2” cumplen con las funciones de Routers de conmutación de etiquetas “LSR”, mientras que los routers “PE1 y PE2” cumplen con las funciones de routers de borde “LER”.

Se colocan dos routers de frontera (PEs) con la finalidad de simular dos POP (puntos de presencia) del proveedor de servicios, ubicados remotamente, para comprobar la conformación de los LSP, que son los encargados de transportar la información de los usuarios de extremo a extremo.

Se dispuso de dos routers Ps, con la finalidad de verificar la asignación de etiquetas dentro del backbone, y observar las operaciones (pop, swap), que los routers LSR realizan basados en la información obtenida de las etiquetas.

La topología de red diseñada para probar estas características descritas se muestra en la figura 3.7.

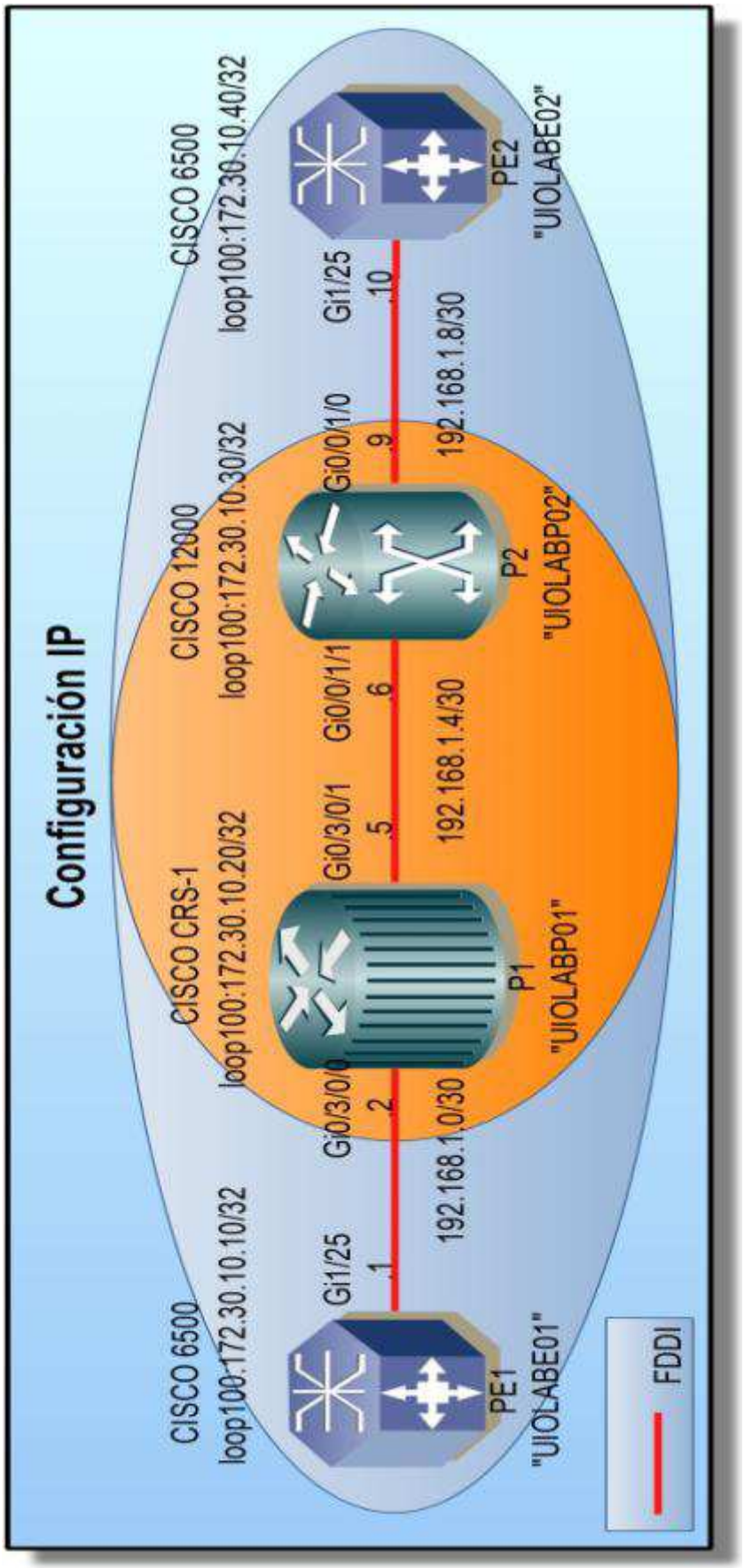


Figura 3.7: Topología 1 "Configuración básica de MPLS *Frame-mode*"

Debido a que si se utilizará un único router LSR, este se considera el penúltimo salto antes de alcanzar el nodo LER de destino. Al tener habilitado por defecto el comportamiento PHP, éste realizará una operación de pop para los paquetes enviados, por lo que no se observará el intercambio de etiquetas (swap), que es una de las funciones básicas que realizan estos routers dentro de un dominio MPLS.

Se utiliza un único enlace entre los diferentes equipos con la finalidad de verificar el establecimiento de los LSP, el procesamiento de los paquetes en cada uno de los routers que conforman la topología, más no la redundancia o balanceo de carga en la red.

Para iniciar con la habilitación de MPLS en modo trama "*frame-mode*" se debe iniciar con la configuración del direccionamiento IP, y la configuración de una interfaz de loopback la cual se le asociará como un identificador del router, y de otros procesos tales como ISIS y BGP, es por esto que a esta interfaz de loopback se la llama "loopback compartida", cuya importancia radica en la mantención de sesiones de ISIS y LDP, gracias a su naturaleza de ser lógica y encontrarse siempre activa sin depender del estado de una interfaz física. En el caso de las pruebas se ha elegido como loopback compartida la loopback 100.

DIRECCIONAMIENTO IP			
EQUIPO	**INTERFAZ**	**DIRECCION IP**	**MÁSCARA**
PE1 "UIOLABPE01"	Gi 1/25	192.168.1.1	255.255.255.252
	loop 100	172.30.10.10	255.255.255.255
PE2 "UIOLABPE02"	Gi 1/25	192.168.1.10	255.255.255.252
	loop 100	172.30.10.40	255.255.255.255
P1 "UIOLABP01"	Gi 0/3/0/0	192.168.1.2	255.255.255.252
	Gi 0/3/0/1	192.168.1.5	255.255.255.252
	loop 100	172.30.10.20	255.255.255.255
P1 "UIOLABP02"	Gi 0/0/1/0	192.168.1.9	255.255.255.252
	Gi 0/0/1/1	192.168.1.6	255.255.255.252
	loop 100	172.30.10.30	255.255.255.255

Tabla 3.8- Direccionamiento IP Topología 1.

La tabla 3.8 muestra el direccionamiento IP asignado a cada uno de los routers que forman parte de la topología de prueba. Respecto al direccionamiento, se ha utilizado dos redes la 172.30.10.0/24 asociada a las interfaces de loopback compartida en cada uno de los routers, y la 192.168.1.0/24 asignada a los diferentes enlaces WAN entre los equipos de la topología.

El siguiente paso es la habilitación de CEF[4] en los routers que conforman el backbone “PE y P”, que es un conjunto de funcionalidades de los routers Cisco para poder ejecutar MPLS. En algunos routers también se permite la habilitación de cef distribuido, el cual mejora sus funcionalidades, ya que este separa la función de control, de la función de datos y permite una conmutación más rápida.

Existen dos protocolos de enrutamiento predominantes en las redes de los proveedores de servicios, OSPF e IS-IS, ambos protocolos de estado de enlace. Para las topologías diseñadas se utiliza IS-IS, pues es el protocolo de enrutamiento que se utiliza en la red de la CNT, se lo escogió por su gran escalabilidad, menor uso de CPU que OSPF y por las facilidades que ofrece en la migración a IPv6.

Los dos protocolos de enrutamiento soportan IPv6, OSPF lo realiza con la versión tres del protocolo, en el caso de querer migrar de IPv4 (soportada por la versión 2) a IPv6 se debe cambiar de versión. La versión original de IS-IS en cambio fue diseñada para soportar múltiples protocolos de capa 3, por lo que fácilmente se puede extender para que soporte IPv6, únicamente precisa de la declaración de una *address family*[5] adicional en su configuración, esto permite que en una fase inicial de migración se pueda tener IPv4 e IPv6 en un solo proceso de enrutamiento IS-IS.

Se utiliza IS-IS integrado para que se produzca un adecuado intercambio de rutas, y que se pueda asignar las etiquetas MPLS necesarias para alcanzar las redes remotas.

---

[4] CEF (*Cisco Express Forwarding*), es un componente esencial para la conmutación de etiqueta y es responsable de la imposición y la disposición de las etiquetas en una red MPLS.

[5] Una *address family o familia de direcciones* es una forma de agrupar un conjunto de direcciones con similares características, usado por IS-IS y MP-BGP para soporte a múltiples protocolos como IPv4 *unicast*, IPv6 *multicast*, VPNv4 *unicast*, etc.

El primer paso es definir las áreas, para esto se debe considerar que un prefijo identifica un área, preparar el plan de direcciones (NET), donde el *system* ID identifica de manera única un router, las direccionamiento NSAP se muestran en la tabla 3.9.

DIRECCIONAMIENTO NET	
EQUIPO	**NET**
PE1 "UIOLABPE01"	49.0001.1720.3001.0010.00
PE2 "UIOLABPE02"	49.0001.1720.3001.0040.00
P1 "UIOLABP01"	49.0001.1720.3001.0020.00
P1 "UIOLABP02"	49.0001.1720.3001.0030.00

Tabla 3.9- Esquema de direccionamiento para IS-IS

El siguiente paso es habilitar IS-IS y el enrutamiento IP en el router; se puede asignar una etiqueta opcional que permite la identificación del proceso, con la etiqueta se pueden tener múltiples procesos en un router pero solo una de estas instancias se puede asociar con MPLS. También es necesario habilitar IS-IS integrado en las interfaces que se desea que participen en el enrutamiento

Para formar la dirección net se utiliza el AFI 49 que indica que es una dirección NSAP privada, se escoge una área única identificada con 0001, después del área se coloca la dirección IP que lo identifica, para esto se modifica la dirección aumentando ceros para completar un estructura de 6 bytes que es la soportada por los routers Cisco por ejemplo: la dirección 172.30.10.10 se transforma en 1720.3001.0010, finalmente se coloca un NSEL de 00 para identificar que es una dirección de red de un dispositivo.

Se escoge un área única para reflejar la manera en que CNT maneja su red, en la que todos los routers son parte de una sola área de nivel 2, ya que esta red se comporta como un backbone a la que se conectan varias redes, esto permitirá que en un futuro se pueda realizar una expansión de la red, basado en la creación de nuevas áreas de nivel 1 en diferentes regiones del país, las que se pegarán al backbone establecido. Otra de las razones para no dividirla en áreas es que la topología creada es pequeña como para poder dividirla en áreas, se utilizan únicamente 4 routers.

Una manera de optimizar el uso de recursos es elegir el tipo de enrutamiento, por defecto soporta nivel 1-2, para el borde de una área, sin embargo no es óptimo para todos los equipos, es preferible definir si el router es de nivel 1 o de nivel 2, en este caso se escogió que sea de nivel 2, con esto se ahorra memoria al utilizar una única LSDB[6], también se ahorra ancho de banda pues se envían menos *hello.*

Es necesario realizar la transformación de una red tipo *broadcast* como Ethernet en una red punto a punto, de esta manera se logra establecer que solo dos routers utilizarán el medio, evitando que se busque un router designado e informando que no existen más routers conectados en el medio tipo *broadcast*.

En las actuales implementaciones de IS-IS se introdujo una extensión en las métricas con la finalidad de dar soporte para la ingeniería de tráfico en MPLS, se disponen de tres opciones *narrow*, que es la implementación por defecto en la que el valor máximo es 63, *transition* que da soporte a las nuevas y antiguas métricas, y finalmente el *wide* que permite el uso de un nuevo formato largo cuyo límite es 16277215. En este caso se procedió a configurar en todos los routers wide para que IS-IS soporte ingeniería de tráfico, que se presentará en pruebas posteriores

Luego de haber configurado el IGP, el siguiente paso para permitir la conmutación MPLS es habilitar el protocolo de distribución de etiquetas, en el caso de la prueba se utiliza LDP, se lo puede habilitar de manera global en el router, permitiendo que todas las interfaces puedan establecer sesiones LDP, o solo por aquellas interfaces que se necesita que hablen MPLS, para la prueba se utiliza la segunda opción, ya que no se habilitará MPLS en todas las interfaces puesto que algunas solo manejarán IP puro con los clientes. Se habilitará en todas aquellas interfaces que se conectan hacia otro router PE o router P.

Existen varios protocolos de distribución de etiquetas LDP, MP-BGP y TDP[7], para la topología se escogió LDP, debido a que este es un protocolo estándar de la IETF, soporta autenticación de sesiones que permite evitar el establecimiento de

[6] *Link State Database* contiene la topología entera de la red, almacena los diferentes estados de enlace intercambiados entre los routers en IS-IS se utiliza una por cada nivel de enrutamiento.
[7] Tag Distribution Protocol, es protocolo de distribución de etiquetas propietario de Cisco.

sesiones con equipos no autorizados, que puedan introducir información falsa en la red de CNT.

A continuación se procede a asignar un LDP router identificador, en el caso de no asignar un LDP router-ID, el router elige como el LDP router-id a la dirección IP más alta configurada, la interfaz que se asigna como LDP router-id para la prueba es la loopback compartida “loopback100”.

3.2.1.2.2 *Comandos de configuración en un sistema IOS*

Las sentencias mostradas a continuación realizan la configuración de la interfaz loopback compartida:

```
Cisco# configure terminal
Cisco(config)# interface loopback<número de la interfaz>
Cisco(config-if)# ip address <dirección IP> <máscara>
```

Los comandos para habilitar CEF en un router que soporte esta funcionalidad son:

```
Cisco# configure terminal
Cisco(config)# ip cef [distributed]
```

Para habilitar IS-IS en el modo de configuración global se coloca las sentencias:

```
Cisco# configure terminal
Cisco(config)# router isis [area-tag]
Cisco(config-router)# net network-entity-title
Cisco(config-router)# passive-interface loopbackXXX
Cisco(config-router)# is-type {level-1 | level1-2 | level-2-only}
Cisco(config-router)#metric-style wide [transition] {level-
1 | level-2 | level-1-2}
```

La sentencia “*router isis*” crea el proceso de enrutamiento ISIS; la sentencia NET configura la dirección NSAP que identifica al router dentro de la red; la sentencia “passive-interface” señala que la dirección de esta interfaz es parte del enrutamiento, pero que no se envíen actualizaciones o se establezcan adyacencias; la sentecia *“is-type”* permitirá definir el nivel de ISIS que soportará el router; y la sentencia “metric-style” permite configurar el tipo de métrica a utilizarse.

Para configurar las interfaces que participan en el proceso de enrutamiento ISIS se dispone de las sentencias:

```
Cisco(config)# interfaz <nombre de la interfaz>
Cisco(config-if)# ip router isis [area-tag]
Cisco(config-if)#  isis network point-to-point
```

El "*area-tag"* identifica el proceso ISIS al que se asociará la interfaz, el comando "*isis network point-to-point*" establece que por esta interfaz se establece una adyacencia punto a punto.

Las configuraciones necesarias para la habilitación de LDP en un router son:

```
Cisco(config)# mpls ldp router-id loopback<número de la interfaz>
Cisco(config)# interface <nombre de la interfaz>
Cisco(config-if)# mpls label protocol ldp
```

Para forzar que una interfaz sea elegida como LDP router-id se usa la sentencia *"mpls ldp router-id",* para permitir que un interfaz establezca una sesión LDP e intercambie información de las etiquetas se usa la sentencia "*mpls label protocol ldp*"

El último paso es la habilitación de MPLS sobre cada una de las interfaces que se comunicarán utilizando MPLS, el comando de habilitación de reenvío MPLS sobre la interfaz en el sistema IOS es:

```
Cisco(config)# interface <nombre de la interfaz>
Cisco(config-if)# mpls ip
```

3.2.1.2.3 *Configuración de MPLS en el IOS XR [16] [25]*

Los pasos para realizar la habilitación de MPLS en el IOS XR son similares a los expuestos anteriormente para el IOS. El IOS XR cambia la sintaxis y la forma de configuración de algunos de los comandos. A continuación se muestra la configuración para un sistema IOS XR:

El primer paso es la configuración del direccionamiento IP, los comandos para realizar esto se muestran a continuación:

```
RP/0/RP0/CPU0:Cisco#configure
RP/0/RP0/CPU0:Cisco(config)# interface <nombre de la interfaz>
RP/0/RP0/CPU0:Cisco(config-if)# ipv4 address <ipv4-address> <mask>
RP/0/RP0/CPU0:Cisco(config-if)# commit
```

Para la configuración de la interfaz de loopback compartida se utilizan los siguientes comandos:

```
RP/0/RP0/CPU0:Cisco(config)# interface loopback<#interfaz>
RP/0/RP0/CPU0:Cisco(config-if)# ipv4 address <dirección ipv4>
<máscara>
RP/0/RP0/CPU0:Cisco(config-if)# commit
```

En el caso del IOS XR la habilitación de CEF no es necesaria ya que esta se encuentra habilitada por defecto.

El siguiente paso es la configuración de IS-IS, los comandos del IOS al IOS XR no varían; pero se debe considerar que todas las configuraciones relacionadas con el protocolo se agrupan en un solo módulo, configurando el enrutamiento IS-IS y las interfaces que participan de dicho enrutamiento en un solo bloque.

La configuración del proceso de enrutamiento IS-IS se puede realizar sin tener que configurar previamente una dirección IP en una interfaz, más el proceso de enrutamiento no iniciará hasta que se configure al menos una dirección. Los pasos para configurar el protocolo en el IOS XR se muestran a continuación; la *instance-id* en IOS XR es obligatoria:

```
RP/0/RP0/CPU0:router# Configure
RP/0/RP0/CPU0:router(config)# router isis instance-id
RP/0/RP0/CPU0:router(config-isis)# net network-entity-title
RP/0/RP0/CPU0:router(config-isis)# is-type {level1 | level-1-2 |
level-2-only}
RP/0/RP0/CPU0:router(config-isis)# address-family [ipv4 | ipv6]
[unicast | multicast]
RP/0/RP0/CPU0:router(config-isis-af)# metric-style wide
RP/0/RP0/CPU0:router(config-isis)# interface GigabitEthernet x/x
RP/0/RP0/CPU0:router(config-isis-if)# point-to-point
RP/0/RP0/CPU0:router(config-isis-if)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-isis-af)# mpls ldp sync
RP/0/RP0/CPU0:router(config-isis-af)# end o commit
```

En las sentencias anteriores se observa la manera de configurar IS-IS agrupado en un solo bloque, para definir que se utilizará IS-IS únicamente en el

enrutamiento de direcciones IPv4, se coloca la sentencia *address-family ipv4 unicast*, esto es necesario ya que por defecto la instancia maneja IPv4 e IPv6.

Las configuraciones correspondientes a una interfaz se las realiza dentro del modo de configuración de enrutamiento, se especifica la interfaz y dentro de estas se colocan los comandos que en el otro IOS se colocaba directamente en el modo de configuración de la interfaz, dentro del sub mondo de configuración de interfaz se debe especificar el tipo de rutas que se intercambiarán por la interfaz.

A continuación se procede con la configuración del protocolo de distribución de etiquetas LDP en donde debido a la característica de IOS XR esta se la hace de manera modular y ya no como lo es en IOS en cada interfaz, los comandos de configuración se muestran a continuación:

```
RP/0/RP0/CPU0:Cisco(config)# mpls ldp
RP/0/RP0/CPU0:Cisco(config-ldp)# router-id <IP loopback100>
RP/0/RP0/CPU0:Cisco(config-ldp)# interface <tipo><número>
RP/0/RP0/CPU0:Cisco(config-ldp-if)# commit
```

En la configuración se muestra el comando “mpls ldp” el cual permite ingresar al módulo de configuración LDP. Se ingresa el LDP router-id mediante el comando “router id `<IP interfaz loopback100>`” asignado de esta manera a la dirección IP de la loopback compartida en el caso de la prueba la loopback 100 como el LDP router-id, y a continuación se procede a agregar cada una de las interfaces que estarán configuradas con el protocolo de distribución de etiquetas LDP.

A continuación se muestra un resumen de las configuraciones realizadas para un router PE (UIOLABE01) con sistema IOS, y las realizadas para un nodo P (UIOLABP01) con sistema IOS XR.

```
! Configuraciones en el IOS
hostname UIOLABE01
!
interface Loopback100
 ip address 172.30.10.10 255.255.255.255
!
interface GigabitEthernet1/25
 ip address 192.168.1.1 255.255.255.252
 ip router isis
 speed nonegotiate
 mpls label protocol ldp
```

```
 mpls ip
 isis network point-to-point
!
router isis
 net 49.0001.1720.3001.0010.00
 is-type level-2-only
 metric-style wide
 passive-interface Loopback100
!
mpls ldp router-id Loopback100
!
end

! Configuraciones en el IOS XR
hostname UIOLABP01
interface Loopback100
 ipv4 address 172.30.10.20 255.255.255.255
!
interface GigabitEthernet0/3/0/0
 cdp
 ipv4 address 192.168.1.2 255.255.255.252
!
interface GigabitEthernet0/3/0/1
 cdp
 ipv4 address 192.168.1.5 255.255.255.252
!
router isis laboratorio
 is-type level-2-only
 net 40.0001.1720.3001.0020.00
 address-family ipv4 unicast
  metric-style wide
 !
 interface Loopback100
  passive
  point-to-point
  address-family ipv4 unicast
  !
 interface GigabitEthernet0/3/0/0
  point-to-point
  address-family ipv4 unicast
   mpls ldp sync
  !
 !
 interface GigabitEthernet0/3/0/1
  point-to-point
  address-family ipv4 unicast
   mpls ldp sync
  !
 !
!
mpls ldp
 router-id 172.30.10.20
 session protection
 log
  neighbor
```

```
 !
 interface GigabitEthernet0/3/0/0
 !
 interface GigabitEthernet0/3/0/1
 !
End
```

3.2.2 DISEÑO DE ESQUEMAS DE RED QUE PERMITAN PROBAR BGP [2] [3] [17]

Uno de los principales requerimientos en la red de un proveedor de servicios es la interconexión con otros proveedores, de esta manera se podrá realizar un intercambio de información de enrutamiento, que permite publicar y acceder a las direcciones de los diferentes servidores de contenido, a los que los usuarios de internet ingresan.

Cada proveedor de servicios identifica los equipos de conectividad que se encuentran bajo su dominio con un número de sistema autónomo (ASN) único, la entidad encargada de asignarlos es el IANA (*Internet Assigned Numbers Authority*), cada región tiene asignado un grupo de SA.

Internet es una red conformada por un conjunto de SA interconectados entre sí, por lo que es necesario un protocolo que se encargue de intercambiar las rutas que permiten alcanzar las diferentes redes ubicadas dentro de un SA, para realizar esto se usa BGP que es un protocolo flexible, diseñado para realizar esta interconexión.

BGP es un protocolo que permite implementar los acuerdos de interconexión suscritos entre proveedores de servicio mediante la utilización de políticas, estas políticas determinan que rutas se intercambian con un SA, para realizar esto utilizan filtros en sus routers de frontera.

Si un proveedor utiliza múltiples enlaces de interconexión entre sistemas autónomos implementando redundancia, al usar BGP puede realizar balanceo de carga por estos enlaces.

Por estas razones se decide diseñar pruebas que permitan mostrar la manera de intercambiar rutas por BGP y probar las diferentes funcionalidades de BGP, como

la manipulación de los atributos del protocolo, el filtrado de rutas, y el balanceo de carga.

3.2.2.1 Objetivos

En un primer escenario se simulará el funcionamiento de tres sistemas autónomos, utilizando una combinación de IS-IS, MPLS, LDP, BGP interno (iBGP) y BGP externo (eBGP), se utilizarán mapas de rutas, listas de prefijos y *Routing policy* para realizar filtrado de rutas y el cambio en los atributos de BGP.

En un segundo escenario se crea una topología en la que se simulará tres ISPs conectados con múltiples enlaces, se mantendrá el uso de IS-IS, LDP, MPLS y BGP del primer escenario, se utilizará el atributo MED para realizar balanceo de carga en los diferentes enlaces que interconectan los SA.

3.2.2.2 Esquemas de Pruebas de BGP

Antes de describir los escenarios es importante tomar en cuenta algunas consideraciones que se tomaron como base para realizar los dos diseños. Los argumentos base son:

Para establecer las sesiones EBGP los routers deben estar conectados directamente a sus vecinos BGP ubicados en otro sistema autónomo, para que de esta manera se pueda establecer el handshake de tres vías de TCP y se pueda intercambiar la información de enrutamiento sin tener que utilizar un IGP en los enlaces que interconectan los sistemas autónomos.

Dentro del sistema autónomo debe utilizarse un IGP, para que se puedan alcanzar a todos los vecinos que no están directamente conectados al router. Con la ayuda del IGP se establecerán sesiones IBGP en una topología full mesh, esto es necesario debido a la restricción de que las rutas aprendidas de un vecino IBGP no se pueden pasar a otros vecinos IBGP, esta regla genera agujeros negros[8] y lazos si no se crea un topología full mesh.

[8] Término utilizado para hacer referencia a routers que no disponen de entradas en la tabla de enrutamiento para alcanzar una red y por lo tanto descartan los paquetes.

Una solución para evitar la utilización de un IGP es la de redistribuir las tablas de enrutamiento aprendidas por BGP en el IGP; sin embargo no es una solución recomendada debido al gran tamaño que tienen las tablas de enrutamiento de internet. Al redistribuirlas provocarían el crecimiento abrupto de las tablas de enrutamiento del IGP afectando su escalabilidad, ya que los IGPs no fueron diseñados para soportar tantas rutas. Otra de las razones por las que no se redistribuye es la inestabilidad de las rutas de internet, el *flapping* de estas generara múltiples cálculos SPF lo que saturará el procesamiento del router.

En las topologías a implementar se procederá a desactivar la sincronización en el IOS, ya que las rutas de BGP no se redistribuirán en el IGP, lo que causará que estas rutas se aprendan únicamente a través de BGP, por lo que la sincronización no se llevará a cabo inhabilitando la publicación de rutas a otros SA. En el caso de IOS XR se ha eliminado la sincronización por lo que no es necesario desactivarla.

3.2.2.2.1 *Descripción de primer escenario*

Las condiciones necesarias para la implementación de BGP en la topología diseñada son:

- Se tendrán tres sistemas autónomos el SA 65000 compuesto por R1 y R2, el SA 65100 integrado por R4 y R5, y el 65200 formado por R5 y R6.
- Se utiliza un solo enlace Ethernet para interconectar los routers que son parte de un SA.
- Los SA están conectados directamente a sus vecinos a través de un enlace Ethernet que no maneja MPLS, se realiza la conmutación basándose en IP.
- Dentro de cada SA se utiliza IS-IS como protocolo de enrutamiento, LDP realizará la distribución de etiquetas.
- En el enlace que interconecta los dos routers que son parte de cada SA se habilitará MPLS como protocolo de transporte.
- Se establecen sesiones IBGP entre los routers que integran cada SA.

En la figura 3.8 se observa la topología diseñada para probar el protocolo BGP.

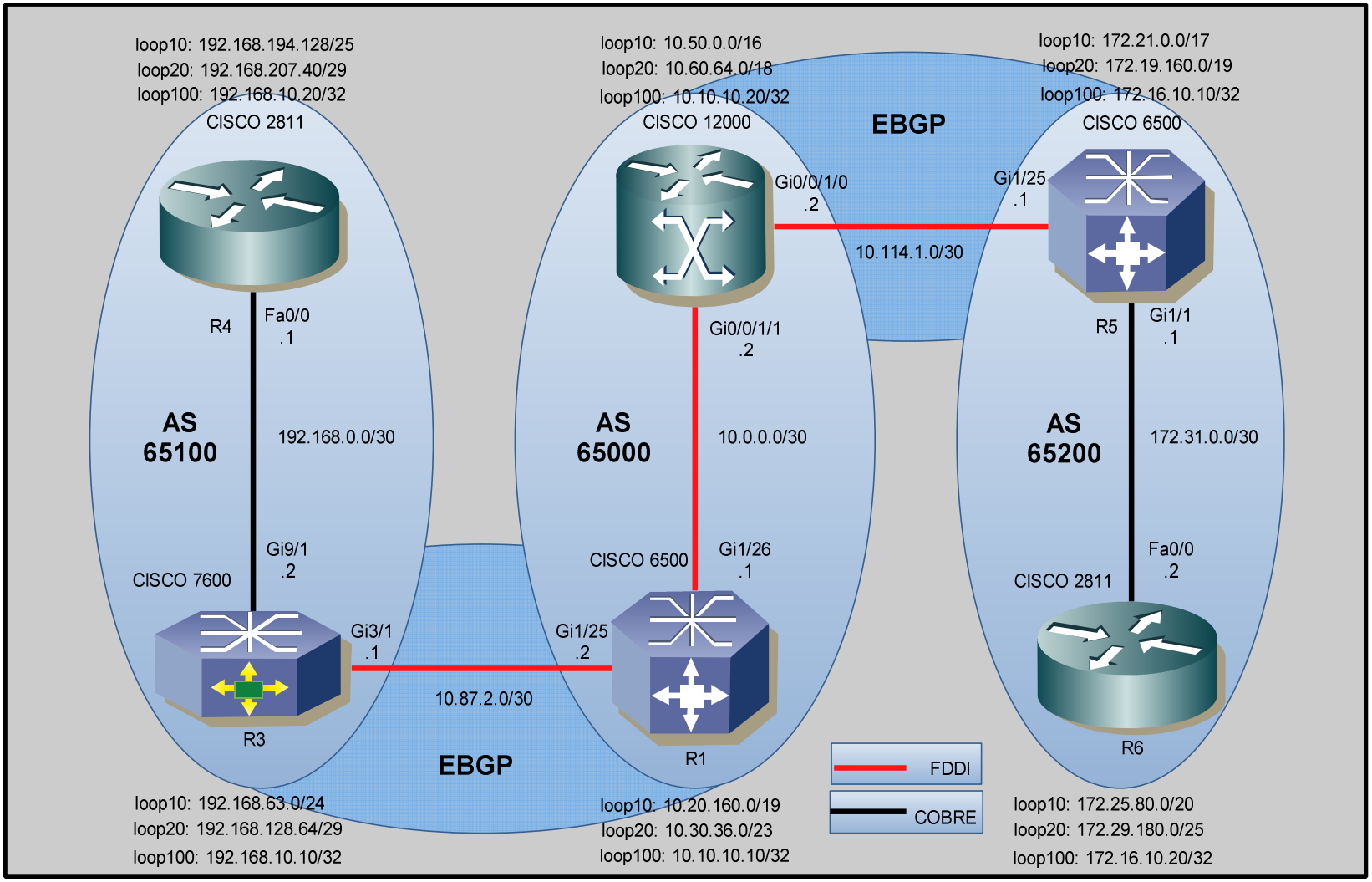


Figura 3.8: Topologia inicial de configuracion BGP

El SA 65000 representa un ISP para este caso CNT, en cambio los SA 65100 y 65200 representan a clientes conectados a la red de CNT, estos clientes utilizan BGP para aprender las redes y rutas que se tiene hacia internet, además publicarán sus propias redes en el SA 65000.

Se utiliza un único enlace entre los SA debido a que los clientes se conectan con un único enlace a sus ISPs, la manera en la que se implementa redundancia en el lado del cliente es conectándose a dos ISPs; sería similar a lo que se observa en SA 65000 que se conecta a dos SA teniendo redundancia. En nuestro caso no implementa redundancia ya que se busca mostrar la perspectiva del proveedor de servicios.

Se utiliza dos routers en cada SA con la finalidad de establecer sesiones IBGP, por las que se aprenden rutas generadas dentro del sistema autónomo; a pesar que un SA se puede ser representado con un solo router, en la realidad estos están compuestos por decenas o cientos de routers dependiendo de la cobertura que tengan, por lo que es adecuado que al menos estén simulados por dos routers.

Se utiliza la dirección IP de la interfaz loopback 100 como la dirección de origen para las actualizaciones BGP para las sesiones IBGP, esta asociación permite que las sesiones BGP se mantengan activas, asegurándonos que no se van a perder las sesiones en caso de un problema físico en una interfaz.

En la topología R4 y R6 no están conectados con otros SA por lo que no establecen sesiones EBGP, se los dispuso de esta manera con la finalidad de mostrar que no todos lo routers que integran un SA se conectan con otros SA. En los otros routers se crean sesiones EBGP, una entre R3 y R1, y otra entre R2 y R5, estas sesiones son las encargas de intercambiar las rutas entre SA.

En R2 en la sesión EBGP establecida con R5 se coloca un *routing policy* que permite que todas las rutas se publiquen, es importante colocarla ya que en el IOS XR usado por este router por defecto se impone una restricción: “se debe al menos establecer una política de entrada y una de salida para intercambiar rutas

en una sesión EBGP, en ausencia de una *routing policy* no se intercambiarán rutas".

Para activar el enrutamiento BGP, se necesita determinar el número de sistema autónomo al que pertenece el router esto se muestra en la topología. Un router puede pertenecer a un único SA, este valor se usa al momento de establecer una sesión, es necesario configurar al menos un parámetro, ya que al menos un subcomando debe ser introducido en el modo de configuración de enrutamiento de BGP para activar el proceso de enrutamiento.

En un segundo paso es necesario establecer una sesión con los vecinos, esto es obligatorio porque BGP no realiza un descubrimiento automático, para esto se configura la dirección IP y el SA del par BGP, con esto se define si es IBGP (mismo SA), o EBGP (diferente SA).

En BGP el router-id se elije como la dirección IP más alta configurada en una interfaz loopback, en caso de que no esté configurada ninguna loopback se usará la dirección más alta de cualquier interfaz, en todos los routers se utiliza la dirección de la loopback 100 como router-id, ya que es la dirección de identificación de los diferentes protocolos.

Los enlaces entre sistemas autónomos no utilizan MPLS, debido a que los clientes en sus routers de frontera no suelen tener MPLS sino que utilizan una interconexión IP sobre cualquier tecnología de capa dos para enviar los paquetes a su proveedor de servicios.

A pesar que dentro de los SA de los clientes se puede usar cualquier protocolo de transporte y enrutamiento, se utiliza MPLS e IS-IS para mostrar que estos pueden ser ISPs pequeños (*tier*[9] 3), que prestan acceso a internet a través de CNT que es proveedor de servicios *tier 2*. Estos clientes pueden ser también otros proveedores de servicio *tier* 2 con los que CNT mantiene interconexiones.

[9] Termino que hace referencia a una jerarquía de proveedores de servicio en internet. *Tier* 1 son proveedores de cobertura internacional que tienen directamente conectados los servidores de contenido como facebook, google, youtube, etc., se conectan directamente a todos los proveedores *tier 1.* En cambio los *tier* 2 son proveedores de cobertura regional o nacional que se conectan a uno o más proveedores *tier* 1. En cambio los *tier* 3 son los que se conectan a los proveedores *tier* 2.

Se considera que los sistemas autónomos 65100 y 65200 pueden ser clientes y proveedores de servicio a la vez, con la finalidad de mostrar que las políticas de enrutamiento, filtrado de rutas, etc., son independientes de la naturaleza de la conexión y que se rigen por los acuerdos a los que lleguen entre los administradores de cada SA.

Esta independencia de rutas implica que los mapas de ruta, listas de prefijo y route-policy se pueden usar en las interconexiones con clientes, como en las interconexiones con otros proveedores, lo que cambia son los atributos a modificar y las rutas que se permiten enviar y recibir, esto se definen en los acuerdos de interconexión a los que llegan los proveedores.

El primer esquema de direccionamiento a tomar en cuenta es el de las direcciones para IS-IS el mismo que mantiene las características del mostrado en la topología inicial y que se muestra en la tabla 3.10.

DIRECCIONAMIENTO ISIS	
EQUIPO	**NET**
R1	49.0001.0100.1001.0010.00
R2	49.0001.0100.1001.0020.00
R3	49.0001.1921.6801.0010.00
R4	49.1921.6800.1001.0020.00
R5	49.0001.1720.1601.0010.00
R6	49.0001.1720.1601.0020.00

Tabla 3.10- Esquema de direccionamiento de IS-IS.

La publicación de redes entre diferentes sistemas autónomos se realiza de manera estática. Para que se pueda publicar una red el router debe tener al menos una interfaz activa con una dirección IP que sea parte de la red a publicar, de lo contrario el router no anunciará la red.

Para cumplir con este requisito se asigna una dirección IP de la red a publicar a una interfaz de loopback, las redes a publicar por BGP corresponden a las usadas en las loopback 10 y 20 en cada router de la topología. El esquema de direccionamiento IP utilizado se detalla en la tabla 3.11.

DIRECCIONAMIENTO IP			
EQUIPO	**INTERFAZ**	**DIRECCIÓN IP**	**MÁSCARA**
R1	Gi 1/25	10.87.2.2	255.255.255.252
	Gi 1/26	10.0.0.1	255.255.255.252
	loop 10	10.20.160.1	255.255.224.0
	loop 20	10.30.36.1	255.255.254.0
	loop 100	10.10.10.10	255.255.255.255
R2	Gi 0/0/1/0	10.114.1.2	255.255.255.252
	Gi 0/0/1/1	10.0.0.2	255.255.255.252
	loop 10	10.50.0.1	255.255.0.0
	loop 20	10.60.64.1	255.255.192.0
	loop 100	10.10.10.20	255.255.255.255
R3	Gi 3/1	10.87.2.1	255.255.255.252
	Gi 9/1	192.168.0.2	255.255.255.252
	loop 10	192.168.63.1	255.255.255.0
	loop 20	192.168.128.66	255.255.255.192
	loop 100	192.168.10.10	255.255.255.255
R4	Fa 0/0	192.168.0.1	255.255.255.252
	loop 10	192.168.194.129	255.255.255.128
	loop 20	192.168.207.41	255.255.255.248
	loop 100	192.168.10.20	255.255.255.255
R5	Gi 1/1	172.31.0.1	255.255.255.252
	Gi 1/25	10.114.1.1	255.255.255.252
	loop 10	172.21.0.1	255.255.128.0
	loop 20	172.19.160.1	255.255.224.0
	loop 100	172.16.10.10	255.255.255.255
R6	Fa 0/0	172.31.0.2	255.255.255.252
	loop 10	172.25.80.1	255.255.240.0
	loop 20	172.29.180.1	255.255.255.128
	loop 100	172.16.10.20	255.255.255.255

Tabla 3.11- Esquema de direccionamiento IP para BGP.

Las direcciones internas del SA no se redistribuyen en BGP, esto se realiza para evitar que todas las redes internas al SA autónomo se publiquen; pues generalmente dentro de un proveedor de servicios las direcciones IP de enlaces,

identificación de routers y demás son privadas y no se pueden intercambiar con otros proveedores, es una manera de controlar las rutas que se publican.

Para la asignación de las direcciones se consideró para el SA 65000 las redes privadas clase A, para 65100 las redes privadas clase C y para el SA 65200 las redes privadas clase B, la interfaces que se conectan entre sistemas autónomos son redes clase A. Para realizar las pruebas en una primera fase únicamente se procederá a configurar el direccionamiento IP, ISIS, MPLS, establecer las sesiones EBGP, IBGP y publicación de rutas por BGP, se comprobará el adecuado funcionamiento de los protocolos, que se intercambien las rutas y que estas se instalen en la tabla de enrutamiento.

En una segunda fase se procede a realizar el filtrado de rutas para lo que se utiliza mapas de ruta, listas de prefijos y *policy-route*, (detallados en el capítulo 4), en estas se mostrará la forma de establecer que rutas se filtran, y se observará la manera de realizar la modificación de los atributos BGP.

3.2.2.2.2 *Descripción de segundo escenario*

Respecto al primer escenario en el diseño de la topología se aumenta lo siguiente:

- Dos enlaces IP uno 10 Gigabit Ethernet entre el R3 y R2 y otro Gigabit Ethernet entre R1 y R5.
- Se establecerán sesiones EBGP en estos enlaces incrementados.

La topología lógica que se obtiene se muestra en la figura 3.9, donde el SA 65000 representa a CNT un ISP *tier* 2, los SA 65100 y 65200 representan a los ISPs *tier* 1 con los que CNT se conecta en el NAP[10] de las Américas ubicado en Miami. Se incrementaron dos enlaces con la finalidad de obtener varias rutas hacia un mismo destino, para utilizar las dos interconexiones disponibles se dividirá el tráfico, una parte se envía por un enlace y la otra por el otro, de esta manera se realiza el balanceo de carga.

[10] *Network Access Point.* Es un punto de interconexión de Internet que permite intercambiar tráfico de datos y servicios entre proveedores de servicio.

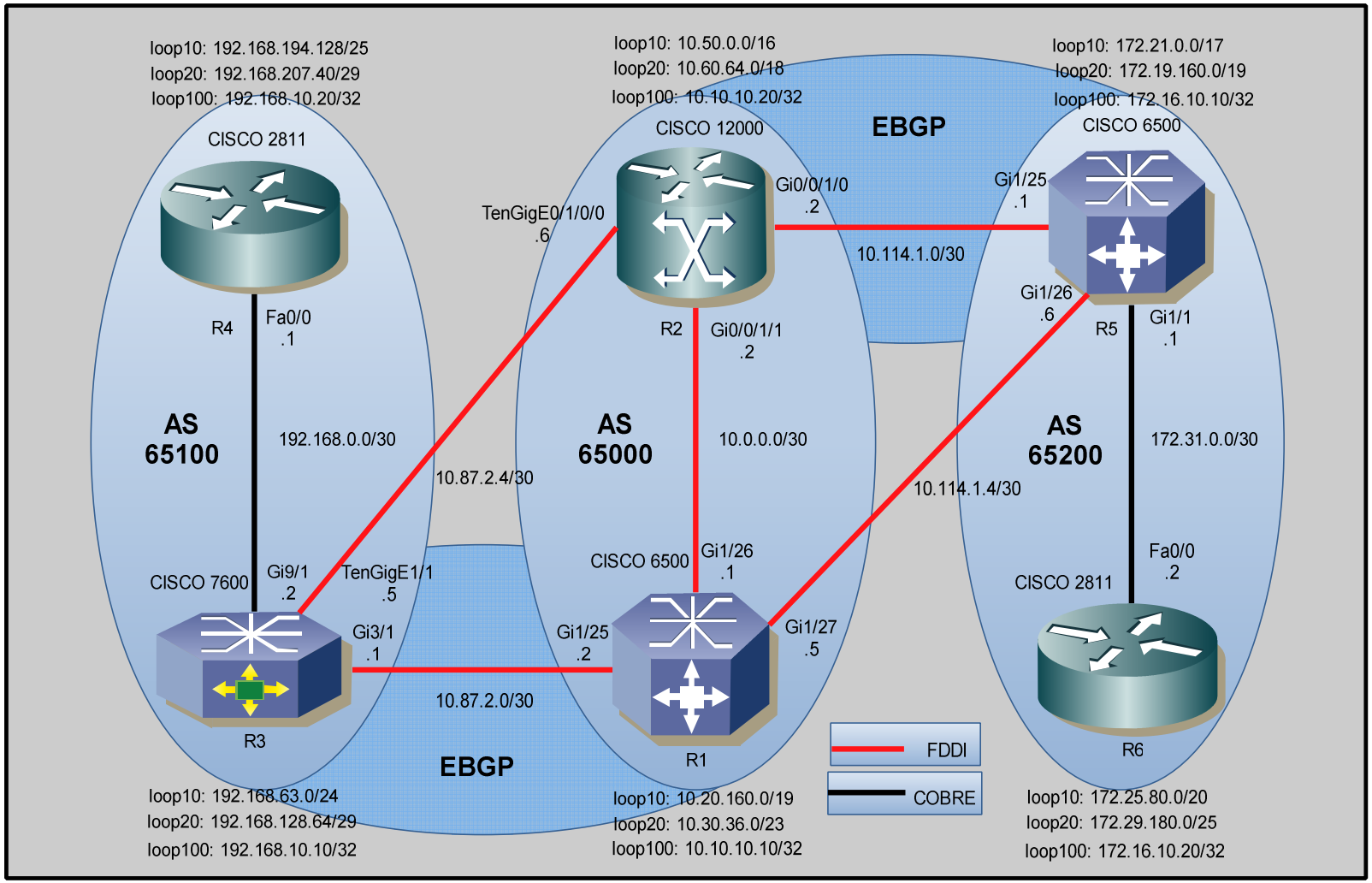


Figura 3.9: Topología lógica segundo escenario

Se realiza balanceo de carga para optimizar el uso de los recursos como el ancho de banda, el procesamiento del CPU o el número de enlaces disponibles entre sistemas autónomos.

Para determinar que tráfico se envía por cada enlace se modificará la dirección que se elige como de siguiente salto para una ruta. La modificación de la dirección de siguiente salto por la que se alcanza una red se realiza al cambiar el atributo MED

El atributo MED se considera la métrica de BGP, se prefiere el valor más bajo y por defecto se utiliza 0, puede ir de 0 a 4294967295, es una métrica externa para una ruta, se envía entre sistemas autónomos y da un indicio de que ruta es la preferida cuando se tienen múltiples puntos de conexión, tiene significado únicamente en el SA que la recibe y no se puede enviar a otros SA vecinos.

El direccionamiento IP adicional utilizado en los nuevos enlaces se muestra en la tabla 3.12.

DIRECCIONAMIENTO IP			
EQUIPO	**INTERFAZ**	**DIRECCIÓN IP**	**MÁSCARA**
R1	Gi 1/27	10.114.1.5	255.255.255.252
R2	TenGigE 0/1/0/0	10.87.2.6	255.255.255.252
R3	TenGigE 1/1	10.87.2.5	255.255.255.252
R5	Gi 1/26	10.114.1.6	255.255.255.252

Tabla 3.12- Direccionamiento IP del segundo escenario.

En las pruebas se mostrará dos formas de manipular el atributo MED, una es haciéndolo con un mapa de ruta, aplicado como una política de salida en el router que publica la ruta, de esta manera se influye en la decisión que toma el SA vecino que recibe la ruta, prefiriendo aquella que tenga el atributo MED más bajo.

Otra opción es cambiando el atributo MED en el router que recibe la ruta, para lo que se implementará un mapa de ruta como una política de entrada. Al cambiar el valor del atributo MED en el router que recibe las rutas, se evita que los SA vecinos influyan en la decisión de que ruta es preferida.

El balanceo de carga se realiza dividiendo las rutas publicadas por el SA 65100 y 65200 en dos grupos de dos redes cada uno, para alcanzar las rutas del SA 65100 se tendrán dos caminos uno es de R5 a R2 alcanzando R3 por el que se envía un grupo, el otro es de R5 a R1 alcanzando R3 por el que enviará el otro grupo, para las redes publicadas por SA 65100 se utilizará los mismos caminos.

En el SA autónomo 65000 no se alterarán los parámetros de las rutas con la finalidad de mostrar el comportamiento de BGP por defecto y compararlo con las alteraciones que se realicen.

3.2.2.3 Configuración de BGP [2] [3] [17]

En esta parte se muestra la manera de realizar las diferentes configuraciones necesarias para la realización de las pruebas en los routers que manejan el sistema IOS y los que manejan el IOS XR, adicionalmente se mostrará el funcionamiento y uso de las listas de prefijos, mapas de ruta y los *routing policy*.

3.2.2.3.1 *Construcción de sesiones de iguales* [4] [5]

El comando de configuración que crea un proceso BGP es:

```
Cisco(config)# router bgp autonomous-system
```

En las sentencias *router bgp* crea el proceso, en *autonomous-system* se coloca el número de SA al que pertenece el router.

Para crear una sesión BGP se utiliza la siguiente sintaxis:

```
Cisco(config)# router bgp autonomous-system
Cisco(config-router)# neighbor ip-address  remote-as as-number
```

La palabra clave *neighbor* se utiliza para indicar que para el vecino de dirección IP "*ip-address*" se establecerá una configuración, en este caso indica la creación una sesión BGP con el SA "*remote-as*" identificado por el ASN configurado en "as-number".

Para utilizar la dirección IP de una interfaz específica como la dirección de origen para las actualizaciones BGP que se envían a un vecino se coloca la sentencia:

```
Cisco(config)# router bgp autonomous-system
Cisco(config-router)# neighbor ip-address update-source interface-
type interface-number
```

Para establecer de manera manual el router-id se utiliza el comando:

```
Cisco(config)# router bgp autonomous-system
Cisco(config-router)# bgp router-id ip-address
```

La sentencia que permite publicar una red es:

```
Cisco(config)# router bgp autonomous-system
Cisco(config-router)# network network-prefix  [mask network-mask]
```

El parámetro mask es opcional, en el caso que no se ingrese una máscara la publicación se realizará como una red *classless.*

Para desactivar la sincronización y permitir la publicación de rutas se dispone de la sentencia:

```
Cisco(config)# router bgp autonomous-system
Cisco(config-router)# no synchronization
```

Para desactivar el auto resumen de BGP en los bordes de la red y obtener un comportamiento sin clase se utiliza:

```
Cisco(config)# router bgp autonomous-system
Cisco(config-router)# no auto-summary
```

A continuación se muestra un ejemplo de las configuraciones de BGP en R4:

```
!
router bgp 65100
 no synchronization
 bgp router-id 192.168.10.20
 bgp log-neighbor-changes
 network 192.168.194.128 mask 255.255.255.128
 network 192.168.207.40 mask 255.255.255.248
 neighbor 192.168.10.10 remote-as 65100
 neighbor 192.168.10.10 update-source Loopback100
 no auto-summary
!
```

3.2.2.3.2 *Configuración mapas de ruta BGP* [4][26][27]

Los mapas de ruta se usan para controlar y modificar la información de enrutamiento, definen las condiciones con las se distribuirán las rutas entre los *routers*, la sintaxis de un mapa de ruta es la siguiente:

```
Cisco(config)# route-map etiqueta-mapa [permit | deny] [secuencia]
Cisco(config-route-map)# match criterio-coincidencia
Cisco(config-route-map)# set accion
```

La etiqueta de mapa es una secuencia de caracteres o un nombre que identifica al mapa de ruta, el número de secuencia indica la posición que una instancia tendrá en relación a otras instancias dentro de un mismo mapa de ruta.

La forma en que estas se aplican a una actualización enviada o recibida de un vecino es: primero se aplica la sentencia con el número de secuencia más bajo, si no hay coincidencias se pasa a la siguiente; esto se continua con todas las que se dispongan, en caso de que no exista correspondencia con ninguna instancia se descarta la actualización, el permit se utilizan para permitir las rutas que coincida con el criterio o se deniegan con deny.

En la tabla 3.13 se observa algunas las sentencias y acciones disponibles.

Criterios de coincidencia	
Sintaxis	**Descripción**
match ip address *dirección*	Coincide con las rutas especificadas en una lista de acceso.
match ip addres perfix-list nombre	Coincide con las rutas especificadas una lista de prefijos.
match metric *value*	Coinciden las rutas que tengan el atributo MED igual al value.
Lista de acciones	
Sintaxis	**Descripción**
set local-preference valor	Cambia el atributo local preference de BGP
set metric valor	Cambia el atributo MED de bgp.
set origin valor	Cambia el atributo origen de una ruta.

Tabla 3.13- Resumen de criterios de coincidencia y acciones[4][5]

Dentro del mapa de rutas se configura un grupo de condiciones usando los comandos match y set, con el primero se indican los criterios que deben coincidir, y con set se especifica una acción a realizar en las rutas que coincidan con lo dispuesto por el comando match. Los criterios de coincidencia pueden ser por ejemplo un conjunto de direcciones IP determinada por una ACL[11] así: *match ip address número-access-list*, donde el número es el de una ACL estándar que se configura con la sentencia: *ip access-list número-lista-acceso [permit | deny] red-origen wild-card*.

Para aplicar un mapa de ruta a las actualizaciones enviadas o recibidas de un vecino específico se usa la sentencia:

```
Cisco(config-router)#  neighbor <dirección> route-map <etiqueta-
mapa> [out | in]
```

La dirección es la IP del vecino, la etiqueta-mapa es el nombre del mapa de ruta que se aplicará a las actualizaciones enviadas (out) o recibidas (in) de un vecino.

3.2.2.4 Configuración Listas de prefijos [4][5]

Las listas de prefijos proveen una manera de identificar rutas en los protocolos de enrutamiento y filtrarla, son flexibles debido a que los cambios y actualizaciones se pueden realizar de forma incremental, para esto cada entrada de la lista se identifican con un número de secuencia, son dependientes del orden por lo que las sentencias se evalúan de acuerdo al número de secuencia, primero el más bajo y al último el más alto. Una vez que se produce una coincidencia en esta permitirá o rechazará el prefijo, el resto de la lista no se evaluará.

Las listas de prefijos se utilizan para filtrar y restringir la información de enrutamiento, con estas se puede controlar las rutas que se instalan en la tabla de enrutamiento, y las rutas que se envían a los vecinos; para asociarla a un vecino y elegir si se aplica a las actualizaciones que ingresan o a las que salen se dispone de la sentencia:

[11] Access Control List, como su nombre lo indica estas listas permiten o deniegan el tráfico que atraviesa un punto específico de la red.

```
Cisco(config-router)#  neighbor dirección-ip prefix-list
<número/nombre-lista> [in | out]
```

Para realizar un cambio en la lista de prefijos, basta con especificar el número de secuencia de la entrada que se quiere añadir, modificar o eliminar. Deniegan todo al final si no se encuentran coincidencias, se configuran de la siguiente manera:

```
Cisco(config)# ip prefix-list {list-name | list-number} [seq-
number] {deny network/length | permit network/length} [ge ge-
length] [le le-length]
```

En la tabla 3.14 se observa con detalle los diferentes parámetros de configuración disponibles en una lista de prefijos.

Parámetro	Descripción
list-name	Nombre que identifica a la lista de prefijos
list-number	Opcional se puede colocar un número que identifica a la lista de prefijos
seq number	(Opcional) y asigna un número de secuencia a la entrada de la lista de prefijos. El rango que soporta va de 1 a 4294967294. Si no se coloca ningún valor el primero se coloca en 5 y se incrementa 5 más en cada entrada.
Deny	Rechaza el prefijo especificado.
Permit	Permite el prefijo especificado.
network/length	Configura la red y la longitud de la máscara de red en bits de 0 a 32, del prefijo que deben coincidir. Puede ser también una dirección IP.
ge *ge-length*	(Opcional) especifica el menor valor de un rango, es decir la longitud mínima del prefijo que debe coincidir, por ejemplo para "10.0.3.0/24 ge 28" especifica el rango de 10.0.3.0/28 a 10.0.3.0/32
le *le-length*	(Opcional) especifica el mayor valor de un rango, es decir la longitud máxima del prefijo que debe coincidir, por ejemplo para "10.0.4.0/24 le 28" especifica el de 10.0.0.4/24 a 10.0.4.240/28

Tabla 3.14- Listado de parámetros de una lista de prefijos. [4][28]

3.2.2.5 Configuración BGP IOS XR [16][29]

El IOS XR está diseñado para soportar de manera nativa a IPv4 e IPv6, por lo que es importante especificar la familia de direcciones que manejará BGP y cuales familias se intercambiarán con vecinos.

Para la configuración de BGP el IOS XR define varios modos de configuración, la forma de acceder a los modos utilizados en la configuración de BGP se muestra a continuación:

Ingreso al modo de configuración del router.

```
RP/0/RP0/CPU0:router# configuration
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)#
```

Ingreso al modo de configuración de la familia de direcciones.

```
RP/0/RP0/CPU0:router# configuration
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# address-family ipv4 unicast
RP/0/RP0/CPU0:router(config-bgp-af)#
```

Ingreso al modo de configuración del *neighbor*.

```
RP/0/RP0/CPU0:router# configuration
RP/0/RP0/CPU0:router(config)# router bgp 140
RP/0/RP0/CPU0:router(config-bgp)# neighbor 10.0.0.1
RP/0/RP0/CPU0:router(config-bgp-nbr)#
```

En el modo de configuración de router se especifican las configuraciones que tendrán efecto en todo el proceso de enrutamiento BGP, al momento de acceder a este modo se crea el proceso BGP y se configura el número de SA al que pertenece el router.

En el modo de configuración de la familia de direcciones se especifican las configuraciones que tendrán efecto en la familia de direcciones especificada. Al acceder a este modo y colocar la sentencia *address-family ipv4 unicast* se está especificando que el proceso BGP realizará enrutamiento para direcciones IPv4.

En el modo de configuración de *neighbor* se colocarán todas las configuraciones relacionas con la sesión establecida con un par BGP; se debe colocar el SA autónomo al que pertenece, la familia de direcciones que intercambiarán y el routing policy aplicado a las actualizaciones.

Al colocar la sentencia *neighbor* se crea una sesión con el par BGP de la dirección IP especificada.

3.2.2.5.1 *Configuración de Routing policy*[16][30]

El IOS XR introduce las *routing policy,* que permiten añadir nuevas características para inspeccionar, filtrar y modificar los atributos de las rutas que se reciben y envían a un vecino. Para su implementación se define el RPL[12] como una interfaz entre el usuario y lo equipos de enrutamiento, reemplazan a las listas de prefijos, listas de acceso y mapas de rutas usadas en el IOS para filtrar rutas.

A continuación se describirán brevemente como configurar una *route policy* y la estructura básica que se debe seguir para realizar el filtrado de rutas y la manipulación de atributos BGP:

```
route-policy <nombre>
        <declaraciones de las políticas>
end-policy
```

Con los comandos de configuración anteriores se define una *route policy,* el nombre puede ser cualquier cadena de caracteres alfanuméricos, en las declaraciones de las políticas se colocan los filtros, cambios en los atributos, etc.; si no existen políticas y se lo aplica a un vecino la acción por defecto es la de eliminar todas las rutas que provengan de este, similar a colocar la sentencia *drop*.

Para permitir el paso de todas las rutas se utiliza la sentencia *pass*, con la sentencia *abort* se elimina la *route policy* que se está configurando y se regresa al modo de configuración global. Para establecer las acciones para una ruta o grupo de rutas específico se usa el siguiente conjunto de comandos:

```
if <expresión condicional> then
        <conjunto de acciones>
elseif <expresión condicional> then
        <conjunto de acciones>
else
        <conjunto de acciones>
endif
```

[12] *Routing Policy Language* (lenguaje de las políticas de enrutamiento), propietario de cisco, diseñado para proporcionar un único y sencillo idioma que permite configurar la diferentes políticas de enrutamiento que se necesitan.

Las sentencias anteriores crean una política, cada expresión condicional (if, elseif) filtra las rutas para las que se realizará el conjunto de acciones configurado, las acciones declaradas después de *else* se ejecutan para todas las rutas que no coincidan con los criterios de las expresiones condicionales.

Las diferentes expresiones condicionales disponibles en el IOS XR se muestran en la tabla 3.15.

Comando	Descripción
destination in (prefijo)	Coincidirá con las rutas que coincidan con un prefijo configurado de la forma: X.X.X.X/XX.
local-preference *value*	Coincidirán las rutas que tengan el atributo local-prefece con un valor igual al especificado.
med *value*	Coincidirán las rutas que tengan el atributo MED con un valor igual al especificado.
next-hop in *dirección*	Coincidirán las rutas que tengan el atributo NEXT-HOP con una dirección igual a la especificada.
source in *dirección*	Coincidirán las rutas que tengan el atributo SOURCE con una dirección igual a la especificada.

Tabla 3.15- Expresiones condicionales [30]

Las diferentes acciones disponibles en el IOS XR para la creación de *routing policy* se muestran en la tabla 3.16.

Comando	Descripción
Done	Acepta una ruta sin realizar un procesamiento adicional.
Drop	Retira las rutas
set local-preference	Especifica un valor que se asignará al atributo *local-preference*.
set med	Cambia el valor del atributo MED.
set origin	Cambia el atributo origen puede ser igp, egp o imcomplete.

Tabla 3.16- Acciones que se pueden realizar [30]

Para especificar un conjunto de prefijos, para los que se desea realizar el filtrado se dispone de los *prefix-set* para crearlo se utiliza las sentencias:

```
prefix-set <nombre>
        <prefijos-IP>
end-set
!
```

En los prefijos-IP se puede declarar la dirección de un host, una dirección de red, o un rango de direcciones con las opciones *ge ge-value* y *le le-value* descritas en la tabla 3.14. Los prefix-set se usan como expresión condicional que coincide con un grupo de direcciones dentro de una *route policy.* La forma de configurar este conjunto de direcciones y usarla como expresión condicional se observa en el ejemplo mostrado a continuación:

```
prefix-set prefijos-ejemplo
        10.12.10.3,
        192.168.2.0/24,
        172.29.0.0/16 ge 27,
        172.17.0.0/23 le 28,
end-set
!

route-policy ejemplo
        if destination in prefijos-ejemplo then
                done
        elseif next-hop in (192.168.2.6) then
                set med 42
        elseif local-preference eq 10 then
                set origin igp
        else
                drop
        endif
end-policy
!
```

En el ejemplo se muestra la manera de configurar un *route policy,* las direcciones que se colocan dentro de un paréntesis declaran un valor. Para aplicarla a los prefijos enviados y recibidos de un vecino en el submodo de configuración de *neighbor* se coloca:

```
RP/0/RP0/CPU0:router(config-bgp-nbr-af)# route-policy <nombre>
in|out
```

A continuación un ejemplo de la configuración en R2:

```
router bgp 65000
 bgp router-id 10.10.10.20
 address-family ipv4 unicast
  network 10.50.0.0/16
```

```
  network 10.60.64.0/18
 !
 neighbor 10.10.10.10
  remote-as 65000
  update-source Loopback100
  address-family ipv4 unicast
  !
 !
 neighbor 10.114.1.1
  remote-as 65200
  address-family ipv4 unicast
   route-policy pass-all in
   route-policy pass-all out
  !
 !
!
```

En resumen los pasos para realizar la configuración del proceso BGP en el IOS XR se muestra en la tabla 3.17.

Comando:	Significado:
route-policy nombre-politica **end-policy**	Crea una política necesaria para el intercambio de rutas.
router bgp número-SA	Inicia el proceso BGP con el número de SA correspondiente.
bgp router-id dirección-ip	Asigna un dirección al router-id.
address-family {ipv4 | ipv6} unicast	Especifica la familia de direcciones que maneja BGP.
neighbor dirección-ip	Establece una sesión con el peer.
remote-as número-SA	Especifica el número de SA del vecino.
address-family {ipv4 | ipv6} unicast	Indica la familia de direcciones que se intercambian con un vecino.
route-policy nombre-politica **{in | out}**	Aplica una routing policy a las actualizaciones compartidas con un vecino.
end o commit	Guarda la configuración.

Tabla 3.17- Configuración de BGP.

3.2.3 DISEÑO DEL ESQUEMA DE RED PARA PROBAR VPNs

Una de las necesidades en la red de un Proveedor de Servicios, es suplir la creciente demanda de comunicaciones de las empresas, corporaciones y pymes

entre sus diferentes oficinas y sucursales, tratando de transportar las altas demandas de tráfico generadas en el entorno empresarial.

Las tecnologías de red MAN *(Metropolitan Area Networks)* y WAN (*Wide Area Networks*), en convergencia con las redes virtuales privadas VPNs soportadas sobre una red troncal MPLS, se convierte en la solución más eficiente y rentable para dar salida a esta creciente demanda de comunicación para las empresas, evitando la construcción de una infraestructura propia, que sería demasiado costoso.

Por estos motivos se decide diseñar pruebas para aprender la manera de utilizar, configurar y crear las VPNs capa dos y capa tres disponibles en MPLS, para atender las diferentes necesidades de los clientes.

3.2.3.1 Objetivos

En el primer escenario de VPN capa 2 se simula la interconexión de dos localidades remotas de un cliente a través de una red WAN MPLS, se usa el *raw mode* para establecer una VPN capa 2. Se observará como para el cliente la existencia de la red MPLS es transparente, este tendrá la percepción de que sus localidades están directamente conectadas.

En el segundo escenario de VPN capa 2 se procede a mostrar otra forma de configurar VNPs capa 2, utilizando el modo etiquetado y el modo sin procesar. En las interfaces se configurará un VC tipo 4 y tipo 5, se mostrará como configurar una topología *hub* and *spoke* típica de las VPN *frame-relay,* en la que se interconectarán tres localidades de un cliente.

Para el caso de las VPNs capa 3, se diseña una prueba en la cual se pueda mostrar la configuración y funcionamiento de una VPN MPLS de capa 3 “VRF”. Observando el comportamiento de los paquetes entre los clientes de una VRF, a través de la red del Proveedor de Servicios, que maneja como mecanismo de transporte “MPLS”, y dentro de la propia red del cliente. Así como también mostrando la redistribución de los protocolos de enrutamiento entre los sitios remotos de una VRF.

Demostrar que cada VRF dispone de una tabla de enrutamiento individual, aislada de la tabla de enrutamiento global, también se demostrará que el direccionamiento IP puede ser similar en varias VRFs sin provocar ambigüedades en sus tablas de enrutamiento.

3.2.3.2 Esquemas para Probar una VPN de Capa 2 [6] [31]

En este caso se procederá a configurar dos escenarios que permitan probar las VPN capa 2 punto a punto, específicamente el soporte que permite transportar tramas Ethernet sobre una red MPLS, no se presentarán todas las posibles situaciones, pero se plantean dos escenarios con los que se cimentarán los fundamentos necesarios para su entendimiento.

Antes de explicar los dos escenarios diseñados, cabe mencionar que para el transporte de Ethernet sobre MPLS se tienen dos modos de operación: el primero se conoce como modo sin procesar (*raw mode*) donde una trama puede o no tener un etiqueta VLAN, en caso de tenerla no tiene significado en el PE de ingreso como en el PE de salida simplemente se envía por la pseudowire que esté configurada y activa, las interfaces que soportan o son configuradas en este modo se denominan VC (*Virtual Circuit*) tipo 5.

En el segundo modo de operación conocido como el modo etiquetado (Tagged mode) cada trama debe contener una etiqueta VLAN la misma que tiene un significado en el PE de ingreso, la etiqueta se usa para distinguir por cual *pseudowire* se envía un paquete cuando se tiene más de una VPN capa 2 configurada bajo una sola interfaz. Interfaces que soportan o son configuradas en este modo se denominan VC (*Virtual Circuit*) tipo 4.

3.2.3.2.1 *Consideraciones del primer escenario "VPN capa 2 punto a punto"*

Las condiciones necesarias para el diseño del esquema de prueba son:

- Se colocan dos routers PE (Cisco 6500) y dos Ps (Cisco CRS-1 y Cisco 12000) que conforman la red del proveedor de servicios.

- Se habilita IS-IS, LDP y MPLS en los routers que conforman la red del proveedor.
- Se utiliza dos router 2800 CE1 y CE2 que simulan las localidades remotas del cliente.
- Se crea un VPN capa 2 entre los routers PEs a los que se conecta el cliente.
- En los routers del cliente se utiliza OSPF[13] como protocolo de enrutamiento.

Antes de realizar las configuraciones de una VPN se debe establecer un conjunto de configuraciones básicas necesarias para que funcione sin inconvenientes, primero se asignan direcciones IP a las interfaces de la red MPLS, un protocolo IGP, un protocolo de distribución de etiquetas y la habilitación de MPLS de manera global o en las interfaces que sea necesario.

Para cumplir con todos estos requerimientos, se parte de la topología lógica básica inicial mostrada en la primera parte, en la que se habilita MPLS en el backbone de un proveedor de servicios, se realizan las configuraciones de los elementos que la conforman utilizando el mismo direccionamiento, mismas interfaces, parámetros de ISIS, MPLS y LDP.

Con todas estas consideraciones a la topología base se le aumentan dos routers 2800 que simulan dos localidades de un cliente que se conectan a través de una red WAN.

Para crear la VPN punto a punto se realizará una configuración conocida como router a router basada en puerto, misma que fue diseñada para transportar Ethernet extremo a extremo de manera transparente, para lograr esto la trama Ethernet sin el preámbulo y FCS es transportada como un único paquete MPLS basado en el *VC type 5.*

La topología que cumple con las características descritas se muestra en la figura 3.10.

[13] *Open Shortest path first* (OSPF) es un protocolo de enrutamiento interior de estado de enlace similar a IS-IS que usa para el intercambio de rutas.

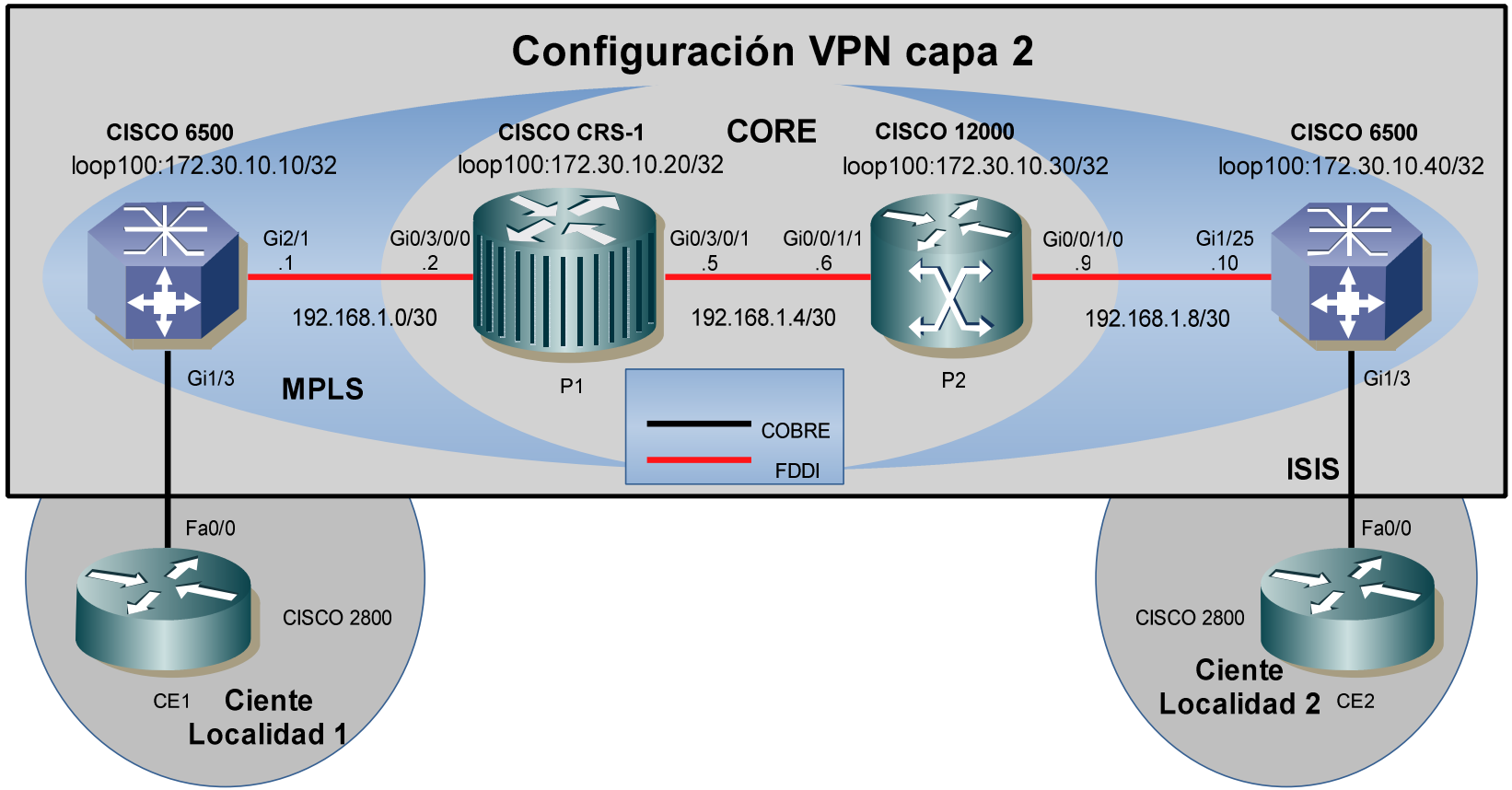


Figura 3.10: Topología Conexión dos localidades

Se crean dos pseudowires una por la que se enviarán los paquetes y otra por la que se recibirán los paquetes enviados desde el otro extremo, se utilizan dos etiquetas para su envío dentro del dominio MPLS la más interna identifica la VPN, mientras que la más externa se utiliza para realizar la conmutación en el dominio MPLS e irá cambiando en cada salto hasta alcanzar el PE de salida.

La asignación de las etiquetas que identifican a la VPN se la realiza mediante LDP. Se crea una sesión LDP entre los dos routers PEs, que permite aprender las etiquetas internas usadas para identificar a la VPN.

Para comprobar el adecuado funcionamiento de la VPN creada, en los routers que simulan a los clientes se configurará interfaces loopback con direcciones de red que emularán las redes LAN internas del cliente, para realizar el enrutamiento necesario se utilizará OSPF; pues es un protocolo altamente utilizado a nivel LAN, se lo habilitará en los routers CE, y se encargará del intercambio las rutas conectadas en cada extremo.

Al observar que se establecen las adyacencias OSPF, y se produce un intercambio de rutas se comprobará el adecuado funcionamiento de la VPN. El direccionamiento usado en las localidades de cliente se observa en la tabla 3.18.

DIRECCIONAMIENTO IP			
EQUIPO	INTERFAZ	DIRECCION IP	MÁSCARA
CE1	Fa 0/0	10.10.1.1	255.255.255.252
	loop 100	192.168.2.1	255.255.255.0
CE2	Fa 0/0	10.10.1.2	255.255.255.252
	loop 100	192.168.1.1	255.255.255.0

Tabla 3.18- Direccionamiento del cliente

Las direcciones IPs utilizadas en los routers del cliente, no tendrán significado dentro del dominio MPLS, por lo que se pueden utilizar las misma redes dentro de la red del proveedor, y en el direccionamiento interno del cliente.

Para comprobar esta independencia se utilizó la red 192.168.1.0/24 como una red LAN del cliente, esta misma red fue utilizada en los enlaces que interconectan los

routers del domino MPLS, y no genera un conflicto de duplicación de IPs siendo esta otra forma de comprobar la transparencia de la VPN capa 2.

3.2.3.2.2 *Consideraciones del segundo escenario "VPN capa 2 modelo HUB and SPOKE"*

Las condiciones necesarias para el diseño del esquema de pruebas del escenario 2 son:

- Se utilizan tres LERs PE1, PE2 y PE3, conectados a través de un nodo LSR P1.
- Se colocan enlaces que interconectan los nodos PEs al nodo P, y uno adicional entre PE1 Y PE2.
- Dentro de la red del proveedor de servicios se utiliza IS-IS, LDP y MPLS en los diferentes routers P y PEs.
- Se tienen dos nodos *spoke* CE1 y CE3, y un nodo *hub* CE2 que representan las localidades del cliente.
- Las tres localidades del cliente se conectan a los nodos PEs del proveedor de servicios.
- Se habilita OSPF en la red del cliente para intercambiar las rutas.
- Se crean dos VPNs una entre CE2 y CE1, la otra entre CE2 y CE3.

Los tres nodos PEs emulan un punto de presencia del proveedor, todos los routers se interconectan a través de un nodo de *core* que realizará únicamente conmutación de etiquetas.

Entre PE1 y PE2 se colocó un enlace adicional con la finalidad de simular una topología en malla parcial que es la manera en que se conectan los equipos de los proveedores de servicios para asegurar la disponibilidad mediante redundancia de enlaces.

La topología que cumple con las características descritas se muestra en la figura 3.11.

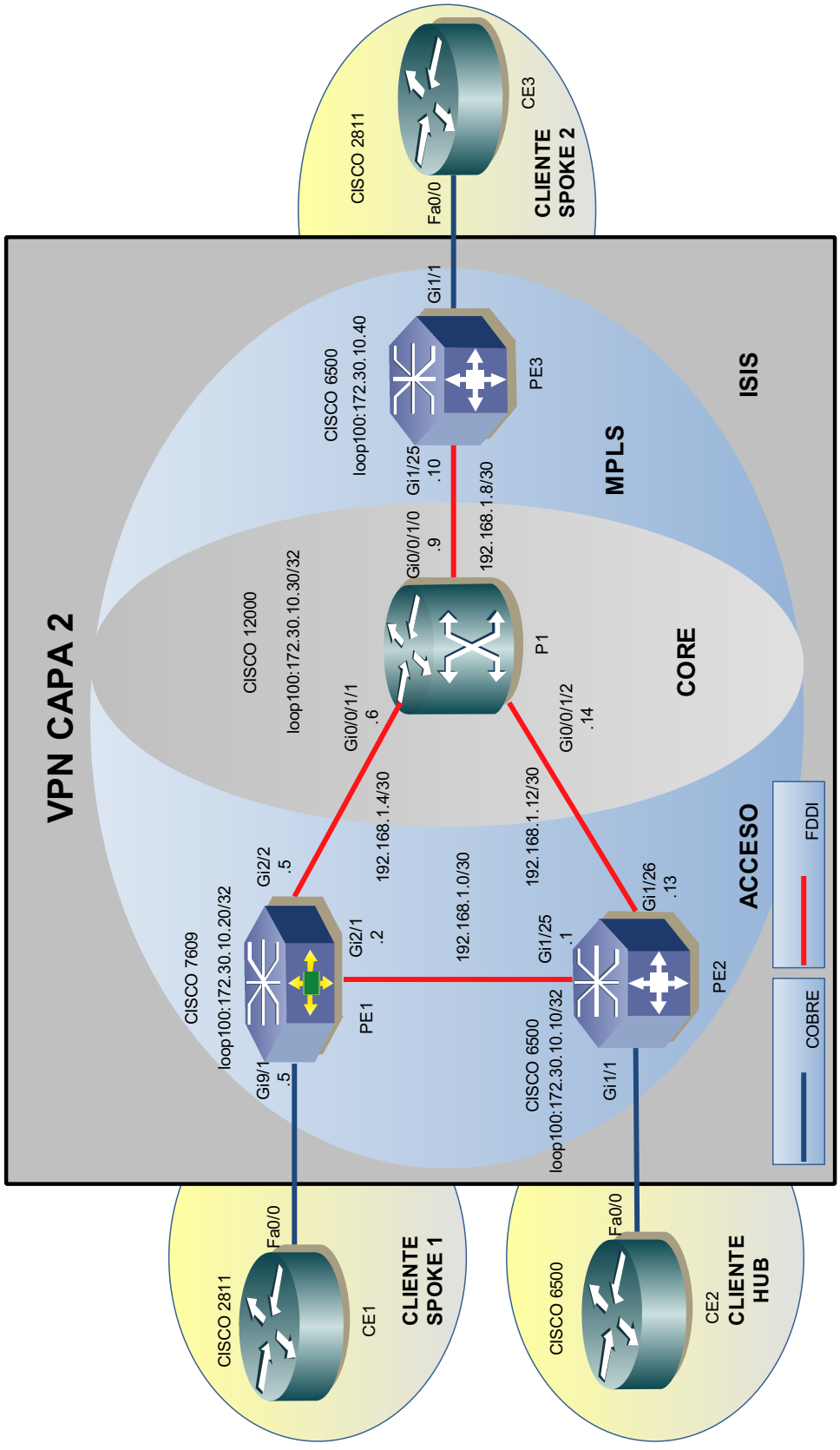


Figura 3.11: Topología conexión HUB and SPOKE

Los nodos spoke CE1 Y CE3 estarán conectados al hub CE2 a través de la red del proveedor de servicios, para establecer la interconexión se establecerán dos VPN una entre CE1 y CE2 con vcid de 1000 y otra entre CE2 y CE3 con un vcid de 2000, por lo que el tráfico dirigido de CE1 a CE2 tendrá que pasar CE3, que será el encargado de reenviarlo a su destino final. El direccionamiento IP se muestra en la tabla 3.19.

DIRECCIONAMIENTO IP			
EQUIPO	**INTERFAZ**	**DIRECCIÓN IP**	**MÁSCARA**
PE1	Gi 2/1	192.168.1.2	255.255.255.252
	Gi2/2	192.168.1.5	255.255.255.252
	loop 100	172.30.10.20	255.255.255.255
PE2	Gi 1/25	192.168.1.10	255.255.255.252
	loop 100	172.30.10.10	255.255.255.255
PE3	Gi 1/25	192.168.1.1	255.255.255.252
	Gi 1/26	192.168.1.13	255.255.255.252
PE3	loop 100	172.30.10.40	255.255.255.255
P1	Gi 0/0/1/0	192.168.1.9	255.255.255.252
	Gi 0/0/1/1	192.168.1.6	255.255.255.252
	Gi 0/0/1/2	192.168.1.14	255.255.255.252
	Loop 100	172.30.10.30	255.255.255.255
CE1	Fa0/0	192.168.1.6	255.255.255.252
	loop 10	192.168.10.1	255.255.255.0
CE3	Fa0/0	192.168.1.2	255.255.255.252
	loop 30	192.168.20.1	255.255.255.0
CE2	Gi 1/1.1000	192.168.1.5	255.255.255.252
	Gi 1/1.2000	192.168.1.1	255.255.255.252
	loop 100	192.168.30.1	255.255.255.0

Tabla 3.19- Direccionamiento IP de la topología.

Dentro de los routers del cliente se configurará OSPF como protocolo de enrutamiento, la simulación de las redes que conforman las LAN del cliente se las realizará con las interfaces loopback, que tendrán asignada una dirección IP de la

red LAN a emular. En el router que cumple las funciones de HUB se utiliza *Router on a stick*[14] para ofrecer conectividad con las dos localidades *spoke*.

Para el adecuado funcionamiento de las VPN se realizarán configuraciones de MPLS, LDP e ISIS de las misma manera que en la topología base por lo que no se detallarán sus configuraciones. El direccionamiento NET se muestra en la tabla 3.20.

DIRECCIONAMIENTO IP	
EQUIPO	**NET**
PE1	49.0001.1720.3001.0020.00
PE2	49.0001.1720.3001.0040.00
PE3	49.0001.1720.3001.0010.00
P1	49.0001.1720.3001.0030.00

Tabla 3.20- Direccionamiento NET de la topología.

En el direccionamiento mostrado en la tabla 3.20 se observa que en el router CE3 se usan subinterfaces[15], que se utilizan para distinguir las conexiones a las localidades remotas mediante VLANs, en el router del cliente a cada subinterfaz se asigna una dirección IP y un encapsulamiento dot1q[16], este encapsulamiento es usado para añadir una etiqueta VLAN al paquete que se envía al proveedor, adicionalmente el encapsulamiento permite distinguir que paquetes de los enviados por el proveedor pertenecen a una subinterfaz.

De manera similar en el router del proveedor de servicios se tendrán subinterfaces, que manejan el encapsulamiento dot1q, esto permite hacer uso del modo operación etiquetado. En el que un flujo se distingue por la etiqueta VLAN colocada en los paquetes, en base a esta clasificación se enviarán por la VPN adecuada para alcanzar la otra localidad del cliente, el encapsulamiento añade

[14] Router-on-a-stick es un tipo de configuración de router en la cual una interfaz física única enruta el tráfico entre múltiples VLAN en una red.
[15] Una subinterfaz es una interfaz lógica que se obtiene al dividir una única interfaz física en múltiples subinterfaces que tienen similares características que las físicas, usan un tipo de encapsulamiento para distinguir entre flujos de tráfico. Permiten implementar el enrutamiento inter VLANs *Router-on-a-stick*.
[16] Nombre alternativo del protocolo IEEE 802.1q, es un mecanismo que permite compartir un enlace físico Ethernet entre múltiples redes lógicas independientes, define el formato de la etiqueta VLAN, la etiqueta permite distinguir que paquetes pertenecen a una red lógica.

una etiqueta a los paquetes que se envían al cliente, permitiendo que este distinga los flujos de tráfico pertenecientes a cada *spoke*.

Para que la configuración sea consistente tanto en el lado del proveedor como en el del cliente se distingue con el mismo valor la subinterfaz, la etiqueta VLAN y el vcid de la VPN.

Con todas estas consideraciones se logrará establecer conexiones de capa 2 entre la localidad principal del cliente o HUB y las localidades secundarias o *spoke*. El envío de paquetes y el establecimiento de adyacencias OSPF se realizará de manera transparente para el cliente permitiendo dar la apariencia de que los routers están directamente conectados en el caso de CE1 y CE3, mientras que en el caso de CE1 se utilizará VLANs para distinguir las conexiones.

3.2.3.2.3 *Comandos de configuración de las VPN capa 2*

Para configurar la VPN punto a punto se dispone de la sentencia:

`xconnect` *`peer-ip-address vcid`* `encapsulation mpls`

La forma de configurar los diferentes parámetros para esta sentencia es la siguiente: en *peer-ip-address* se coloca la dirección IP del de la interfaz loopback que identifica al proceso ldp en el router del otro extremo de la VPN, el vcid (*virtual circuit identifier*) es un campo de 32 bits que identifica de manera única una pseudowire y por ende a la VPN de capa 2 en los dos PEs, por lo tanto debe tener el mismo valor en los dos routers, finalmente la parte *encapsulation MPLS* de la sentencia indica el tipo de encapsulación que se usará para el envío de los paquetes.

Para la configuración de OSPF se utilizan los siguientes comandos:

```
Cisco(config)#router ospf <ID de proceso>
Cisco(config-router)#network <Direccion de red><wild card>
Cisco(config-router)#passive-interface loopback100
```

Las sentencias anteriores habilitan el proceso de enrutamiento OSPF en un dispositivo, se usa un identificador de proceso ya que se puede tener más de un

proceso de enrutamiento en un router, la sentencia *network* se usa para asociar que redes e interfaces serán parte del proceso, finalmente *passive-interface* permite habilitar la publicación de la red pero no establece adyacencias por la interfaz.

La configuración de una sub interfaz es:

```
Cisco#configure terminal
Cisco(config)#interface Gi1/1.1000
Cisco(config-subif)#ip address <direction IP><Máscara>
Cisco(config-subif)#encapsulation dot1Q <número>
```

Con lo anterior se configura una subinterfaz en el router del cliente, la segunda sentencia crea la subinterfraz el .1000 la distingue de otras, dentro de esta el número corresponde con el valor que asigna a la etiqueta VLAN.

Se configura de la siguiente manera:

```
Cisco#configure terminal
Cisco(config)#interface Gi1/1.1000
Cisco(config-subif)# xconnect peer-ip-address vcid encapsulation
mpls
Cisco(config-subif)#encapsulation dot1Q <VLAN>
```

En la configuración se observa que se crea una subinterfaz, dentro de esta se define el tipo de encapsulamiento a usar en el enlace con el cliente, y se crea la VPN capa 2, se utilizan dos subinterfaces para crear las dos VPNs necesarias para el esquema.

Las configuraciones anteriores se realizan en el lado del HUB, mientras que en los *spoke* la configuración es la misma que se utilizó para el primer escenario.

3.2.3.3 Esquema para Probar una VPN Capa 3 "VRF" [9] [10] [11] [12]

3.2.3.3.1 *Consideraciones del escenario de pruebas de VPNs capa 3 "VRFs"*[9] [11]

Las condiciones necesarias para el diseño del esquema de prueba de VPN capa 3 son:

- Se dispuso dos routers LER PE1 y PE2 (Cisco 6500), conectados a través de dos routers LSR P1 (Cisco CRS-1) y P2 (Cisco 12000).
- Se dispuso de dos routers CE3 y CE4 (2800), dos generadores de tráfico (IXIA 400 T) que representan las localidades de los clientes.
- Se utilizan enlaces únicos entre los equipos de conmutación que conforman la red del proveedor de servicios.
- Cada una de las localidades del cliente se conecta con un único enlace a la red del proveedor de servicios en los nodos PE.
- Se habilita IS-IS, LDP y MPLS en los routers que conforman la red del proveedor.
- Se crean dos VPN capa 3 entre los routers PEs, cada VPN interconecta dos localidades de un cliente.
- El enrutamiento que se utilizará para un cliente es RIPv2, y para el otro se utilizará OSPF.

Los routers “PE1, P1, P2 y PE2”, forman un backbone MPLS representando la infraestructura de un Proveedor de Servicios, los routers “CE3 y CE4” representan y cumplen las funciones del router de frontera de un cliente que se pega a la nube del Proveedor de Servicios.

CE3 forma junto a uno de los generadores de tráfico “IXIA 400T” una red empresarial para un cliente “Cliente A”, cumpliendo la función de sucursales de la red del cliente, de igual forma el router CE4 y otro generador de tráfico forman una red empresarial con dos sucursales para un cliente diferente “Cliente B”.

Para iniciar con la configuración de las VPN capa 3 MPLS “VRF” se requiere la configuración y habilitación del backbone MPLS, cuya configuración se revisó en la habilitación de MPLS en un backbone de un proveedor de servicios, y es la base para el funcionamiento de las VPN de capa 3 en discusión.

La topología que cumple con las características descritas se muestra en la figura 3.12.

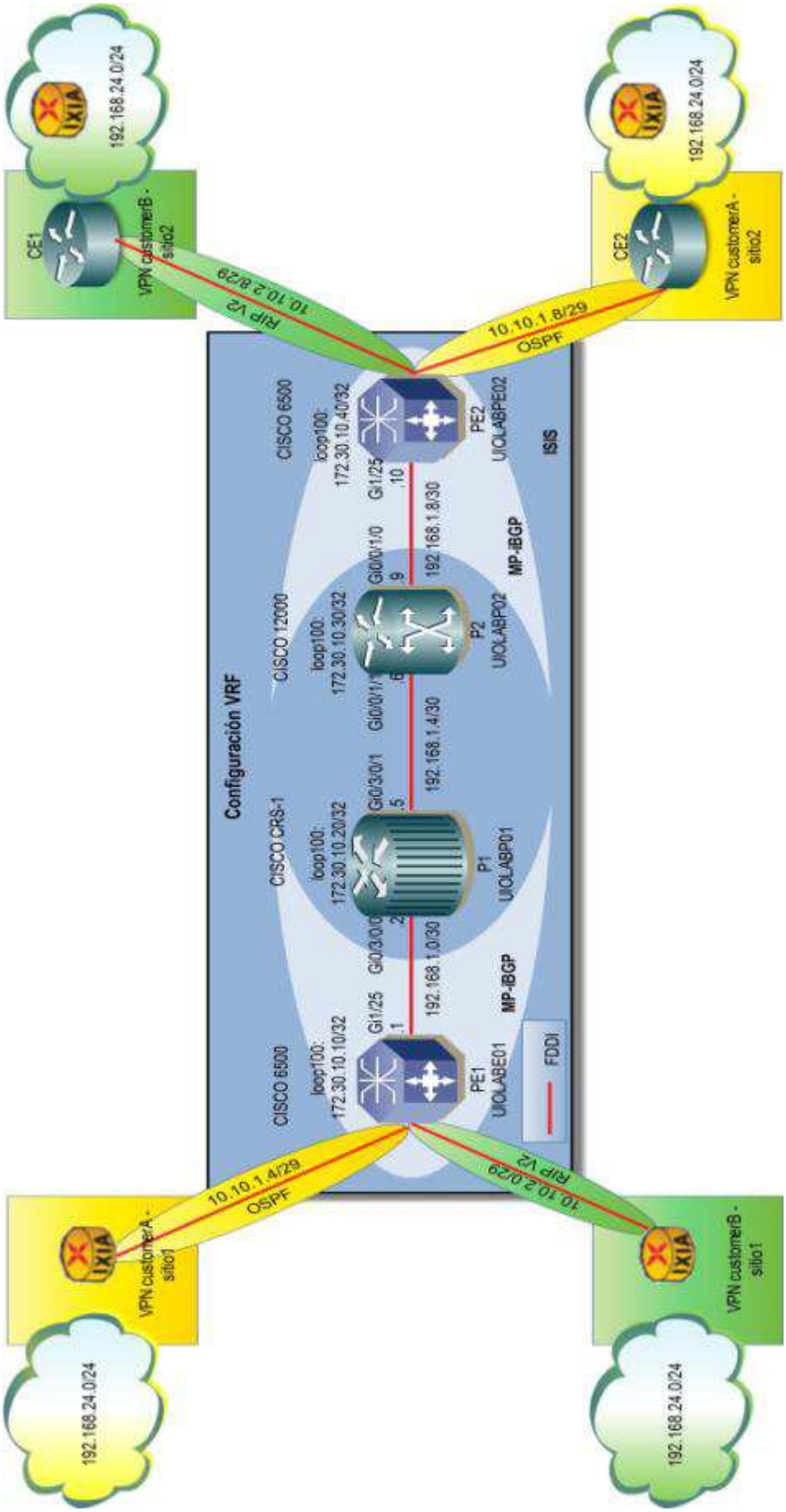


Figura 3.12: Topología de pruebas para configuración de VPNs VRF

Los pasos para la habilitación de MPLS son:

- Habilitación de CEF
- Configuración del IGP “ISIS”
- Habilitar el protocolo de distribución de etiquetas “LDP”
- Habilitación de MPLS en cada una de las interfaces que reenviarán MPLS y se conectan hacia un PE o P router.

El diseño de la prueba se basó en una topología básica de un backbone MPLS, en la cual se dispondrá de enlaces únicos entre los equipos de conmutación, debido a que se necesita verificar el comportamiento de los paquetes entre los clientes de una VPN, sin establecer balanceo del tráfico, por lo que no se dispuso de enlaces redundantes entre los equipos.

Los requerimientos que se presentarán de aquí en adelante son los que se necesitan en un router de frontera (PE), al que se pega el Cliente de la VPN para el funcionamiento de una VPN MPLS capa 3.

Los requerimientos en un router de intercambio de etiquetas LSR (P) para el funcionamiento de las VPN VRF, son tan solo la habilitación del reenvío MPLS, no manejan BGP ya que el tráfico de las VRFs es transparente para dichos routers, solo visualizan el label stack del paquete, intercambiando la etiqueta más externa para alcanzar el siguiente salto.

Uno de los requerimientos para la prueba es el traspaso y anuncio de las rutas de cliente a través del backbone MPLS VPN entre los routers PE, debido a que las VRF manejan un protocolo de enrutamiento distinto e independiente al IGP del *backbone,* las rutas no pueden ser distribuidas a través de este*, y* se hace uso de MP-BGP (Multiprotocol BGP) para realizar la redistribución de protocolos*,* permitiendo el conocimiento de todos los prefijos de red del cliente en cada uno de los PE routers participantes de la instancia VRF.

La habilitación de MP-BGP es un proceso de dos pasos, en el primero de ellos se habilita globalmente BGP en el PE router y sus vecinos PE que intercambiarán

rutas de clientes MPLS VPN, para luego activar el intercambio MP-BGP de rutas, bajo la familia de direcciones VPNv4 (*VPN-IPv4 address family)*.

A continuación se crean dos instancias VRFs CustomerA y CustomerB, en los routers PEs del proveedor de servicios. El nombre asignado a un VRF tiene significado únicamente local y no se requiere que esta identificación coincida en todos los routers PE que comparten la VRF, sin embargo en las pruebas se le asigna el mismo nombre para mantener una consistencia en las configuraciones de manera que el entendimiento se facilite.

CustomerA interconecta las localidades remotas del cliente 1 y CustomerB las localidades del cliente 2, permitiendo el traspaso de información entre las localidades. A cada VRF se le asigna un identificador único conocido como *route distinguisher*.

El *route distinguisher* para la VRF, tiene dos formatos: ASN:nn y el formato IP-address:nn**.** El ASN es el número de sistema autónomo que el *Internet Assigned Numbers Authority (IANA)* asigna al proveedor de servicios y el ***nn*** es el número que el proveedor de servicios asigna a una VRF, y es un número único de administración para la VRF, el IP-address es la dirección IP de la interfaz en la que se conecta el cliente.

Los dos formatos son válidos para identificar de manera única a una VRF dentro de la red del proveedor de servicios. Para el caso de la prueba se eligió el formato “AS:nn” para identificar a las VRFs se eligió este formato debido a que permite tener una mejor administración de las VRFs creadas en la red, existen proveedores de servicio que manejan varios SA y si se utilizará la dirección IP como identificador se dificultaría encontrar el SA en que la VRF está configurada.

El RD crea las tablas de enrutamiento y reenvío, se añade al principio de los prefijos IPv4 de los clientes para convertirlos en prefijos únicos dentro de la familia de direcciones VPNv4.

La distribución de las redes VPNv4 es controlada por el uso de los Route-Target, implementadas por las comunidades extendidas de BGP, cuando en un PE

aprende una red desde el CE esta red es inyectada dentro de BGP y junto a esto se añaden los RT que son comunidades extendidas de BGP, las cuales permiten el ingreso/egreso de rutas de la VRF lo cual permitiría que los sitios de cliente pertenezcan a una VPN, pero también permiten establecer complejas arquitecturas VPN donde pueden participar de varias VPNs, asignándole varios route target.

Cada una de las instancias VRFs será asignada a una interfaz en la cual se conecta la localidad del cliente a la red del proveedor de servicios. Las asignaciones de la topología se las realiza a través de interfaces VLAN para conectar los generadores de tráfico, debido a que los generadores de tráfico no manejan enrutamiento y se comportan como una estación de trabajo, permitiendo mostrar la flexibilidad de una VRF, que permite la integración de equipos de capa 2 y capa 3 bajo una misma infraestructura.

Para conectar los routers que simulan la localidad del cliente se utilizarán interfaces físicas, en las que se asociará una VRF, permitiendo que los routers de frontera del cliente y el proveedor de servicios manejen un protocolo de enrutamiento independiente al IGP usado en el backbone MPLS.

La habilitación del protocolo de enrutamiento entre el PE-CE varía en función de que protocolo se encuentra en funcionamiento entre el Cliente y el Proveedor de Servicios sea este “RIP v2, OSPF, EIGRP o EBGP”, las rutas estáticas también son una alternativa para establecer la conectividad entre el PE y CE.

Se ha elegido como los protocolos entre PE-CE, las opciones de RIPv2 y OSPF, estos métodos de enrutamiento son los más usados dentro de redes corporativas y clientes que utilizan la infraestructura de CNT, a continuación se describirán estas dos opciones de enrutamiento entre el cliente y el Proveedor de Servicios.

El cliente 1 que utiliza la VRF CustomerA maneja el protocolo de enrutamiento RIPv2 con una familia de direcciones IPv4 asociada a la VRF, se debe asegurar la redistribución de rutas del cliente en MP-BGP, para que este distribuya las rutas entre los PEs participantes de la VPN.

El cliente 2 que utiliza la VRF CustomerB maneja el protocolo de enrutamiento OSPF con un proceso OSPF asociado a la VRF, se debe asegurar la redistribución de rutas del cliente en MP-BGP, para que este distribuya las rutas entre los PEs participantes de la VPN.

3.2.3.3.2 *Configuración de una VRF.*

La configuración de BGP se realiza de la misma forma que se mostró en las topologías de BGP. La habilitación de una instancia VRF mostrada en la figura 3.13 en el router PE se realiza con los siguientes comandos:

```
Cisco(config)# ip vrf <nombre_vrf>
Cisco(config-vrf)# rd <AS:nn>
Cisco(config-vrf)# route-target export <AS:nn>
Cisco(config-vrf)# route-target import <AS:nn>
```

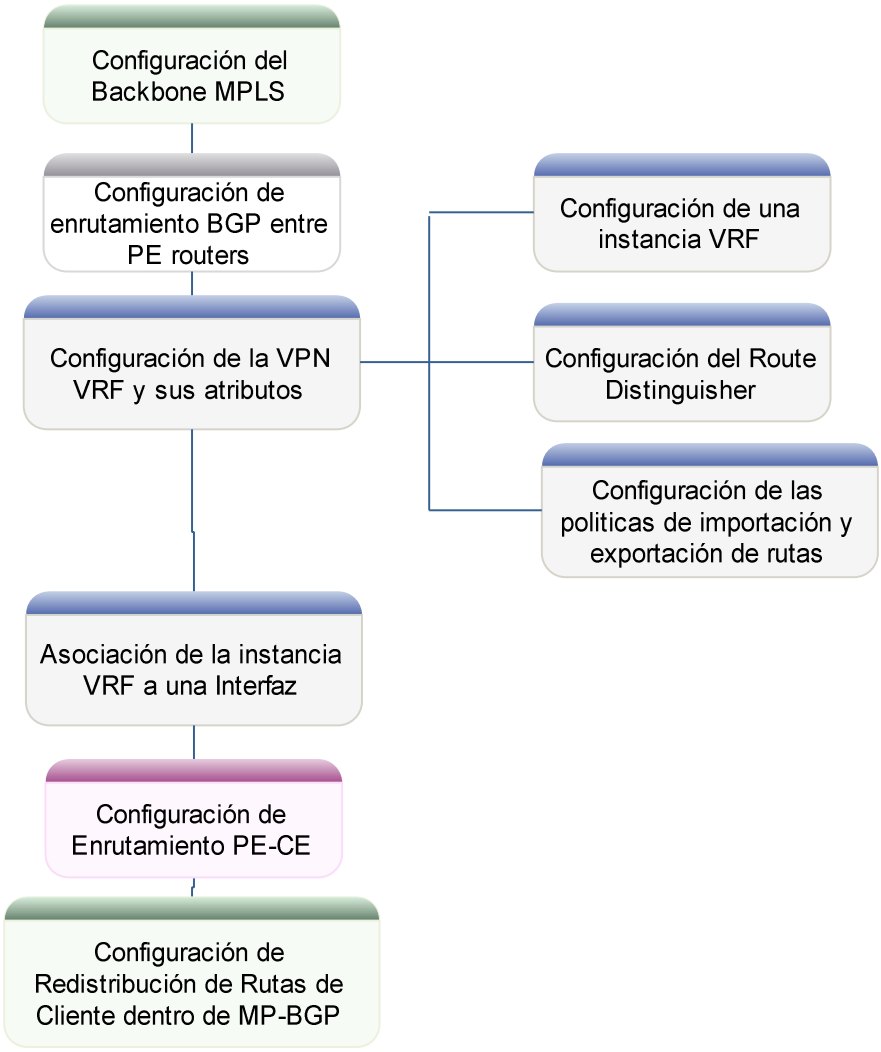


Figura 3.13: Flujograma de configuración de VPNs VRF

El comando "**ip vrf** <nombre_vrf>" habilita una instancia VRF en donde el "nombre_VRF" es la identificación de la VRF en configuración, la escritura del nombre de la VRF es "*case-sensitive*" sensible a mayúsculas y minúsculas, el siguiente comando "**rd** <AS:nn>", configura el *route distinguisher* para la VRF.

Las dos siguientes configuraciones permiten establecer las políticas de importación y exportación de las rutas desde y hacia los equipos pertenecientes a una VRF, el comando "**route-target export** <AS:nn>" permite asignar el valor del atributo que se propagará, junto a las rutas VPNv4 a exportar sobre BGP, identificando la pertenencia de las rutas a una VPN, el comando "**route-target import** <AS:nn>" identifica el valor del atributo de rutas VPNv4, que se buscarán en las actualizaciones de rutas en BGP, para insertar las rutas que coincidan con este atributo dentro de la tabla de enrutamiento de la VRF.

Como siguiente paso de configuración, se debe asociar la instancia VRF a una interfaz o subinterfaz, donde el Cliente se conecta a la nube de Backbone del Proveedor de Servicios. Los comandos de configuración se muestran a continuación:

```
Cisco(config)# interface <nombre_de_la_interfaz>
Cisco(config-if)# ip vrf forwarding <nombre_vrf>
Cisco(config-if)# ip address <ipv4-address> <mask>
```

Para realizar la configuración se selecciona la interfaz a ser asociada a la instancia VRF y se ingresa en el modo de configuración de interfaz con el comando "**interface** <nombre_de_la_interfaz>", para luego en este modo configurar y establecer la asociación con la instancia VRF con el comando "**ip vrf forwarding** <nombre_vrf>", luego establecer la dirección IP del enlace en dicha interfaz con el comando "**ip address** <ipv4-address> <mask>", si antes de asociar la interfaz con la VRF esta se encontraba configurada previamente, la dirección IP será removida de la interfaz y tendrá que ser reconfigurada después de la asociación. A continuación se presenta un ejemplo de configuración de una instancia VRF:

```
ip vrf voice
rd 65000:100
```

```
route-target export 65000:100
route-target import 65000:100
!
interface GigabitEthernet1/1
 ip vrf forwarding voice
 ip address 10.10.1.5 255.255.255.252
!
```

3.2.3.3.3 *Configuración de RIP v2 para enrutamiento PE-CE*

A continuación se muestran los comandos de configuración, para establecer la conectividad entre el PE y CE router, con el uso del protocolo RIP v2:

```
Cisco(config)# router rip
Cisco(config-router)# version 2
Cisco(config-router-af)# address-family ipv4 vrf nombre_vrf
Cisco(config-router-af)# version 2
Cisco(config-router-af)# redistribute bgp número_as metric
transparent
Cisco(config-router-af)# network red
Cisco(config-router-af)# no auto-summary
Cisco(config-router-af)# exit-address-family
```

Donde el comando "**router rip**" habilita RIP en el router PE, el comando "**versión 2**" configura el uso de RIP en su versión 2. A continuación se procede a configurar el enrutamiento para la instancia VRF sobre un grupo llamado familia de direcciones IPv4 con el comando "**address-family ipv4 vrf** nombre_vrf".

Las rutas MP-BGP se importan en la VRF del cliente mediante el comando "**redistribute bgp** número_as **metric** transparent", el cual redistribuye las rutas en RIP para anunciar los sitios conectados del cliente, la métrica es un parámetro importante para poder ser distribuido por MP-BGP, ya sea un valor de métrica o el valor "transparent" que asegura que las métricas que se anuncian por MP-BGP se conserven y se distribuyan en RIP sin modificar.

El resto de comandos es la configuración estándar del protocolo, como el comando "**network**", el cual habilita las redes para RIP, mientras que el comando "**no auto-summary**" es utilizado para que las redes no se sumaricen en los bordes de la red principal.

A continuación se presenta un ejemplo de la configuración de RIPv2 que se hará uso en la prueba diseñada:

```
router rip
version 2
 !
address-family ipv4 vrf voice
redistribute bgp 65000 metric 0
network 10.0.0.0
no auto-summary
version 2
exit-address-family
```

3.2.3.3.4 *Configuración de OSPF para enrutamiento PE-CE*

En el caso de establecer OSPF como protocolo de enrutamiento entre el PE y CE, se tiene que establecer un proceso OSPF por separado para cada instancia VRF de cliente y cuya configuración se muestra a continuación:

```
Cisco(config)# router ospf id_proceso vrf nombre_vrf
Cisco(config-router)# redistribute bgp número_as subnets
Cisco(config-router)# network network wildcard area 0
```

El primero de los comandos "**router ospf** id_proceso **vrf** nombre_vrf" habilita un proceso ospf para una vrf, el siguiente comando al igual que en RIPv2, se utiliza para redistribución de las rutas MP-BGP (rutas de sitios remotos), pero en el proceso respectivo de OSPF para anunciar los sitios del cliente conectados, dicho comando es "**redistribute bgp** número_as **subnets**", donde la palabra clave "subnets" permite asegurar tanto las subredes y redes, y no solo las redes principales sean distribuidas.

El resto de comandos son la configuración estándar para el protocolo, en donde el comando "**network** network wildcard **area** 0", habilita las redes para el proceso OSPF respectivo a ser compartidas.

A continuación se presenta un ejemplo de la configuración de OSPF que se hará uso en la prueba diseñada:

```
router ospf 1 vrf voice
log-adjacency-changes
redistribute connected
redistribute static
redistribute bgp 65000 subnets
network 10.10.1.0 0.0.0.7 area 0
```

3.2.3.4 Redistribución de rutas de cliente en MP-BGP [12]

Como paso final en las configuraciones de una VPN MPLS de capa 3 está el redistribuir las rutas de los Clientes aprendidas por los diferentes protocolos de enrutamiento entre PE y CE, cuya configuración se muestra a continuación:

```
Cisco(config)# router bgp sistema_autónomo
Cisco(config-router)# address-family vpnv4
Cisco(config-router-af)# neighbor <dirección_IP> activate
Cisco(config-router-af)# neighbor <dirección_IP> send-community
extended
Cisco(config-router-af)# no auto-summary
Cisco(config-router-af)# exit-address-family
Cisco(config-router)# address-family ipv4 vrf nombre_vpn
Cisco(config-router-af)# redistribute [ospf|bgp|rip|eigrp|
connected|static] [id_prceso|número AS]
Cisco(config-router-af)# no auto-summary
Cisco(config-router-af)# no synchronization
Cisco(config-router-af)# exit-address-family
```

En la primera parte de configuraciones se muestra la habilitación de MP-BGP, el comando "**address-family vpnv4**" es usado para entrar en el modo de configuración de la famillla de direcciones VPNv4, para luego habilitar el intercambio MP-BGP con un router PE remoto que comparta la VPN mediante el comando "**neighbor** <dirección_IP> **activate**" donde la dirección IP es de dicho Router PE remoto.

El comando "**neighbor** <dirección_IP> **send-community extended**" se encuentra configurado por defecto y permite el intercambio de comunidades extendidas de BGP, tales como la ruta destino "route target" y sitio de origen, pero si se desea que también se intercambien comunidades estándares de BGP, se remplaza la palabra clave "extended" por la palabra "both", para finalizar esta primera configuración se tiene el comando "**no auto-summary**", el cual se configura por defecto y sirve para especificar que las rutas redistribuidas no deben ser sumarizadas en una única red principal en el border de la red.

El siguiente paso es configurar los parámetros de redistribución de rutas de una VRF en específico, para lo cual la vrf se le asigna a una familia de direcciones con el comando "**address-family ipv4 vrf** nombre_vpn".

El siguiente comando especifica el tipo de rutas que se permitirán redistribuir por MP-BGP, lo cual dependerá del protocolo de enrutamiento configurado entre el PE y CE, las posibles configuraciones que se tiene son:

"**redistribute rip**" es usado para redistribuir rutas de Cliente aprendidas con RIPv2 en MP-BGP, "**redistribute osp** id_proceso **vrf** nombre_vrf" se usa para redistribuir dentro de MP-BGP las rutas aprendidas por el respectivo proceso OSPF asignado a la VRF.

Y si se está usando rutas estáticas entre el PE y CE el comando de configuración que permite la redistribución de las rutas aprendidas es "**redistribute static**", en el caso de que se quieran redistribuir las rutas de los equipos conectados directamente al PE existe también el comando "**redistribute connected**".

Para finalizar la configuración de esta familia de direcciones se tienen los comandos "**no auto-summary**" y "**no synchronization**" los cuales están configurados por defecto y permiten la no sumarización de rutas y deshabilitar la sincronización.

Al haber configurado los parámetros indicados, el funcionamiento de la VRF en el *backbone* MPLS debe encontrarse habilitado, y simplemente el cliente debe configurar su equipo de frontera (CE) con el protocolo de enrutamiento apropiado y que se encuentra manejando con el equipo del Proveedor de Servicios para comenzar a generar el tráfico entre sus sitios remotos.

A continuación se presenta un ejemplo de la configuración de MP-BGP para la redistribución de rutas aprendidas por RIPv2 y OSPF, similar a la que se utilizará en la prueba diseñada:

```
router bgp 65000
 no synchronization
 bgp log-neighbor-changes
 neighbor 10.30.10.10 remote-as 65000
 neighbor 10.30.10.10 update-source Loopback100
 no auto-summary
 !
 address-family vpnv4
 neighbor 10.30.10.10 activate
 neighbor 10.30.10.10 send-community both
```

```
 exit-address-family
 !
 !Para el caso de que el protocolo de enrutamiento PE-CE sea RIPv2
 !la redistribucion se establece a continuacion
 !
 address-family ipv4 vrf voice
 redistribute rip
 no synchronization
 exit-address-family
 !
 !Para el caso de que el protocolo de enrutamiento PE-CE sea OSPF
 !la redistribucion se establece a continuacion
 !
 address-family ipv4 vrf voice2
 redistribute ospf 1 vrf voice2
 no synchronization
 exit-address-family
!
```

3.2.4 DISEÑO DE ESQUEMAS DE RED PARA PROBAR QoS [13][19]

La necesidad de ofrecer servicios convergentes voz, video y datos, bajo una misma infraestructura de red, ha llevado a que los proveedores de servicio utilicen QoS para garantizar que se cumplan los requerimientos específicos de cada uno de los flujos de tráfico dentro de sus redes.

Al implementar calidad de servicio se asegura que los paquetes de aplicaciones como VoIP, videoconferencia, navegación web, transacciones sobre bases de datos, etc. tengan los parámetros de ancho de banda, retardo, pérdida de paquetes, etc. que necesitan ser asegurados.

Otra de las razones para utilizar QoS es que los recursos necesarios en una red WAN son costosos, por lo que se necesita realizar un uso óptimo de los mismos. A continuación se elaboran pruebas que permiten observar la manera de utilizar y configurar los diferentes algoritmos de QoS disponibles en los equipos Cisco del laboratorio.

Para dar QoS en una red lo principal es definir el tipo de comportamiento que se tendrá para cada flujo de tráfico en los diferentes nodos, para esto es importante especificar la cantidad de recursos que se destinarán para cada flujo, el modelo comportamiento de Cisco nos brinda una abstracción para entender la manera de

implementar QoS en los routers de una red, se lo detalla a continuación y se lo toma como base para la elaboración de las pruebas.

3.2.4.1 Modelo de comportamiento de QoS de Cisco [7]

Existen varios métodos para implementar calidad de servicio en una red de datos los cuales de detallaron en el capítulo 2, estos modelos se utilizarán en un red MPLS para dar QoS en los flujos de tráfico. Para realizar una implementación de QoS consistente en lo diferentes elementos de la red, Cisco define un modelo de comportamiento de QoS.

El modelo de QoS se basa en el concepto de *traffic-management node* (TMN). Este concepto es una abstracción de un conjunto de acciones que un equipo aplica a uno o más flujos de tráfico en un punto particular durante el envío de los paquetes. TMN identifica uno o más flujos de tráfico y define las acciones que se realizarán para cada flujo. El modelo TMN mostrado en la figura 3.14 tiene cuatro componentes: clasificación, pre encolamiento, encolamiento y post encolamiento, todos opcionales y configurables.

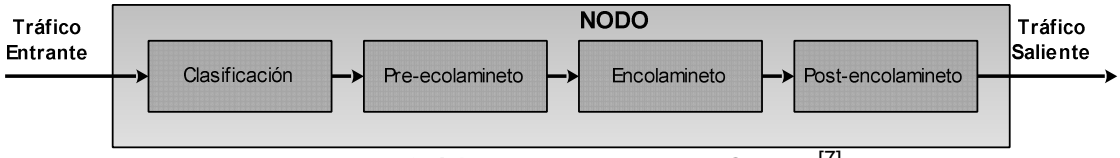


Figura 3.14: Modelo TMN de Cisco. [7]

Un paquete puede encontrar cero o más TMN al atravesar un equipo, los puntos más comunes donde un paquete encuentra un TMN en las interfaces de entrada y salida de un equipo, pues es en estos puntos es donde se producen eventos de congestión con mayor frecuencia.

3.2.4.1.1 *Componente de clasificación*

El primer componente recibe un agregado de tráfico y se encarga de clasificarlo en flujos, para determinar que paquetes se asignan a un determinado flujo usa la información que contiene un paquete, comúnmente se usan las cabeceras de capa dos, tres o cuatro, también puede usarse la información de contexto como la interfaz de entrada.

El TMN asocia cada flujo de tráfico con una clase a la que se le asigna nombre, en caso de que un paquete no coincida con los criterios de clasificación será parte de la clase por defecto, cuyo nombre en los equipos Cisco es *class-default*, en caso de ausencia de este componente todo el tráfico ira a la clase por defecto.

3.2.4.1.2 *Componente de pre encolamiento*

Este componente agrupa un conjunto de acciones de QoS como el *policing*, el marcado el descartarte y la compresión de la cabecera de un paquete, afecta la operación de los componentes subsecuentes, no obliga a la existencia del encolamiento y no afecta el resultado del componente de clasificación por lo que no realiza una reclasificación de paquetes.

3.2.4.1.3 *Componente de encolamiento*

También opcional se encarga de la administración del ancho de banda disponible en periodos de congestión, e incluye dos subcomponentes: *enqueuing y dequeuing*. Los subcomponentes usan un conjunto de parámetros para controlar como el tráfico entra y sale de la cola si TMN está ubicado en un punto donde no ocurre congestión este componente no es necesario.

Componente de *enqueuing:* Este componente se encarga de controlar el tamaño de la cola y decidir que paquetes ingresan en la cola. Por ejemplo al establecer el máximo tamaño de una cola se instaura una forma de control que implementa una política de control *tail drop*[17].

Componente de *denqueuing:* Este componente se encarga de controlar la forma en que los paquetes salen de una cola, cuatro atributos pueden influenciar en la forma de desencolar:

- El mínimo ancho de banda garantizado que representa el ancho de banda que la cola recibirá en el peor de los casos.

[17] Este tipo de encolamiento acepta paquetes hasta que alcanza en máximo tamaño de la cola, los paquetes que arriben a partir de este punto se descartan y solo se aceptan otros si la cola tiene capacidad para aceptar nuevo tráfico.

- En ancho de banda máximo define la asignación de ancho de banda para una cola en el mejor de los casos.
- El exceso de ancho de banda define la distribución del sobrante de esta más allá del mínimo garantizado.
- El atributo de prioridad define que una cola debe ser atendida antes de otras colas con menor prioridad.

En TMN se puede utilizar un administrador de dos parámetros o uno de tres parámetros. Se usa el de dos parámetros si los valores establecidos para el ancho de banda mínimo y máximo son independientes, el valor asignado al ancho de banda en exceso depende de uno de estos dos. El administrador de tres parámetros soporta la configuración independiente de la cantidad de ancho de banda mínimo, máximo y exceso para cada cola.

Una cola ofrece mejores prestaciones de latencia y jitter si recibe más ancho de banda en exceso. Se tienen valores por defecto dentro del modelo TMN, si no se configura el ancho de banda mínimo no se garantiza nada para una cola, en cambio en ausencia de un máximo la cola recibe todo el ancho de banda disponible.

En el caso del ancho de banda en exceso hay dos variantes, si se configura de tres parámetros, el ancho de banda en exceso se comparte de manera equitativa entre otras, en cambio si se usa dos parámetros el ancho de banda se comparte de manera proporcional al mínimo ancho de banda garantizado. Si no existe este parámetro se reparte de manera equitativa entre las colas.

3.2.4.1.4 *Componente de post encolamiento*

Este define el último grupo de acciones antes de que el paquete abandone el TMN, se usa este componente cuando la secuencia de los paquetes es importante, dado que el componente de encolamiento generalmente reordena los paquetes en las diferentes colas, es importante reordenarlos para que se mantenga la secuencia con la que ingresa al TMN. Por ejemplo en los métodos de

compresión se numeran los paquetes, los mismos que se ordenan en este componente para su transmisión.

3.2.4.2 Objetivo

En este escenario se procede a realizar algunas pruebas para observar cómo responden los algoritmos de QoS a diferentes flujos de tráfico y eventos de congestión. Se realizará *traffic policing*, marcado del tráfico, manejo de congestión y *traffic shaping*.

3.2.4.3 Esquema de red para probar QoS

Las condiciones necesarias para la topología de QoS se detallan a continuación:

- Se colocan dos routers LERs (Cisco 6500), y dos LSRs (Cisco 7600 y Cisco 12000).
- Todos lo routers dentro de la red se interconectan con enlaces de fibra giga bit Ethernet.
- Se configurará IS-IS, LDP, MPLS en los routers de la red del proveedor servicios.
- Se utilizan dos generadores de tráfico, tres interfaces de estos se conectan a los routers PEs para simular las localidades de los clientes.
- Para interconectar las localidades de los clientes se utilizan VRFs.
- Se utiliza OSPF como protocolo de enrutamiento dentro las VRFs.

Las configuraciones básicas necesarias de direccionamiento IP, MPLS, LDP e ISIS son las mismas que se describieron en el escenario de habilitación de un backbone MPLS por lo que no se detallarán al respecto, para realizar las pruebas de QoS se aumentan generadores de tráfico en los routers de frontera, para de esta manera visualizar el comportamiento de la red frente a eventos simulados de congestión.

Un cambio que se introdujo respecto al escenario en el que se habilita MPLS es el cambio del router Cisco CRS-1 por un Cisco 7600, este cambio se realiza con la

finalidad de mostrar que para las configuraciones de QoS se realizan de la misma manera tanto en el IOS como en el IOS XR.

Los generadores de tráfico mostrados en la figura están conectados a cada nodo PE, y cada interfaz de los generadores representa un cliente, el tráfico se envía del lugar 1 al lugar 2 del mismo cliente, para esto se tendrá una VRF para cada cliente, se tendrán 3 procesos OSPF habilitados en cada PE, cada uno de estos se relacionará con una VRF y será el encargado de realizar el enrutamiento para que se alcancen las diferentes localidades del cliente, el direccionamiento IP usado para las VRF y las interfaces de los generadores se muestra en la tabla 3.21.

DIRECCIONAMIENTO IP			
EQUIPO	**INTERFAZ**	**DIRECCIÓN IP**	**MÁSCARA**
PE1	Gi 1/1	192.168.9.1	255.255.255.0
	Gi ½	192.168.10.1	255.255.255.0
	Gi 1/3	192.168.11.1	255.255.255.0
PE2	Gi 1/1	192.168.3.1	255.255.255.0
	Gi ½	192.168.4.1	255.255.255.0
	Gi 1/3	192.168.5.1	255.255.255.0
IXIA1	Gi 2/1	192.168.9.2	255.255.255.0
	Gi 2/2	192.168.10.2	255.255.255.0
	Gi 2/3	192.168.11.2	255.255.255.0
IXIA2	Gi 2/1	192.168.3.1	255.255.255.0
	Gi 2/2	192.168.4.1	255.255.255.0
	Gi 2/3	192.168.5.1	255.255.255.0

Tabla 3.21- Direccionamiento IP de las VRF.

Se utilizan VRFs para intercambiar el tráfico entre clientes con la finalidad de mostrar que para ofrecer QoS no importa que este pertenezca a una VPN, sino que un tráfico se lo clasifica y asigna una clase dependiendo de ciertos criterios de selección que decida usar el proveedor, en las pruebas los generadores envían los paquetes marcados, de manera que el proveedor en base a estos campos pueda distinguir el tipo de tráfico y darle el tratamiento adecuado. En la figura 3.15 se observa la topología diseñada para probar QoS.

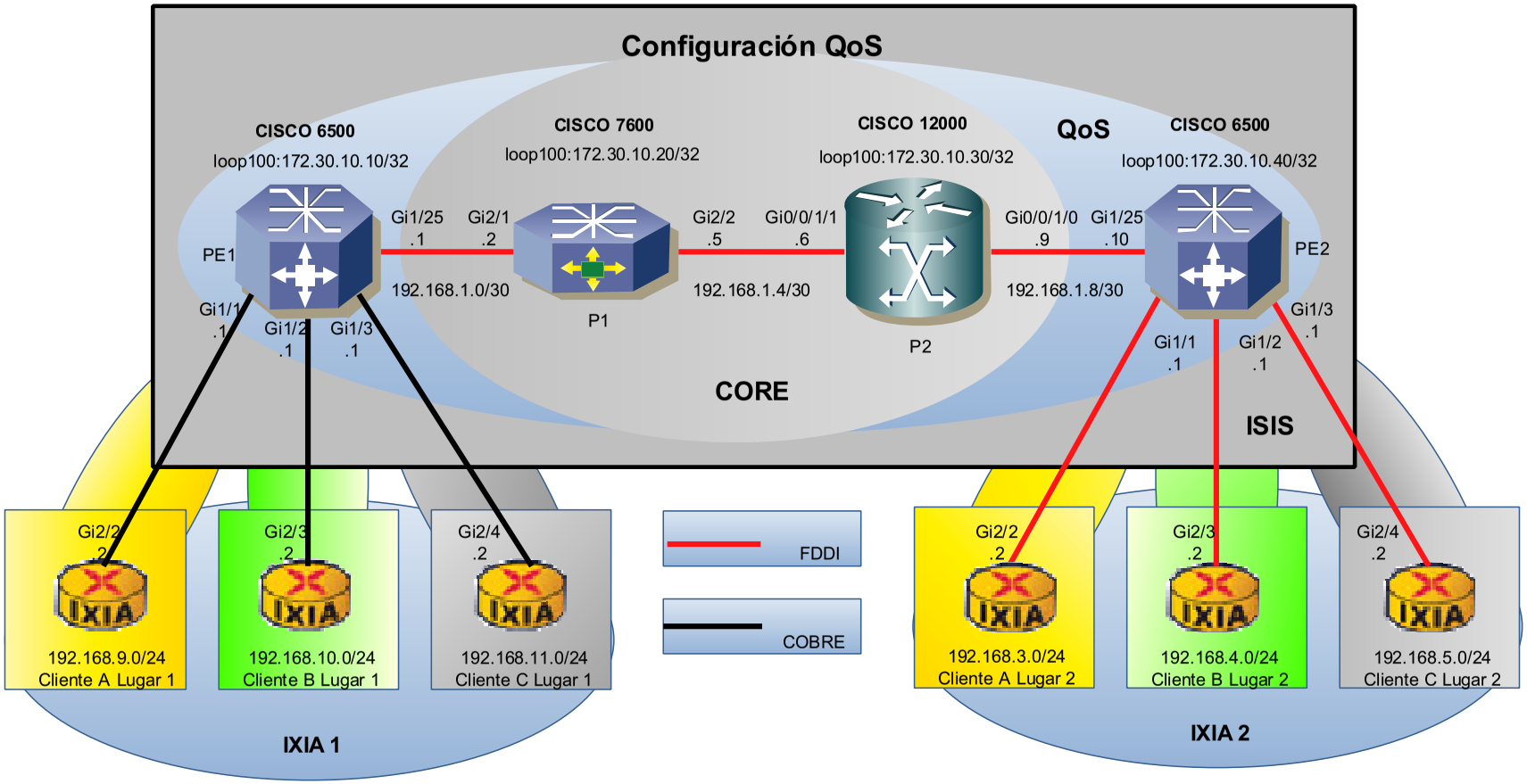


Figura 3.15: Topología para probar QoS

Las diferentes funcionalidades de QoS disponibles en los routers dependen de las características específicas de los equipos y de las tarjetas que los integran, por lo que las pruebas a desarrollar se realizan en función de las características de QoS disponibles.

Los equipos Me6500 utilizados como routers PEs son *switches* de capa 3, por lo que poseen limitadas funcionalidades de QoS, en estos equipos se realizarán las pruebas de marcado de tráfico, y las de *trafficc policing.*

3.2.4.3.1 *Pruebas de traffic policing*

Para la realización de esta prueba se utilizan los dos generadores de tráfico, conectados en los nodos PEs de la topología, se utilizan dos de las tres interfaces del generador IXIA1, Gi2/2 que representa una localidad, se conecta a Gi1/1 de UIOLABE01, el tráfico se envía por la VRF del cliente1; Gi2/3 que representa la localidad del cliente 2, se conecta a Gi1/2 de UIOLABE02, el tráfico se envía por la VRF del cliente 2. En el generador IXIA2 se conecta a UIOLABE02 con las mismas interfaces que IXIA1 a UIOLABE01.

Del generador IXIA1 conectado al PE1 se envía un flujo de 200 Mbps por cada interfaz, el destino es el generador IXIA2 conectado al PE2, en este generador se graficará el tráfico entrante en cada interfaz para observar como las *traffic policing* limitan el tráfico que ingresa a un equipo. Para la realización de los gráficos se toma en cuenta que el tráfico enviado por Gi2/2 del IXIA1 se recepta en la Gi2/2 del IXIA2, de la misma manera el tráfico de Gi2/3 de IXIA1 se recepta en Gi2/3 de IXIA2.

Se crearon límites de 10, 15, 25, 45, 60, 70, 75, 80, 90 y 100 Mbps, con la finalidad de mostrar que se puede configurar cualquier valor y que los resultados serán los mismos, esto permite tener gran flexibilidad en las velocidades que se ofrecen a los clientes de un proveedor de servicios, los *traffic policing* se utilizan para controlar que el tráfico no exceda los parámetros suscritos en un SLA.

3.2.4.3.2 *Prueba de Marcado y clasificación del tráfico*

Se decidió crear tres clases de tráfico, los nombres asignados para estas fueron: DatosCriticos, Datos y DatosNoCriticos y como su nombre lo indica habrá tráfico que tendrán mayor importancia y por lo tanto necesitará un mejor tratamiento dentro de la red. Para asegurar mejores características de envío y que las pérdidas sean menores se asignará la mayor cantidad de recursos a la clase DatosCriticos, una asignación intermedia a Datos y la menor cantidad a DatosNoCriticos.

Para realizar una distinción del tráfico en los routers de frontera se utiliza precedencia IP, el marcado de los paquetes se realiza en los generadores de tráfico, que se encargan de asignar un valor a este campo al momento de generarlos. Los valores que se asigna son: en el IXIA 1 la interfaz Gi2/2 marcará con 3, Gi2/3 con 1 y Gi2/4 con 5 en cambio para el IXIA 2 Gi2/2 marcará con 1, Gi2/3 con 3 y Gi2/4 con 5.

Esta asignación de valores tiene como objetivo mostrar que la clasificación de los paquetes que pertenecen a una clase se la realiza por lo marcado en los campos específicos utilizados por QoS y que el hecho de tener una VRF no implica que todo el tráfico que ésta genere se asigne a una clase.

En los routers de frontera, los criterios de coincidencia para realizar la clasificación de los paquetes será la precedencia IP, se utiliza precedencia IP ya que como se observó en el capítulo 2 dentro de la red de CNT se encuentra en uso este modelo de QoS. Los paquetes marcados con el valor 5 pertenecerán a la clase DatosCriticios, los que tengan el valor de 3 serán de la clase Datos y los que tengan el valor de 1 serán de clase DatosNoCriticos.

En los routers PE se realiza el marcado del campo EXP con los mismos valores que se tienen en la precedencia del paquete IP, este marcado se lo realizará en una política de salida, pues la operación push en los Me 6500 (usados como PE) se la realiza al salir de la interfaz. Con esto se cambia el valor del campo EXP para enviarlo a nodos P.

En cambio en los routers P se utilizará en campo EXP para realizar la distinción de los flujos y dar un tratamiento adecuado. La clasificación para determinar que paquetes pertenecen a una clase, se efectúa de manera similar a lo realizado en los nodos PEs, esto es: paquetes con EXP 1 pertenecen a DatosNoCriticos, con EXP de 3 a Datos y con EXP igual 5 a DatosCriticos.

3.2.4.3.3 *Manejo de congestión y traffic shaping.*

En la primera parte se muestra el comportamiento de los equipos en ausencia de QoS, para realizar estas pruebas se mantiene la utilización y conexión de los dos generadores que se utilizaron para la prueba del *traffic policing,* para observar cómo se comportan los equipos frente a un evento de congestión sin ningún parámetro de QoS se retiraron todas las políticas de las diferentes interfaces.

Se utilizó un único generador de tráfico, dos interfaces envían el tráfico Gi2/3 y Gi2/4, se las conectó a Gi1/1 y Gi1/2 de UIOLABE01 respectivamente; dos interfaces Gi2/1 y Gi2/2 reciben el tráfico que circula por la red, están conectadas a Gi1/1 y Gi1/2 de UIOLABE02 respectivamente. En las interfaces Gi2/3 y Gi2/4 se configura un flujo de 780Mbps y 980Mpbs respectivamente, estos flujos saturarán los enlaces disponibles, permitiendo observar el comportamiento por defecto de los equipos cuando existe cogestión en la red.

En un segunda parte se procede a crear políticas que asigna recursos a cada equipo. La asignación de recursos en el router P1 y P2 se realizará de la siguiente manera:

- Para la clase DatosNoCriticos se asegura un mínimo ancho de banda del 10 %.
- Para la clase Datos se asegura un ancho de banda mínimo del 20%.
- Para la clase Datos críticos se asegura un ancho de banda mínimo de 30%.

Los valores anteriormente expuestos se tomaron de las políticas que CNT tiene implementadas en su red, esto se observó en el capítulo 2. Esta asignación se

realiza para mantener la asignación de recursos descrita en la elaboración de la prueba del marcado y clasificación del tráfico.

De las múltiples clases utilizadas en la red de CNT se tomaron los valores de la clase CM-Video que tiene el 30% de recursos y se la asignó a la clase DatosCriticos, se tomó el valor de 20 % asignado a la clase CM-Datosnocriticos y se los asignó a clase datos, finalmente el valor de 10% de la clase CM-Datoscriticos se lo asignó a la clase DatosNoCriticos.

En una implementación de QoS en una red, se tiene que mantener una asignación de recursos igual en todos los nodos, esto garantiza que el tráfico tenga el mismo tratamiento en todos los saltos.

En los nodos PE no se realiza una asignación de recursos para las clases debido a las limitadas características de QoS de las que disponen los equipos ME6500.

La comprobación del adecuado funcionamiento de las políticas se las realiza en UIOLABP02 (Cisco 12000), este router utiliza tarjetas SIP para conectarse a UIOLABP01 y UIOLABE02. Se realizan las pruebas en las tarjetas SIP porque dentro de la red de CNT se usan para la interconexión entre los diferentes equipos de núcleo, acceso y distribución. En las interfaces de estas SIP se colocan las políticas de QoS a probar.

Para realizar las pruebas de estas políticas fue necesario realizar algunos cambios en la topología y en las configuraciones de la red.

En la topología de la figura 3.16 se observa que las modificaciones introducidas respecto a la topología descrita en el capítulo 3 fueron: las interfaces Gi2/2 y Gi2/3 de IXIA 2 antes conectadas en las interfaces Gi1/1 y Gi1/2 de PE2, serán ahora conectadas a P2; se modificó el direccionamiento IP en los routers P2 y PE2, para el resto de equipos el direccionamiento se mantiene, el nuevo direccionamiento para PE2 y P2 se muestra en la tabla 3.22.

La topología de la red utilizada se muestra en la figura 3.16.

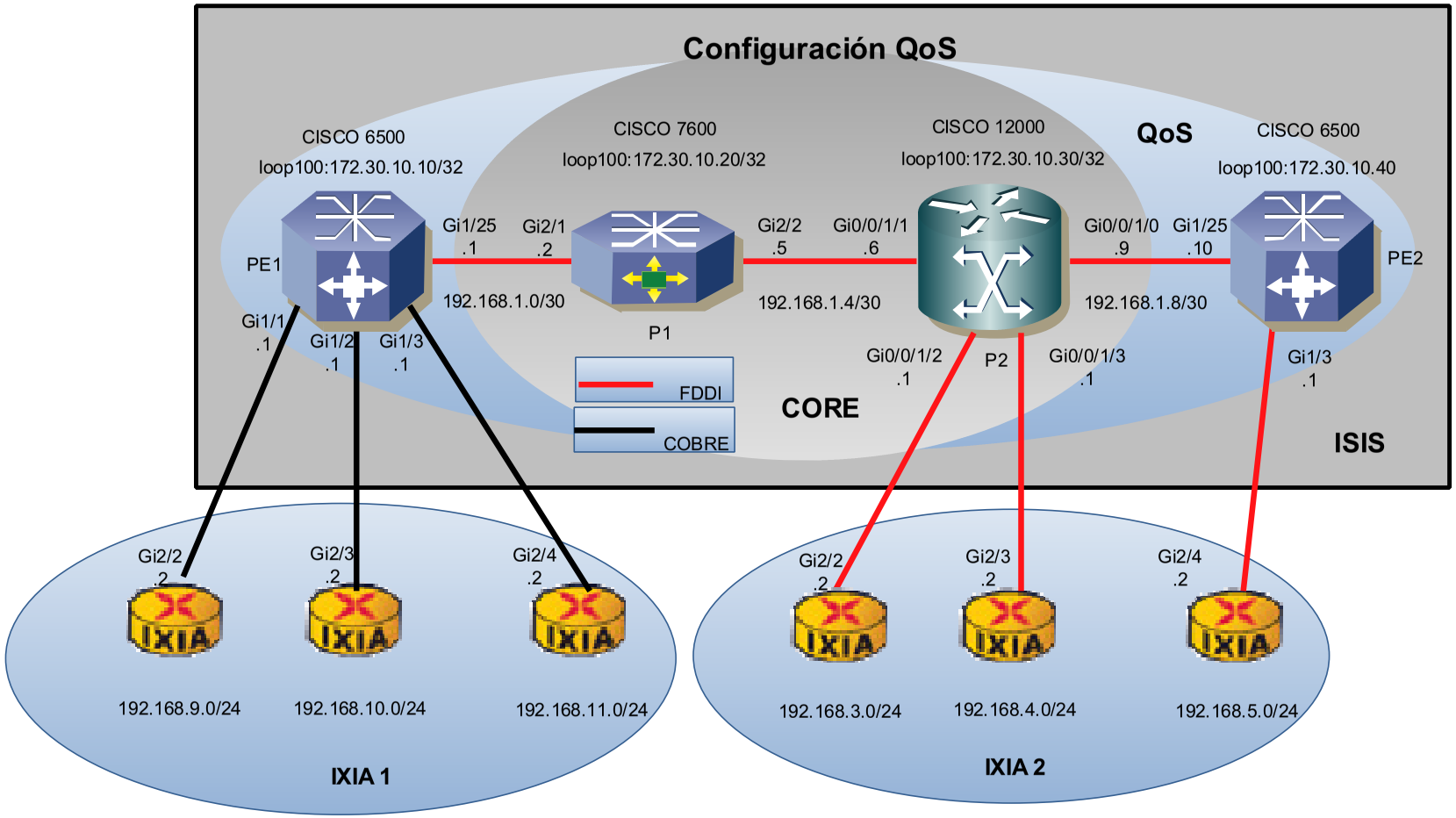


Figura 3.16: Modificación de la topología para realizar las pruebas

Se retiraron las VRFs del cliente 1 y 2 de los nodos PEs, se añadió las interfaces Gi0/0/1/2, Gi0/0/1/3 de P2 y Gi1/1, Gi1/2 de PE1 al proceso de enrutamiento ISIS, de esta manera se tendrá conectividad entre las interfaces de los generadores IXIA, permitiendo que se envié tráfico de IXIA 2 a IXIA 1, en este último se realizarán los gráficos.

En la tabla 3.22 se observa el direccionamiento IP adicional utilizado para el cambio realizado en la topología.

DIRECCIONAMIENTO IP			
EQUIPO	**INTERFAZ**	**DIRECCIÓN IP**	**MÁSCARA**
P2	Gi 0/0/1/0	192.168.1.9	255.255.255.252
	Gi 0/0/1/1	192.168.1.6	255.255.255.252
	Gi 0/0/1/2	192.168.3.1	255.255.255.0
	Gi 0/0/1/3	192.168.4.1	255.255.255.0
PE2	Gi 1/3	192.168.5.1	255.255.255.0
	Gi 1/25	192.168.1.10	255.255.255.252

Tabla 3.22- Direccionamiento IP router "P2 y PE2"

Estas modificaciones fueron necesarias porque la política se aplicó en la interfaz Gi0/0/1/1 de P2 y se necesita crear congestión para esa interfaz, si se mantenía la anterior configuración la congestión se hubiera creado en la interfaz Gi1/25 de PE2 y no se podría probar las políticas.

3.2.4.4 Interfaz de línea de comandos modular para QoS [7][18]

El IOS e IOS XR de Cisco usan *Modular QoS Command-Line Interface* (MQC) como plantilla para implementar el modelo de comportamiento TMN, MQC facilita la utilización de QoS suministrando un conjunto de comandos comunes con una misma sintaxis y semántica, provee una gran flexibilidad en la selección de la implementación de QoS en las plataformas, tiene tres componentes:

- `Class map`: Define una clase de tráfico basado en criterios de selección, corresponde al componente de clasificación del modelo TMN.

- *Policy map*: Define una política que contiene acciones de QoS que se aplicarán a las clases de tráfico. Provee la configuración para los componentes de pre encolamiento, encolamiento y post encolamiento del modelo TMN.
- *Police Service:* Asocia una política con un objetivo y dirección dentro de un equipo, para esto previamente se debe haber definido la política con el *policy map.* Al separar la definición de la política de la invocación de la política se reduce la complejidad. La configuración del *police service* determina el punto y la dirección en que se fijará la política, generalmente se lo une con una interfaz.

3.2.4.4.1 *Clasificación del tráfico* [7] [18]

Antes de realizar cualquier tratamiento al tráfico es necesario habilitar QoS de manera global en el router; para realizar esto se utiliza:

```
Cisco>enable
Cisco#configure terminal
Cisco(config)#mls qos
```

Para configurar la clasificación del tráfico se utiliza los comandos *class-map,* que definen el componente de clasificación del modelo TMN, estos comandos incluyen uno o más comandos *match,* que proveen un amplio rango criterios de clasificación, enmarcan un conjunto de criterios que van desde la capa enlace (por ejemplo la dirección MAC) a la capa aplicación (Por ejemplo una URL).

Dentro de un *policy* el proceso de clasificación de un paquete finaliza cuando el paquete se asigna a una clase, la clasificación asocia un paquete a una única clase, en caso de que un paquete no cumpla con ninguno de los criterios de clasificación se asigna a la clase por defecto *class-default.*

En los criterios de clasificación que usan listas de acceso, basta con que el paquete cumpla con uno de los criterios configurados en la lista de acceso para que sea considerado parte de una clase.

En la tabla 3.23 se observa los comandos disponibles para realizar esta tarea.

Sintaxis	Descripción
class-map nombre_clase	Crea una clase de tráfico con un nombre asignado por el usuario. El nombre puede tener una máximo de 40 caracteres, en este caso el tráfico debe cumplir con todos los criterios de clasificación para ser parte de la clase.
class-map match-all nombre_clase	Indica que un paquete debe cumplir con todos los criterios de clasificación para ser parte de una clase similar a un and.
class-map match-any nombre_clase	Indica que un paquete al menos debe cumplir con un criterio de clasificación para pertenecer a una clase similar a un or.
match any	Indica que cualquier paquete cumple con el criterio.
match access-group { valor| **name** *valor* }	Utiliza como criterio de clasificación una lista de acceso nombrada o numerada.
match access-group [ipv4| ipv6]valor	Utiliza como criterio de clasificación una lista de acceso en el IOS XR.
match precedence list	Selecciona los paquetes que tienen el valor de precedencia IPv4 o IPv6 iguales a los listados.
match mpls experimental topmost list	Selecciona los paquetes que tienen el valor de campo EXP de MPLS iguales a los listados.
match input-interface *value*	Selecciona los paquetes basado en la interfaz por la que arriban.

Tabla 3.23- Criterios para crear un class-map.[7]

A continuación se expone la manera de configurar las clases de tráfico y los criterios de coincidencia que se utilizan para seleccionar los paquetes que son parte de las clases:

```
Cisco#configure terminal
Cisco(config)#class-map <nombre_clase>
Cisco(config-cmap)#match <sentecia_coincidencia>
Cisco(config)#class-map match-any <nombre_clase>
Cisco(config-cmap)#match <sentecia_coincidencia>
Cisco(config-cmap)#match <sentecia_coincidencia>
```

Las sentencias anteriores presentan una manera genérica de configurar las diferentes clases, en el parámetro <nombre_clase> puede ir cualquier cadena de caracteres, en la <sentencia_coincidencia> va uno de los criterios de coincidencia de la tabla 3.23, no se limita el número de criterios (match), sino que se pueden tener los que sean necesarios para elegir que tráfico pertenece a una clase.

3.2.4.4.2 *Marcado del tráfico* [18] [32]

Esta es una de las acciones del componente de pre encolamiento del modelo TMN, para realizar el marcado de los campos de un paquete se usa el comando *set,* que soporta una amplia gama de criterios de marcado, incluyendo campos de capa 2, capa 3 e internos. Una clase puede incluir múltiples comandos *set* para marcar diferentes campos en la tabla 3.24 se listan algunos de los comandos *set*.

Sintaxis	Descripción
set precedence *value*	Cambia el valor de la precedencia IPv4 e IPv6
set mpls experimental imposition *value*	Coloca el valor señalado en el campo EXP en todas las etiquetas que se impongan en el paquete.
set mpls experimental topmost *value*	Cambia el valor del campo EXP en la cima del stack.

Tabla 3.24- Comandos para marcar el tráfico.[7]

En MPLS un nodo automáticamente marca el campo EXP de MPLS durante las operaciones de encapsulamiento, al realizar una operación de *push* se establecerá el campo EXP (en todas las etiquetas impuestas) de acuerdo a lo marcado en el paquete encapsulado. El valor colocado en la etiqueta corresponderá con el campo EXP existente en un paquete MPLS, con el campo precedencia IP en un paquete IP, o con el campo prioridad de usuarios en un paquete 802.1q de una trama Ethernet.

En una operación de swap se conserva el valor existente en el campo EXP, en una operación pop no se realiza un marcado en la cabecera expuesta, se mantiene como está.

Este es el comportamiento que se tiene por defecto cuando no se realiza la configuración de un marcado explicito, se altera al usar los comandos *set.* Si se coloca el comando *set mpls experimental topmost* en una política de entrada se marca el paquete antes de que se realicen las operaciones de envío MPLS (*pop*, *swap* y *push*), en cambio si se lo coloca en una política colocada en la salida lo marcará después de que todas las operaciones de envío se hayan realizado.

En caso de usar un *set mpls experimental imposition,* no se realizará el marcado del paquete hasta que se lleve a cabo una operación de *push*, al colocar la etiqueta esta tendrá el campo EXP con el valor especificado por el comando.

A continuación se muestra la manera de configurar un *policy map* que realiza las operaciones de marcado*:*

```
Cisco#configure terminal
Cisco(config)#policy-map <nombre>
Cisco(config-pmap)#class <nombre_clase>
Cisco(config-pmap-c)#set <sentencia>
Cisco(config-pmap)#class <nombre_clase>
Cisco(config-pmap-c)#set <sentencia>
Cisco(config-pmap-c)#set <sentencia>
```

Como se observa en las configuraciones lo primero que se realiza es crear un *policy map* y asignarle un nombre, dentro de este se configura las acciones para las diferentes clases de tráfico.

Las clases de tráfico debieron ser creadas con anterioridad y contendrá los criterios de clasificación de los paquetes, las acciones configuradas dentro de una clase se realizarán para los paquetes que son parte de esta.

3.2.4.4.3 *Traffic Policing* [7]

El comando *police* vigila que el flujo de tráfico cumpla con un perfil, procesa los paquetes basándose en la comparación con el perfil, es la manera práctica de implementar CAR definido en el capítulo 2.

Es otra de las acciones del componente de pre encolamiento en el modelo TMN. Es el encargado de definir los límites de la tasa de tráfico que ingresan a una

clase, para realizar el control del tráfico existen varias sintaxis mostradas en la tabla 3.25.

Sintaxis	Descripción
police rate-value [bc-value [be-value]]	Definición de *pólice* en términos absolutos con una sintaxis compacta.
police cir value [**bc** value [**be** value]]	Definición de *pólice* en términos absolutos con las palabras clave.
police cir percent value [**bc** value ms [**be** value ms]]	Definición de *pólice* en términos relativos al ancho de banda señalado.

Tabla 3.25- Comandos que permiten limitar el tráfico. [7]

El algoritmo *token bucket* permite realizar el control del tráfico, los valores cir y bc determinarán el tráfico que cumple con el perfil, el valor be define el tráfico en exceso, todos los valores de los parámetros están en bps.

Todo tráfico que exceda los valores especificados por estos parámetros se considera tráfico que viola el perfil, para cada tipo de tráfico se puede realizar una acción diferente. A continuación se muestra un ejemplo de cómo se debería de configurar y asociarlo a una clase.

```
Cisco#configure terminal
Cisco(config)#policy-map <nombre_politica>
Cisco(config-pmap)#class <nombre_clase1>
Cisco(config-pmap-c)#police <perfil de tráfico>
Cisco(config-pmap-c-police)#conform-action <acción>
Cisco(config-pmap-c-police)#exceed-action <acción>
Cisco(config-pmap-c-police)#violate-action <acción>
Cisco(config-pmap)#class <nombre_clase1>
Cisco(config-pmap-c)#police <perfil de tráfico>
Cisco(config-pmap-c-police)#conform-action <acción>
Cisco(config-pmap-c-police)#exit
```

En las configuraciones anteriores se puede observar como el primer paso es definir un nombre para la política, después se especifica la clase de tráfico para la que se realizará el control, y se definen las diferentes acciones a tomar en caso de que el tráfico este conforme, exceda o viole el perfil, se pueden definir varios perfiles para cada una de clases creadas.

Las acciones que se pueden realizar dentro de un *pólice* se describen en la tabla 3.26.

Acción	Descripción
Drop	Descarta los paquetes
Transmit	Transmite los paquetes sin modificaciones
set-mpls-exp-imposition-transmit valor	Marca el campo EXP al colocar una nueva etiqueta
set-mpls-exp-topmost-transmit valor	Marca el campo EXP de la etiqueta en la cima de la pila
set-prec-transmit valor	Marca el campo precedencia IP

Tabla 3.26- Acciones disponibles dentro de *pólice* para realizar el marcado.[7]

3.2.4.4.4 *Traffic Shaping* [18]

El comando *shape* configura un perfil para el tráfico, define el máximo ancho de banda para una clase, por lo que realiza la implementación del atributo máximo ancho de banda en la componente de encolamiento del modelo TMN.

Realiza el encolamiento de paquetes si la forma en la que arriba el tráfico excede el perfil del tráfico, el perfil se define con una tasa y una o dos ráfagas para definir el máximo ancho de banda; se dispone de las sentencias de la tabla 3.27.

Sintaxis	Descripción
shape average *rate-value* [burst]	Definición de un perfil promedio con un *token bucket* en términos absolutos y un intervalo fijo.
shape average *rate-value* [*bc-value* [*be-value*]]	Definición de un perfil promedio con un *token bucket* en términos absolutos y un intervalo variable.
shape peak *rate-val*ue [*bc-value* [b*e-value*]]	Definición de un perfil pico con un *token bucket* en términos absolutos y un intervalo variable.
shape average percent *rate-value* [bc-value ms [be-value **ms**]]	Definición de un perfil promedio con un *token bucket* en términos relativos al ancho de banda y un intervalo fijo.

Tabla 3.27- Comandos para realizar moldeado de tráfico. [7]

Se usa el comando *shape average* para cumplir una tasa máxima promedio, tiene dos versiones una de dos y otra de tres parámetros, en la primera se usa una tasa y una ráfaga para definir a *token bucket*, el intervalo de tiempo se escoge de manera automática. En la segunda opción usa una tasa (*rate-value*) y opcional bc y be, con estos se define a *token bucket* el intervalo de tiempo resulta de dividir bc para la tasa.

En cada intervalo se colocan bc *tokens* en un contenedor de tamaño bc+be, los paquetes se envían si existen los suficientes *tokens* caso contrario se encolan.

El comando **shape peak** usa la tasa pico, usa tres parámetros la tasa, bc y be, el intervalo se calcula de la misma manera que el anterior; pero la diferencia está en que se producen tokens a una tasa bc + be en cada intervalo.

Una tercera opción es la de representarle en términos relativos, en este caso se especifica la tasa como un porcentaje de ancho de banda del punto en el que colocará la política, de manera opcional se puede especificar el bc y be pero en unidades de tiempo por defecto en ms para realizar la configuración se la realiza de la siguiente manera:

```
Cisco> enable
Cisco# configure terminal
Cisco(config)#policy-map <nombre policy>
Cisco(config-pmap)#class <nombre_clase1>
Cisco(config-pmap)#shape average <parametros>
```

3.2.4.4.5 *Manejo de congestión* [7]

Se usan los comandos **bandwidth**, **bandwidth remaining percent** and **priority** para definir una política de encolamiento en el modelo MQC, se configuran el mínimo, el exceso de ancho de banda y prioridad del subcomponente de dese encolamiento del modelo TMN, se complementa con el comando *shape* descrito anteriormente.

La sentencia *bandwith* define el mínimo ancho de banda que una cola recibe en periodos de congestión, la forma simple de este define una tasa en Kbps pero

también ofrece una opción para que sea un porcentaje del ancho de banda del punto en el que se lo coloca.

La sentencia *bandwidth remaining percent* asigna el exceso de ancho de banda, se asigna un exceso en caso de que exista ancho de banda que no esté siendo usado por otras clases, la sintaxis de los comandos se muestra en la tabla 3.28.

Sintaxis	Descripción
Bandwidth *value*	Asignación del mínimo ancho de banda.
Bandwidth percent *value*	Asignación del mínimo ancho de banda relativo al ancho de banda señalado
Bandwidth remaining percent *value*	Asignación de ancho de banda en exceso.
queue-limit[*value* **[packets|bytes|cells|ms|us]**	Máximo tamaño de la cola.

Tabla 3.28- Comandos para realizar manejo de congestión.[7]

El comando **queue-limit** defiende el máximo tamaño para una cola, cuando el número de paquetes alcanza el máximo, los nuevos paquetes que arriben se descartan. En la tabla 3.28 la sintaxis y sus opciones. La manera de configurarlos dentro de un policy map es:

```
Cisco> enable
Cisco# configure terminal
Cisco(config)#policy-map <nombre policy>
Cisco(config-pmap)#class <nombre_clase1>
Cisco(config-pmap)#bandwith percent <porcentaje>
```

Para aplicar cualquier *police-map* a un interfaz se usan los siguientes comandos:

```
Cisco> enable
Cisco#configure terminal
Cisco(config)#interface <tipo de interfaz>
Cisco(config-if)#service-police input|output <nombre política>
```

Estas sentencias permiten asociar una política a una interfaz para esto primero de define el tipo de interfaz y su número, a continuación la sentencia *service-police*, asocia una *policy-map* con una interfaz.

La palabra clave input indica que la política se aplicará al tráfico que ingresa por esa interfaz y output al tráfico que sale de esta.

3.2.5 DISEÑO DE ESQUEMA DE RED PARA PROBAR INGENIERIA DE TRÁFICO (TE) [9] [12] [39]

En *Traffic Engineering* actualmente se destacan dos funciones, una es la optimización de los recursos y tratamiento de la red a diferentes tipos de tráfico (optimización de recursos de transmisión, solución de contingencias de saturación, retardo, entre otros), consiguiendo implementaciones que van más allá de la capacidad del IGP.

Otra función de *Traffic Engineering* es la restauración, en la que el Proveedor de Servicio puede proteger en forma selectiva algunos links de la red, o todos los links de la red. El concepto detrás de los mecanismos de restauración de MPLS TE es el de "*make-beforebreak*[18]", en donde el reenrutamiento de tráfico luego de una falla se realiza por un camino pre-establecido, y no en forma dinámica como sucede con el IGP.

3.2.5.1 Objetivos

Se diseñará un esquema de prueba que permita analizar las distintas prestaciones que se pueden obtener al aplicar Ingeniería de Tráfico sobre una topología que simule un backbone MPLS de un Proveedor de Servicios.

Se crean túneles de Ingeniería de Tráfico (TE) con el objetivo de manipular selectivamente los flujos de información dentro de la red, además de mostrar las diferentes formas de creación de los túneles TE.

Como un segundo punto en el diseño de la prueba se planteó la creación de túneles de backup, los cuales junto al mecanismo de restauración FRR (Fast ReRoute), permitan mostrar una solución ante fallas en los enlaces del backbone MPLS.

[18] Este proceso provee establecer una configuración en la cual una ruta de respaldo es creada antes de que la ruta principal falle, evitando de esta forma que la comunicación quede inhabilitada ante una falla de enlace en una ruta.

3.2.5.2 Esquema para probar Ingeniería de Tráfico MPLS (TE)

3.2.5.2.1 *Consideraciones del escenario de pruebas*

Las condiciones que debe cumplir la topología diseñada para permitir la implementación de Túneles de Ingeniería de Tráfico en MPLS son:

- Para el caso de la prueba se ha dispuesto de cuatro routers, dos de los cuales cumplen las funciones de Routers de Edge (PE1, PE2) y dos de Routers de Core (P1, P2), los cuales simularán una típica topología de red MPLS.
- Cada PE router se interconecta con cada uno de los routers de core “P” con un enlace Ethernet, además de un enlace Ethernet entre los P routers, para conseguir una topología P*artial Mesh.*
- Habilitar el reenvío MPLS sobre las interfaces que interconectan PE routers con P routers y entre P routers.
- Se utiliza como protocolo de enrutamiento interno (IGP) IS-IS para la distribución de rutas y LDP como el protocolo de distribución de etiquetas.

Se dispuso de cuatro routers como se muestra en la figura 3.17 para tener una topología *partial mesh*, en la cual se ofrezca redundancia a nivel de equipos de enrutamiento en el core, teniendo la posibilidad de enrutar el tráfico por diferentes rutas; para lo que se dispuso de dos P routers, a los cuales se interconectan cada uno de los PE routers, evitando la interrupción de la transmisión de información en el caso de que falle uno de los equipos de core o sus enlaces. La topología fue diseñada para permitir el balanceo de tráfico con la implementación de túneles TE, como la protección de enlaces.

La utilización de MPLS para el transporte de datos es necesaria para habilitar los túneles en modo “mpls TE”, y permitir el etiquetamiento de los paquetes en el router de cabecera del túnel, para su transporte hacia el router de egreso, en donde LDP se encarga de la distribución de las etiquetas.

En la figura 3.17 se observa la topología creada para realizar las pruebas de ingeniería de tráfico MPLS.

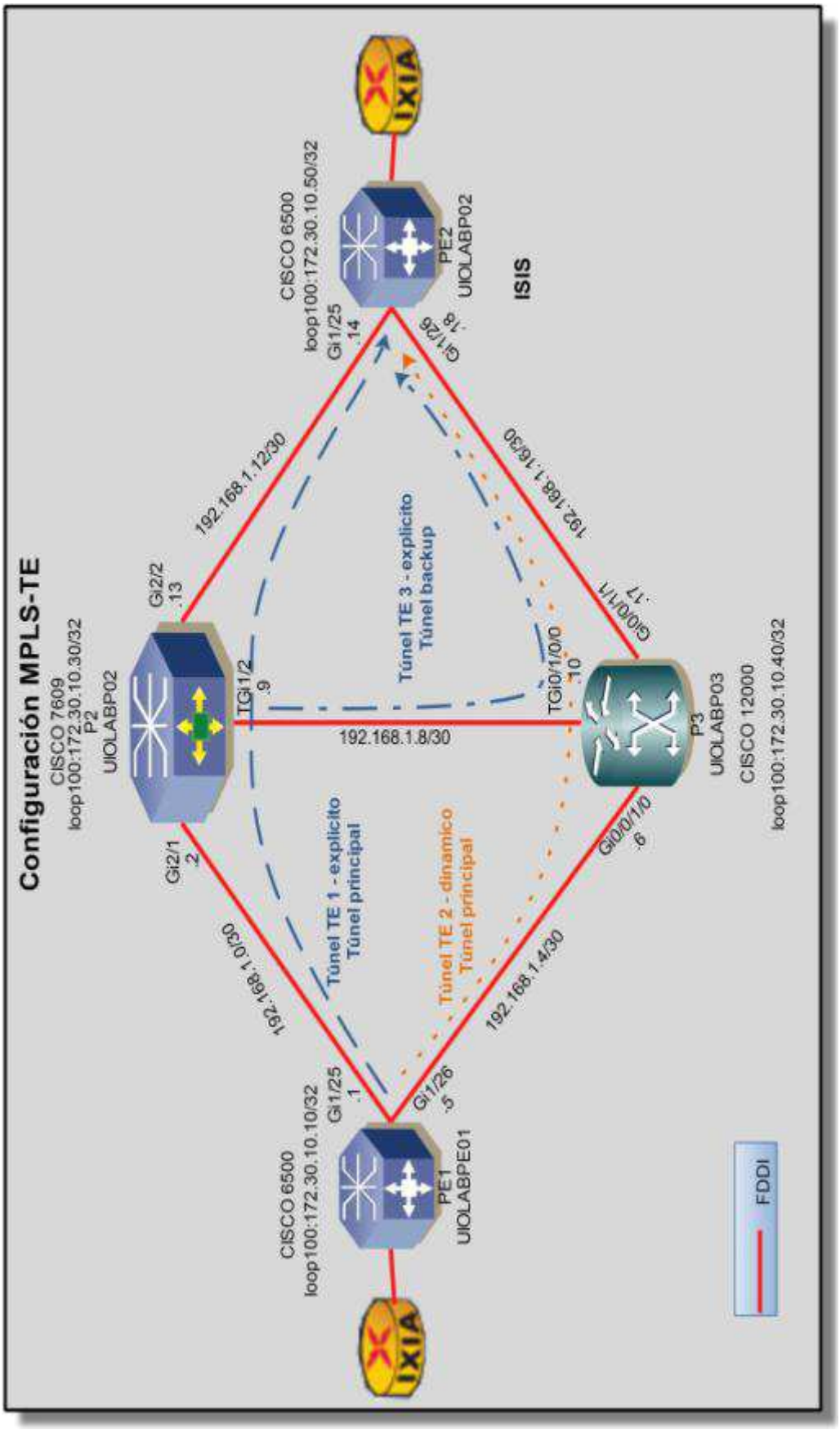


Figura 3.17: Topología de prueba MPLS-TE

Como IGP se eligió IS-IS por sus extensiones para TE que dispone, estas extensiones permiten el transporte de información sobre los recursos disponibles para la construcción de un túnel, como lo es el ancho de banda en un enlace. La tabla 3.29 muestra el direccionamiento IP asignado a cada uno de los Routers que forman parte de la topología de prueba.

DIRECCIONAMIENTO IP			
EQUIPO	**INTERFAZ**	**DIRECCIÓN IP**	**MÁSCARA**
PE1 "UIOLABPE01"	Gi 1/25	192.168.1.1	255.255.255.252
	Gi 1/26	192.168.1.5	255.255.255.252
	loop 100	172.30.10.10	255.255.255.255
PE2 "UIOLABPE02"	Gi 1/25	192.168.1.14	255.255.255.252
	Gi 1/26	192.168.1.18	255.255.255.252
	loop 100	172.30.10.50	255.255.255.255
P1 "UIOLABP01"	Te ½	192.168.1.9	255.255.255.252
	Gi 2/1	192.168.1.2	255.255.255.252
	Gi 2/2	192.168.1.13	255.255.255.252
	loop 100	172.30.10.30	255.255.255.255
P1 "UIOLABP02"	Te 0/1/0/0	192.168.1.10	255.255.255.252
	Gi 0/0/1/0	192.168.1.6	255.255.255.252
	Gi 0/0/1/1	192.168.1.17	255.255.255.252
	loop 100	172.30.10.40	255.255.255.255

Tabla 3.29- Direccionamiento IP.

La tabla 3.30 indica la asignación de direccionamiento IS-IS para los nodos de la red MPLS.

Numeración NET ISIS Nodos Red MPLS	
Nodo	**NET**
UIOLABPE01	49.1720.3001.0010.00
UIOLABPE02	49.1720.3001.0050.00
UIOLABP01	49.1720.3001.0030.00
UIOLABP02	49.1720.3001.0040.00

Tabla 3.30- Direccionamiento NET.

La primera de las pruebas que se establecerá es la configuración de túneles *Traffic Engineering (TE)* con rutas dinámicas y rutas explícitas entre los routers de

Edge. En la prueba se procederá a la creación de dos túneles de Ingeniería de Tráfico, uno con una ruta explicita y otro con una ruta dinámica, los cuales tienen como router de origen el router PE1 y como destino el router PE2, se dispuso del mismo origen y destino para los túneles TE, con el objetivo de balancear la carga de tráfico enviada desde el router PE1 al router PE2, y no viceversa debido a que los túneles TE solo envían el tráfico de forma unidireccional.

No se crearon túneles TE en el otro sentido entre los PE routers, para verificar el comportamiento del tráfico utilizando los Túneles TE y solo en base al IGP.

Uno de los requerimientos para los túneles es la habilitación de una interfaz de loopback para ser asociada con el túnel TE, en el caso de la prueba se utilizará la loopback compartida (loopback 100), la cual se habilita como parte de la configuración del reenvío MPLS.

A continuación se habilita globalmente *Traffic Engineering* en el router así como también por todas las interfaces que interconectan los equipos MPLS del proveedor de servicios (PE y P), para establecerlas como posibles candidatas para formar parte de una ruta LSP de TE. Además sobre las mismas interfaces se establecerán los parámetros de ancho de banda a ser reservados por RSVP, los cuales se usarán para la determinación y asignación de los recursos para las sesiones de Ingeniería de Tráfico.

Después de habilitado TE en el router e interfaces que puedan ser elegidas para formar parte de un LSP TE, y los parámetros de reserva de ancho de banda con RSVP, se crea dos interfaces túnel en el router de frontera UIOLABE01.

Los túneles de Ingeniería de Tráfico se deben configurar con una dirección IP para poder enviar tráfico sobre él, se recomienda usar “ip unnumbered”[19] y asociarla con la interfaz de loopback compartida para conservar el espacio de direcciones IP, cada una de las interfaces túnel estarán asociadas a la dirección

[19] *IP Unnumbered* es un método que habilita el procesamiento IP en una interfaz Punto-Punto, sin asignar una dirección IP a dicha interfaz y de esta manera conservando el espacio de direcciones IP, y para lo cual se selecciona una interfaz que va prestar su dirección IP configurada a la interfaz en la que se configura el comando, de esta manera se tiene una dirección IP compartida entre dos interfaces, de preferencia se usan las direcciones de loopback ya que estas siempre se encuentran en estado activo.

IP de la loopback 100 del router UIOLABE01 (172.30.10.10); el modo de operación del túnel, para ambos será “mpls TE”.

La dirección de destino del extremo del túnel, en ambos túneles se establece con la IP de la loopback del router PE UIOLABE02 (172.30.10.50), de esta forma se dará soporte TE de extremo a extremo entre los PEs; el proceso mediante el cual se elige la ruta LSP TE túnel, para el caso de la prueba se establecerá para un túnel una ruta explicita que seguirá los saltos (192.168.1.2, 192.168.1.14, 172.30.10.50) y para el otro de una forma dinámica, con el objeto de verificar que forma es más rentable dentro de la red del ISP.

Otro de los parámetros de un túnel TE fue la cantidad de ancho de banda a ser reservado para el túnel TE a lo largo de su camino LSP establecido, el cual en una primera prueba se establecerán anchos de banda diferentes para cada interfaz túnel, para luego establecerlos en un ancho de banda igual para los dos túneles, con el objeto de observar el comportamiento de balanceo de tráfico en estos dos ambientes. Para la habilitación del envío de tráfico sobre los túneles TE se utilizará ISIS para que los túneles entren en los cálculos de SPF.

Como paso final de la habilitación los túneles TE, es la que IGP tenga el soporte para Ingeniería de Tráfico; en el caso del IGP en uso para la prueba IS-IS, la configuración solo se refiere a unos comandos de extensión para la configuración ya establecida previamente en el funcionamiento de MPLS.

La siguiente prueba que se configura es el establecimiento de túneles *Traffic Engineering (TE)* de *backup* para la protección de enlaces.

En la prueba se procede a la creación de un túnel TE de *backup*, para proteger el enlace entre el router P2 y PE2, reenrutando el tráfico que transporten los túneles principales, que utilicen dicho enlace como parte de su LSP hacia el túnel de backup. Siendo necesaria la habilitación del mecanismo de restauración FRR sobre la interfaz túnel a ser protegida, para la prueba se plantea proteger el tráfico del túnel principal de ruta explicita.

El Túnel de backup será construido de una forma explícita, ya que de esta forma se controla el camino que tomará el tráfico reenrutado, y se maneja los flujos de información de una mejor manera.

3.2.5.3 Configuraciones de MPLS *TRAFFIC ENGINEERING* TE

A continuación se exponen los comandos de configuración, para establecer tanto un túnel TE con ruta explícita como con ruta dinámica.

Configuración global del Soporte de Ingeniería de Tráfico en el router:

```
Router(config)#mpls traffic-eng tunnels
```

Configuración del Soporte de Ingeniería de Tráfico en la interfaz

```
Router# configure terminal
Router(config)#interface {tipo} {número}
Router(config-if)#ip address {dirección-ip} {Máscara}
Router(config-if)#mpls traffic-eng tunnels
```

Configuración del ancho de banda reservado en la interfaz y el máximo ancho de banda asignado por flujo TE

```
Router# configure terminal
Router(config)#interface {tipo} {número}
Router(config-if)#ip rsvp bandwidth {ancho de banda reservado
  1-1000000 kbps} {Maximo ancho de banda reservado por flujo
  1-1000000 kbps}
```

Comandos de configuración de una interfaz túnel TE:

```
Router# configure terminal
Router(config)#interface Tunnel{number}
Router(config-if)#ip unnumbered loopback {number}
Router(config-if)#tunnel mode mpls traffic-eng
Router(config-if)#tunnel destination {IP address of remote
loopback}
Router(config-if)#tunnel mpls traffic-eng autoroute announce
Router(config-if)#tunnel mpls traffic-eng bandwidth {number Kbps}
Router(config-if)#tunnel mpls  traffic-eng priority {setup
priority-value} {hold-priority value}
Router(config-if)#tunnel mpls traffic-eng path-option {priority}
 [dynamic [bandwidth {override bandwidth  config value} |
 attributes {lsp attribute list name} | lockdown]| explicit
{identifier | name name]]
```

El comando “**interface Tunnel**{number}” crea una interfaz de Tunnel e ingresa en su modo de configuración en donde se configuran las características del túnel. El comando de configuración es “**ip unnumbered loopback** {number}” asigna la dirección de origen del túnel TE.

El siguiente comando “**tunnel mode mpls traffic-eng**” habilita el túnel para manejar MPLS TE, el comando “**tunnel destination** {IP address of remote loopback}” configura el destino del túnel TE, y este es el ID MPLS del router extremo del túnel.

El comando “**tunnel mpls traffic-eng autoroute announce**”, permite al IGP tomar en cuenta al túnel en los cálculos SPF (Shortest Path First), y con lo cual se habilita el envío de tráfico sobre el túnel.

El comando “**tunnel mpls traffic-eng bandwidth** {*number kbps*}”, es un comando opcional y especifica la cantidad de ancho de banda a ser reservado para el túnel TE a lo largo de su camino LSP establecido.

El comando “**tunnel mpls traffic-eng priority** {*setup priority-value*} {*hold-priority value*}” permite configurar la prioridad del túnel TE, el campo “setup priority-value” es la prioridad que se utilizará cuando se señaliza un LSP para un túnel TE y determina que túneles ya existentes pueden ser sustituidos, el campo “*hold-priority value*” es un valor opcional que se asocia al LSP de un túnel, para determinar si el LSP podría ser precedido por otro LSP señalizado con menor prioridad.

Los valores permitidos para ambos campos de prioridad son de 0-7, donde un valor de 0 representa la más alta prioridad y 7 la menor prioridad, un LSP con prioridad menor a otro LSP puede apropiarse de dicho LSP.

Por defecto el campo “*setup priority-value*” tiene un valor de 7 y el campo “*hold-priority value*” el mismo valor de “*setup priority-value*”.

El siguiente comando permite la configuración del camino LSP que tomará el túnel TE; este comando tiene dos variantes la primera es en la que el camino LSP se

establece dinámicamente en base al IGP y CSPF[20], la ruta elegida será dinámica y cuyo comando de configuración es **"tunnel mpls traffic-eng path-option** número **dynamic**", la otra opción es donde el camino LSP se construye de una manera explícita, en el router de cabecera del túnel MPLS TE, el comando de configuración es "**tunnel mpls traffic-eng path-option** número **explicit name** LSP_explicito", donde el campo "LSP_explicito" representa el nombre del LSP a configurar de forma explícita, y cuya configuración se muestra a continuación:

```
Router(config)#ip explicit-path name LSP_explicito enable
Router(cfg-ip-expl-path)#next-address direcciónIP
Router(cfg-ip-expl-path)#next-address direcciónIP
```

El comando "**ip explicit-path name** LSP_explicito **enable**" habilita el modo de configuración de una ruta explicita, donde "LSP_explicito" es el nombre que se le da al LSP en configuración, el siguiente comando "**next-address** direcciónIP" establece las direcciones IP de forma *hop-by-hop* a través del backbone.

Comandos adicionales que habilitan la extensión de soporte TE sobre ISIS son:

```
Router(config)#router isis id_proceso
Router(config-router)#mpls traff       ic-eng level [1|2]
Router(config-router)#mpls traffic-eng router-id interfaz número
```

El comando "**mpls traffic-eng level** [1|2]" configuran el dominio de nivel 1 o 2 de ISIS para Ingeniería de Tráfico, y el comando "**mpls traffic-eng router-id** interfaz número" establece el identificador del router necesario para los procesos de Ingeniería de Tráfico.

El comando "**tunnel mpls traffic-eng fast-reroute**" se debe configurar en la interfaz túnel que se requiere proteger.

Para un nodo en el que se protegerá un túnel, se necesita la configuración del comando "**mpls traffic-eng backup-path** túnel_backup" dentro de la interfaz que

[20] *CSPF (Constrained Shortest Path First First)* es un algoritmo de "ruta-más-corta" modificado el cual toma en cuenta las posibles restricciones en el cálculo de un LSP a través del dominio MPLS. CSPF considera los siguientes factores: Información topológica generada por OSPF o IS-IS, atributos asociados con el estado de la red, ancho de banda total, ancho de banda reservado y disponible en cada enlace, información facilitada por las extensiones TE, detalles administrativos introducidos por el usuario, donde se detallan el número máximo de saltos, requerimientos de ancho de banda para ciertos LSP, entre otros.

se considera proteger y forma parte del túnel TE. A continuación se presenta un ejemplo de configuración de túneles TE:

```
mpls traffic-eng tunnels
!
!
interface Tunnel1
 ip unnumbered Loopback100
 tunnel destination 172.30.10.50
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 5 5
 tunnel mpls traffic-eng bandwidth  1000
 tunnel mpls traffic-eng path-option 1 explicit name LSP1
 tunnel mpls traffic-eng fast-reroute
!
!
interface Tunnel3
 ip unnumbered Loopback100
 tunnel destination 172.30.10.50
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng bandwidth  512
 tunnel mpls traffic-eng path-option 1 dynamic
!
!
interface Loopback100
 ip address 172.30.10.10 255.255.255.255
!
!
interface GigabitEthernet1/25
 ip address 192.168.1.1 255.255.255.252
 ip router isis
 speed nonegotiate
 mpls traffic-eng tunnels
 mpls label protocol ldp
 mpls ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 5000 5000
!
!
router isis
 net 49.1720.3001.0010.00
 is-type level-2-only
 metric-style wide
 passive-interface Loopback100
 mpls traffic-eng router-id Loopback100
 mpls traffic-eng level-2
!
!
ip explicit-path name LSP1 enable
```

```
 next-address 192.168.1.2
 next-address 192.168.1.14
 next-address 172.30.10.50
!
```

3.2.6 DISEÑO DE LA PRUEBA DE MULTICAST SOBRE EL BACKBONE MPLS. [12] [40]

Durante el tiempo se ha observado el interés y la necesidad de implementar tecnologías nuevas o servicios nuevos a ofrecer a los clientes de un ISP, siendo uno de estos el permitir dar el soporte para la implementación del servicio de traspaso de información multicast. Por tales razones, CNT EP empezó a observar la importancia que tiene el buen uso de esta tecnología, para poder ofertar a sus clientes el producto de televisión utilizando la tecnología de IP/TV (multicasting).

3.2.6.1 Objetivos

Se planea implementar la simulación de un backbone MPLS básico de un Proveedor de Servicios, sobre el cual, se permita dar el soporte para la implementación del servicio de traspaso de información multicast para los clientes, siendo un ejemplo de esto la distribución de streaming de video hacia varios usuarios, y su aplicación o producto a ofrecer a los clientes podría ser “IP-TV”.

Con esta prueba se planea mostrar un ejemplo del comportamiento de multicast sobre un backbone MPLS, adicionalmente se planteará la integración del router Cisco 7609-S como un router PE a la red MPLS operativa de CNT EP, para mostrar unas pruebas del IP-TV que se encuentra en desarrollo.

3.2.6.1.1 *Consideraciones del escenario de pruebas*

Las condiciones que debe cumplir la topología diseñada para permitir la implementación de Multicast en MPLS son:

- Se colocan dos routers PE (Cisco 6500) y dos Ps (Cisco CRS-1 y Cisco 12000) que conforman la red del proveedor de servicios.
- Se utilizan dos PCs para simular un servidor y un cliente de streaming.

- Habilitar el reenvío MPLS sobre las interfaces que interconectan PE routers con P routers y entre P routers.
- Se utiliza como protocolo de enrutamiento interno (IGP) IS-IS para la distribución de rutas.
- Se utiliza LDP como el protocolo de distribución de etiquetas.

La prueba se encuentra basada en la topología de prueba, en la configuración inicial de la habilitación del *backbone* MPLS, manejando como protocolo de enrutamiento IS-IS y para la distribución de etiquetas LDP; para luego implementar la transmisión de información de un streaming de video generado sobre una interfaz del router UIOLABE01, hacia el router UIOLABE02 en el cual se encontrarán los clientes que requieren dicha información, mediante la habilitación de enrutamiento multicast en cada uno de los routers del backbone, tanto para un sistema IOS e IOS XR.

Para la prueba de multicast se ha elegido un árbol de distribución compartido, debido a que este se basa en un punto central de información de fuentes y grupos multicast, denominado Rendezvous Point (RP) en un escenario *PIM Sparse Mode* (PIM-SM), este punto central de información se establecerá de manera manual para todos los grupos multicast de la red.

Se eligió PIM-SM debido a que como se trata de una red de gran utilización en el caso de un Proveedor de servicios, no se requiere que se inunde la red con tráfico innecesario que podría causar congestión y problemas para el resto de servicios que se ofrecen en la red, y PIM-SM permite el tráfico únicamente a los segmentos de red que se interesa en recibir el tráfico y han realizado un pedido explícito de los datos.

El primer paso es la habilitación global de multicast, tanto en los router P y PE, debido a que la prueba se basa en PIM-SM "*Protocol Independent Multicast Sparse Mode*", se requiere también la configuración manual del RP "*Rendezvous Point*", el cual manejará y controlará la información de los grupos y fuentes *multicast*. La topología en uso se muestra en la figura 3.18.

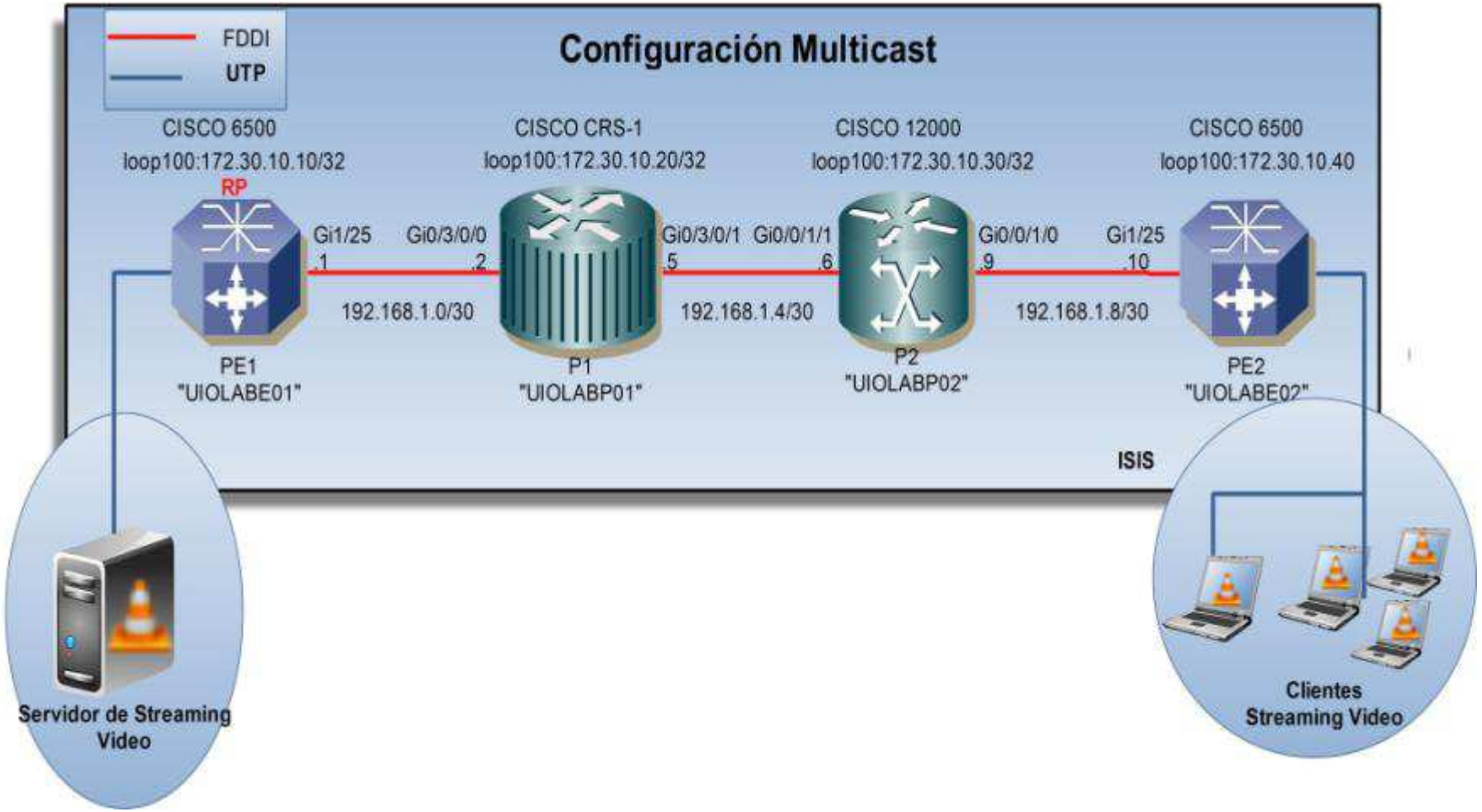


Figura 3.18: Topología de prueba Multicast sobre backbone MPLS

Se eligió configurar el "*Rendezvous Point*" asociado a loopback 100 del router UIOLABE01 debido a que este se encuentra lo más cercano para manejar los flujos de las fuentes de *streaming*.

El siguiente paso es la habilitación de PIM en las interfaces del backbone para el soporte de *Multicast*, para poder formar parte de un segmento del árbol de distribución, incluyendo su habilitación sobre la fuente de actualizaciones de BGP, en el caso de las pruebas que hemos venido manejando la interfaz de loopback compartida, configurada como la loopback100.

Como una prueba adicional se procedió a la integración del router Cisco 7609 a la red del backbone MPLS de CNT EP, habilitando ISIS, LDP y los parámetros de *multicast* para mostrar una idea del servicio de IP-TV que se encuentra en desarrollo en CNT. Estos parámetros de configuración no se mostrarán debido a su grado de confidencialidad.

3.2.6.2 Configuraciones de *Multicast* [12] [40] [41]

El comando que permite configurar *multicast* de forma global es:

```
Cisco# configure terminal
Cisco(config)# ip multicast-routing
```

La configuración del RP se muestra a continuación:

```
Cisco# configure terminal
Cisco(config)# ip pim rp-address <direcciónIP del RP>
```

La dirección IP del RP es el ID MPLS del router elegido para ser el punto de distribución del árbol.

La configuración de PIM *Sparse Mode* en las interfaces es la siguiente:

```
Cisco# configure terminal
Cisco(config)# interface <nombre_interfaz>
Cisco(config-if)# ip pim sparse-mode
```

Donde el comando "**ip pim sparse-mode**" habilita PIM en modo *sparse* en una interfaz del core MPLS que maneja tráfico de multicast.

A continuación se muestra la configuración para un sistema IOS XR:

De igual manera es necesario la habilitación del enrutamiento multicast para lo cual los comandos de configuración son los siguientes:

```
RP/0/RP0/CPU0:Cisco#configure
RP/0/RP0/CPU0:Cisco(config)#multicast-routing
RP/0/RP0/CPU0:Cisco(config-mcast)#address-family ipv4
RP/0/RP0/CPU0:Cisco(config-mcast-default-ipv4-if)#interface
Loopback100
RP/0/RP0/CPU0:Cisco(config-mcast-default-ipv4-if)#enable
RP/0/RP0/CPU0:Cisco(config-mcast-default-ipv4-if)#interface
TenGigE0/0/0/0
RP/0/RP0/CPU0:Cisco(config-mcast-default-ipv4-if)#enable
```

Donde la diferencia es que el comando "**multicast-routing**" ya no habilita la funcionalidad *multicast* globalmente sino de una manera modular, y solo en aquellas interfaces que se encuentren configuradas en dicho módulo. En este módulo también se pueden agrupar por familias de direcciones ya que se puede tener *multicast* IPv4 o IPv6 o dentro de una instancia VRF, para lo cual se usa el comando "**address-family ipv4**" el cual especifica que se manejará *multicast* dentro de un ambiente de direcciones IPv4, luego se agregan las interfaces que manejarán el enrutamiento *multicast* con el comando "**interface** `<nombre_interfaz>`", para luego con el comando "**enable**" habilitar a la interfaz para el transporte de *multicast*.

El otro protocolo a configurar para el funcionamiento de *multicast* es PIM en su modo *Sparse* y de igual manera este se lo configura de manera modular y cuyos comandos de configuración son:

```
RP/0/RP0/CPU0:Cisco#configure
RP/0/RP0/CPU0:Cisco(config)#router pim vrf default address-family
ipv4
RP/0/RP0/CPU0:Cisco(config-pim-default-ipv4)#rp-address
<direcciónIP del RP>
RP/0/RP0/CPU0:Cisco(config-pim-default-ipv4)#interface Loopback100
RP/0/RP0/CPU0:Cisco(config-pim-default-ipv4-if)#enable
RP/0/RP0/CPU0:Cisco(config-pim-default-ipv4-if)#)#interface
TenGigE0/0/0/0
RP/0/RP0/CPU0:Cisco(config-pim-default-ipv4-if)#)#enable
```

En el sistema IOS XR el modo de PIM soportado es el "*Sparse Mode*" y no así el modo "*Sparse Dense Mode*", por lo que en su configuración no se especifica el tipo de modo de operación de PIM ya que al habilitar PIM por defecto este trabaja en el modo "*Sparse Mode*", el comando de configuración "**router pim vrf default address-family ipv4**" habilita el protocolo PIM, la palabra clave "vrf default" especifica que trabaje sobre la tabla de enrutamiento general o global, y la palabra clave "address-family" especifica dentro de que grupo de direcciones trabajará PIM ya que en este sistema puede trabajar tanto para direcciones IPv4 como para direcciones IPv6.

Una vez dentro del modo de configuración de PIM el comando "**rp-address** <direcciónIP del RP>" configura la dirección del router elegido como el punto de distribución del árbol, cuya dirección IP es la configurada en la loopback compartida que es ID MPLS del router, luego de igual manera que con *multicast routing* se agregan las interfaces que manejarán el protocolo PIM con el comando "**interface** `<nombre_interfaz>`", luego con el comando "**enable**" habilitar a la interfaz para el funcionamiento de PIM.

A continuación se presenta un ejemplo de la habilitación de multicast sobre un router PE con sistema IOS:

```
ip multicast-routing
ip multicast multipath
!
interface Loopback100
 ip address 172.30.10.10 255.255.255.255
 ip pim sparse-mode
!
interface GigabitEthernet1/1
 ip address 192.168.100.2 255.255.255.252
 ip pim sparse-mode
!
ip pim rp-address 172.30.10.10
```

A continuación se presenta un ejemplo de la habilitación de multicast sobre un router P con sistema IOS XR:

```
multicast-routing
 address-family ipv4
  interface Loopback100
   enable
```

```
  !
  interface GigabitEthernet0/0/1/0
   enable
  !
  interface GigabitEthernet0/0/1/1
   enable
  !
  nsf
  multipath
  interface all enable
 !
!
router igmp
 version 2
!
router pim
 address-family ipv4
  rp-address 172.30.10.10
  log neighbor changes
  interface Loopback100
   enable
  !
  interface GigabitEthernet0/0/1/0
   enable
  !
  interface GigabitEthernet0/0/1/1
   enable
```

3.2.7 DISEÑO DE PRUEBAS DE *SERVICE INSTANCE* [20] [33]

Este escenario se diseñó para probar una configuración utilizada en la red MPLS de la CNT E.P. que presentaba problemas. Con las pruebas se pretende determinar que parte de la red está generando las dificultades y realizar las medidas correctivas necesarias.

El escenario del problema es el siguiente: en la ciudad de Loja se tiene un punto de presencia de la empresa, donde se dispone de un equipo 7600 que se encarga de concentrar el tráfico proveniente de switches y DSLAMs que permiten el acceso a red; estos elementos están ubicados en diferentes localidades de la provincia.

Uno de estos switches de acceso tiene conectado dos DSLAMs que se utilizan para brindar servicios de internet residencial con conexiones PPPoE[21]. El tráfico

[21] Point-to-Point protocolo over Ethernet es un protocolo que permite encapsular paquetes PPP en una trama Ethernet. Utilizado para establecer una conexión a internet a travez de un servidor.

de cada DSLAM se asigna a una VLAN específica, por lo que en el enlace que conecta al switch con el router 7600 se tendrán dos VLANs una para identificar a cada DSLAM.

En el router 7600 se tiene una única VLAN por la que se envía el tráfico PPPoE hacia los servidores BRAS[22] ubicados en Guayaquil, para realizar esto se decidió utilizar service instances. Estas permiten agregar el tráfico de las dos VLANs y enviarlo por una sola, esta función es realizada por la tarjeta 7600-ES+20G3CXL misma que tiene varias características que permiten realizar agregación de flujos, diseñada para los nodos de edge de los proveedores de servicio.

En este escenario surgió el problema que algunos de los usuarios de estos DLAMs no lograban establecer la sesión PPPoE y por ende no lograban acceder a internet. Como la utilización de las service instance que permiten realizar agregación de servicios es nueva dentro de la red MPLS de la CNT se decidió crear un escenario para probar que no estaban generando ningún problema.

Antes de describir el escenario que simulará lo descrito anteriormente se realizará una descripción rápida de los conceptos y configuraciones relacionadas con las service instance.

3.2.7.1 Objetivo

En este esquema de simulación se pondrá a prueba el funcionamiento de la agregación de servicios en la tarjeta 7600-ES+20G3CXL, la misma que cuenta con un conjunto de características que permiten concentrar el tráfico de varios clientes en los nodos de frontera.

3.2.7.2 Escenario para las pruebas de *service instance*.

Las consideraciones de topología lógica son:

- Se utilizan 2 PCs que simulan la conexión de clientes PPPoE.

[22] *Broadband remote access server,* se encarga de autenticar a los clientes y permitirles el acceso a internet controla el ancho de banda asignado a cada cliente.

- Para emular los DSLAMs se usó dos interfaces de un generador de tráfico IXIA.
- El equipo Cisco 6500 se encarga de ofrecer conectividad a los DSLAMs a través de VLANs.
- Un router 7600 se encarga de simular un nodo PE que realiza la agregación de tráfico y se integrará a la red IP/MPLS de CNT.
- Se establecerá un túnel hacia el BRAS de Guayaquil para acceder a internet.
- En el servidor BRAS CNT creó dos usuarios PPPoE que permiten realizar las pruebas de acceso a internet.

En la figura 3.19 se muestra la topología creada para probar las *service instance.*

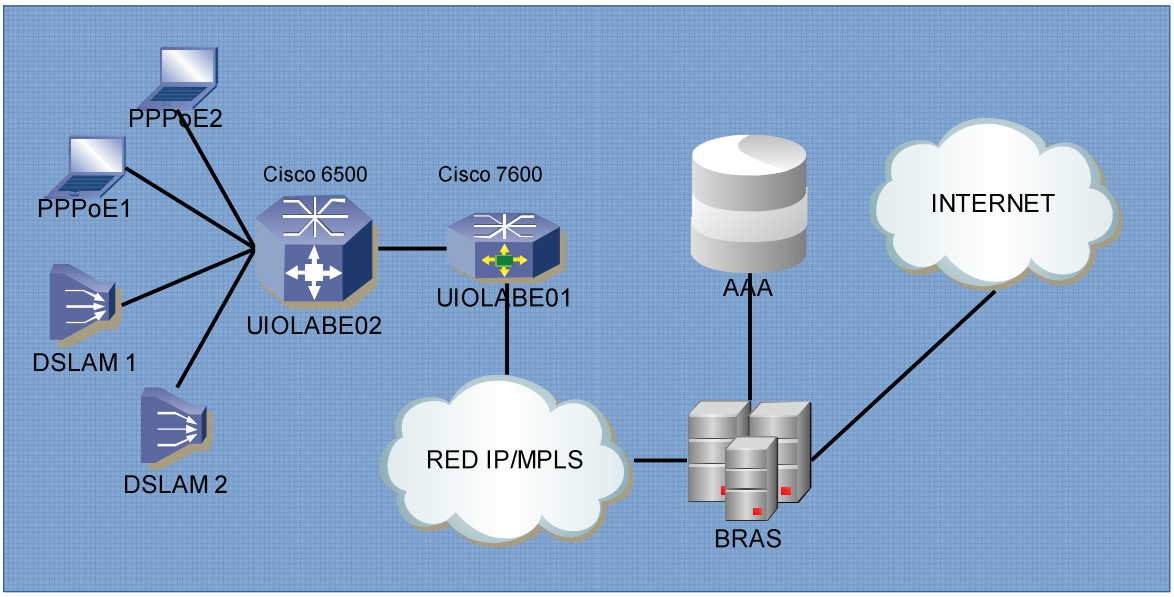


Figura 3.19: Topología para probar *service instance*.

En este caso se ha simulado la conexión de dos DSLAMs a un switch (Me6500,) para esto se utilizó un generador de tráfico IXIA 400T en el que se simuló un *MAC flooding*[23] con 400 Mbps de utilización del enlace de 1 Gbps, con 1500 direcciones por cada dispositivo, simulando la conexión de 3000 usuarios simultáneos al LER, adicionalmente se tienen dos PC para establecer una conexión PPPoE con el BRAS y navegar en internet con la finalidad de observar si la inundación de

[23] Es la inundación de direcciones MACs por una sola interfaz.

direcciones no produce una denegación de servicio, pues se sospecha que las *service instance* no manejan de manera adecuado un número grande de MACs.

Se utilizaron dos VLANs en el 6500 y en cada una se colocó un DSLAM y un PC, en el puerto del equipo de 7600 se crearon dos *service instance* uno por cada VLAN, de esta manera se agregan dos flujos ubicados en VLANs diferentes en una sola.

En el equipo 7600 se utiliza una VLAN global, que tiene significado en todo el equipo, se creara una interfaz VLAN en la se configura un túnel de capa 2 MPLS hacia un equipo border de Guayaquil el cual se encuentra conectado a los servidores BRAS y AAA[24], los que en última instancia permitirán el acceso a internet a través de una conexión PPPoE mediante un usuario y una contraseña.

Previo a realizar las pruebas fue necesaria la integración del equipo de laboratorio 7609 a red nacional MPLS de la CNT EP para esto se lo integró con el equipo PE de Mariscal. Los pasos se describen a continuación.

- Se configuró un protocolo IGP para el aprendizaje de las rutas alcanzables dentro de la red, el protocolo configurado y utilizado por CNT EP es IS-IS, se estableció una adyacencia de nivel 2 entre los dos nodos, con esto se logra un total conocimiento para alcanzar los diferentes nodos y redes conectadas.
- Se configuró un protocolo de distribución de etiquetas entre los dos nodos; el protocolo que se configuró es LDP, el cual permite aprender la información de la asociación de una etiqueta con una red en FRAME-MODE llenando las tablas LFIB necesarias para el envío de los paquetes en MPLS
- Se procedió a habilitar la conmutación y encapsulación MPLS en las interfaces que participan en la transmisión y recepción de los paquetes.

[24] Servidor de Acceso, Autenticación, Autorización a los recursos de la red.

- Finalmente se configuró un protocolo EGP para alcanzar las rutas externas al sistema autónomo, se configuró BGPv4 y se establecieron sesiones entre el equipo y los tres route reflector[25] disponibles en la red.

El direccionamiento IP necesario para la configuración de las interfaces que se conectan a la red MPLS de la CNT no se especifica pues se utiliza direcciones que son parte del direccionamiento interno de CNT y que no se pueden dar a conocer, de la misma manera las claves utilizadas por los protocolos para realizar autenticación se cambiaron con la finalidad de proteger a la red, en la parte armada en el laboratorio no se necesitan direcciones IP pues se realizarán agregación de servicios de capa 2.

3.2.7.3 *Flexible QinQ Mapping and Service Awareness* [21] [34]

QinQ Mapping y *Service Awareness* permite a los proveedores de servicio ofertar servicios *triple-play*, acceso residencial de Internet desde un DSLAM, switches de agregación de clientes y VPNs de capa 2 y capa 3 corporativas proporcionando un punto de terminación de tramas dot1q, doble etiquetamiento (estándar 802.1ad[26]) dentro de una subinterfaz de capa 3 en el nodo de acceso.

El nodo de acceso se conecta con el DSLAM a través de las tarjetas Cisco serie 7600 ES + line. Esto proporciona una manera flexible para identificar instancias de los clientes basados en las etiquetas VLAN, y mapear estas instancias con servicios en la red. *QinQ Mapping y Service Awareness* en las tarjetas Cisco serie 7600 ES + line es soportado a través de *Ethernet Virtual Connection Services (EVCS) "service instances"*.

EVCS usa el concepto de EVC (circuitos Ethernet virtual) y las instancias de servicio. El EVC es una representación de una instancia extremo a extremo de nivel 2 de un servicio ofrecido por un proveedor a un cliente, engloba los

[25] Es un equipo con el que todos los routers de la red establecen las sesiones iBGP, y se encarga de distribuir las rutas que esta aprende, ofreciendo una alternativa altamente escalable que elimina la necesidad de full mesh de BGP manteniendo la red libre de bucles.
[26] Conocido como QinQ permite la encapsulación de múltiples VLANs en una trama formando una pila y aumentando el número de VLANs disponibles.

diferentes parámetros del servicio que está siendo ofertado. Una *service instance* es la creación de un EVC en un puerto dado de un router.

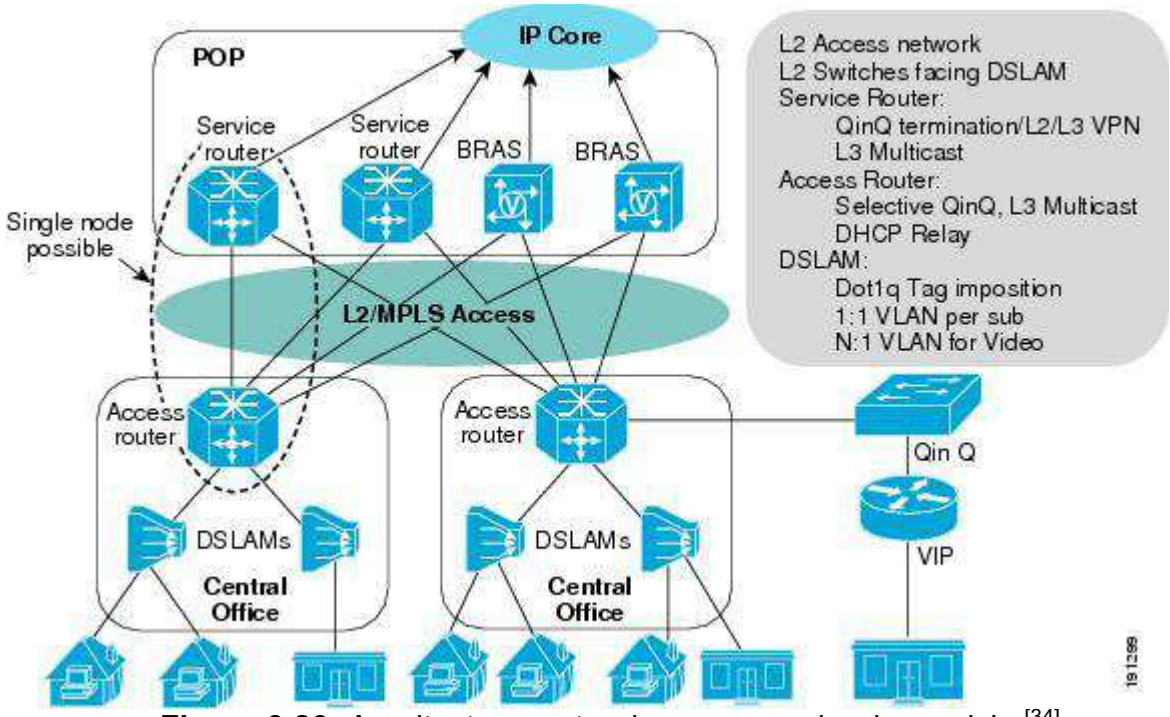


Figura 3.20: Arquitectura metro de un proveedor de servicio.[34]

La figura 3.20 muestra una típica arquitectura metro donde se usa la traslación de VLANs en los puertos por los que acceden los DSLAM de esta manera se puede ofrecer diferentes servicios de capa 2 o capa 3 a los clientes que se conectan a los DLAMs.

QinQ Mapping and Service Awareness on Cisco 7600 Series ES+ line cards provee las siguientes funcionalidades:

Conexiones VLANs con significado local:

- Etiqueta simple Ethernet con conmutación local donde la etiqueta de tráfico dot1q recibida de un puerto se interconecta con otro puerto, cambiando la etiqueta. Se trata de un servicio de mapas 1-a-1 y no hay aprendizaje MAC involucrado.
- Etiquetamiento doble Ethernet con conmutación local, en la que el tráfico doblemente etiquetado es recibido en un puerto que esta interconectado

con otro puerto, cambiando ambas etiquetas. No hay aprendizaje MAC involucrado.

- *Hairpinning*: Se trata de una conexión cruzada entre dos EFC[27] en el mismo puerto.

QinQ Selectivo (traducción 1 a 2):

- Conexión cruzada QinQ selectiva añade una etiqueta al tráfico dot1 que recibió y luego lo envía por túneles al extremo remoto con conmutación de nivel 2 o EoMPLS.

Traducción de Doble etiquetamiento (traducción 2 a 2) conmutación de Capa 2. Dos etiquetas recibidas en las tramas se extraen "*pop*" y dos nuevas etiquetas son colocadas "*push*":

- Conexión cruzada QinQ selectiva añade una etiqueta al tráfico dot1 que recibió y luego lo envía por túneles al extremo remoto con conmutación de nivel 2 o EoMPLS.
- Conmutación de capa 2 QinQ selectiva añade una etiqueta al tráfico dot1 que recibió y realiza conmutación de capa 2 en una SVI[28] basada en la etiqueta externa para configurar servicios adicionales.

Traducción de Doble etiquetamiento (traducción 2 a 1)

- *Ethernet MultiPoint Bridging over* Ethernet (MPBE)[29]: La etiqueta doble entrante es mapeada a una única etiqueta dot1q que se utiliza para hacer MPBE.
- Enrutamiento de doble etiquetamiento: Igual que el enrutamiento tradicional de etiquetas dot1q, excepto que el etiquetamiento doble identifica a la VLAN ocultas.

---

[27] Ethernet Flow Point es una interfaz lógica que conecta un *bridge domain* con una interfaz física, un *bridge domain* es un dominio de broadcast local que utiliza una VLAN con significado global en el router y realizar la agregación de diferentes flujos a un solo dominio.

[28] Switch virtual interface es una interfaz virtual relacionada con una VLAN que permite ofrecer procesamiento de capa 3.

[29] Es una arquitectura que permite agregar varios flujos de tráfico ubicados en diferentes interfaces físicas y lógicas en un solo dominio de broadcast dentro de un *bridge-domain.*

VLAN de significado Local: Las etiquetas VLAN tienen significado únicamente en el puerto.

Para las tarjetas 7600 ES se tienen las siguientes limitantes máximo 8000 *service instance* por puerto y un máximo de 16000 por las tarjetas, la forma de configurar las service instance se realiza de la siguiente manera:

3.2.7.3.1 *Pasos de configuración:*

```
Router# enable
Router# configure terminal
Router(config)# interface gigabitethernet slot/port
Router(config-if)#no ip address
Router(config-if)# service instance id ethernet [service-name]
Router(config-if-srv)# encapsulation dot1q vlan-id
Router(config-if-srv)# rewrite ingress tag {push {dot1q vlan-id |
dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id}
| pop {1 | 2} | translate {1-to-1 {dot1q vlan-id | dot1ad vlan-
id}| 2-to-1 dot1q vlan-id | dot1ad vlan-id}| 1-to-2 {dot1q vlan-id
second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-id} | 2-to-2
{dot1q vlan-id second-dot1q vlan-id | dot1ad vlan-id dot1q vlan-
id}} symmetric
Router(config-if-srv)# [no] bridge-domain bridge-id
```

3.2.7.3.2 *Detalle de pasos de configuración:*

La descripción de los pasos de la tabla 3.31 son: para "*encapsulation dot1q 13*" se disponen de varias opciones para definir los criterios de coincidencia con las VLANs, se puede especificar una, como en el ejemplo la VLAN 13; un rango; una lista; o cualquiera con la palabra "*any"*. Si se usa un criterio que coincide con dos etiquetas la primera debe ser única y la segunda puede ser un rango una lista o cualquiera. Se dispone también de "*default tag"* que coincide con todas las tramas estén o no etiquetadas y el criterio "*untagged"* que coincide con todos los paquetes no etiquetados.

De la misma manera para el paso "*rewrite ingress tag pop 1 symmetric"* se dispone de varias opciones para realizar el remarcado de las etiquetas, las tres operaciones que realiza son *"pop"* que remueve una etiqueta existente, "*push"* que coloca una nueva etiqueta y "*traslate"* que cambia el valor de la etiqueta, se tienen restricciones: no se puede tener más de un remarcado por service instance, las operaciones *push*, *pop* y *traslate* se puede usar únicamente cuando

se coincide con una única etiqueta no soporta listas ni rangos. A continuación en la tabla 3.31 un resumen de los pasos para configurar una *service instance*.

Comandos	Propósito
Router# enable	Activa el modo EXEC privilegiado. Si se le solicita, introduzca su contraseña.
Router# configure terminal	Entra en el modo de configuración global.
Router(config)# interface gigabitethernet 4/1	Especifica la interfaz a configurar.
Router(config-if)# no ip address	Remueve una dirección IP o el procesamiento IP.
Router(config-if)# service instance 101 ethernet	Crea un service instance (una instancia de un EVC) en una interfaz y establece el dispositivo en el submodo de configuración config-if-srv.
Router(config-if-srv)# encapsulation dot1q 13	Define los criterios de coincidencia para seleccionar que tramas del flujo que ingresa a la interfaz son parte de la *service instance*.
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric	Especifica la manipulación de la etiqueta que se realizará en las tramas que ingresan y salen en el service *instance.*la palabra *symmetric* indica que la encapsulación se realizará tanto en las tramas que ingresan como en las que salen
Router(config-if-srv)# bridge-domain 12	Vincula la instancia de servicio a una instancia de dominio bridge donde el bridge-id es el identificador de la instancia de dominio bridge y corresponde a una VLAN global.

Tabla 3.31- Pasos para configurar *service instance.*[34]

El remarcado de las etiquetas se debe de realizar de manera simétrica, esto significa que la reescritura de la etiqueta en la dirección de ingreso debe tener una reescritura reversa en la dirección de salida. Por ejemplo con el "*rewrite ingress tag pop 1 symmetric"* se especifica que se debe realizar una operación de "*pop*" en la primera etiqueta del paquete que ingresa, en cambio al colocar "*symmetric*" se realiza una operación de "*push"* para volver a colocar la etiqueta VLAN en el paquete que sale de la interfaz.

Este ejemplo muestra cómo configurar una instancia de servicio con la etiqueta única (Dot1q) en la encapsulación.

```
Router# enable
Router# configure terminal
Router(config)# interface GigabitEthernet7/1
Router(config-if)# no ip address
Router(config-if)# service instance 71 ethernet
Router(config-if-srv)# encapsulation dot1q 71
Router(config-if-srv)# rewrite ingress tag pop 1 symmetric
Router(config-if-srv)# bridge-domain 10
```

REFERENCIAS BIBLIOGRAFICAS CAPÍTULO 3

LIBROS

[1] **MARTEY**, Abe; **STURGESS**, Scott. "*IS-IS Network Design Solutions*". Cisco Press. Febrero 2002.

[2] **FARAZ**; ZAHEER; **LIU**; MARTEY. **"***Troubleshooting IP Routing Protocols*". Cisco Press. Mayo 2002.

[3] **DOYLE**, Jeff; **DEHAVEN**, Carroll. "*Routing TCP/IP, Volume II*". Cisco Press. Abril 2001.

[4] **HALABI**, Sam; **MCPHERSON**, Danny. "*Internet Rounting Architectures*". Segunda Edición. Cisco Press. Agosto 2000.

[5] **PARKHURST**, William; "*Cisco BGP-4 Command and Configuration Handbook*". Cisco Press. 2001.

[6] **LUO**; PIGNATARO; **BOKOTEY**; CHAN. "*Layer 2 VPN Architectures*". Cisco Press. Marzo 2005.

[7] **ALVAREZ**, Santiago. "*QoS for IP/MPLS Networks*". Cisco Press. Junio 2002.

[8] **SINCHE**, Soraya. "*Sistemas de Cableado Estructurado*". Apuntes de Clase. Semestre Septiembre 2008 – Febrero 2009

[9] **LOBO**, Lancy; **LAKSHMAN**, Umesh. "*MPLS Configuration on Cisco IOS Software*". Cisco Press. Octubre 2005.

[10] **ALWAYN**, Vivek. "*Advanced MPLS Design and Implementation*". Cisco Press. Septiembre 2001.

[11] **GUICHARD**, Jim; **PEPELNJAK**, Ivan. "*MPLS and VPN Architectures*", Cisco Press, Octubre 2000.

[12] **LEWIS**, Mark. "*Troubleshooting Virtual Private Networks*". Cisco Press. Mayo 2004

TESIS

[13] **NIETO**, Luisiana. "*Diseño y configuración de calidad de servicio en la tecnología MPLS para un proveedor de servicios de internet*". EPN. Mayo 2010.

PDF, RFC, PAPERS

[14] **ANÓNIMO**. "*Building Scalable Cisco Internetworks*". Student Guide. Cisco System. Version 3.0. Volume 1. 2006.

[15] ***ANÓNIMO***. "*Cisco IOS IP Routing Protocols Command Reference*". Cisco System. Noviembre 2008.

[16] **ANÓNIMO**. "*Cisco IOS XR Routing Configuration Guide*". Cisco System. 2007.

[17] **ANÓNIMO**. "*Building Scalable Cisco Internetworks*". Student Guide. Cisco System. Version 3.0. Volume 2. 2006.

[18] **ANÓNIMO**. "*Cisco IOS Quality of Service Solutions Configuration Guide*". Cisco System.

[19] **ANÓNIMO**. "*Configuring MPLS QoS". Cisco System*.

[20] **ANÓNIMO**. "*EVC Fundamentals". Cisco System*.

[21] **ANÓNIMO**. "*Configuring Ethernet Virtual Connections (EVCs)*". Cisco System.
URL: http://www.Cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/12.2_52_ey/configuration/guide/swevc.pdf

[22] **ANÓNIMO**. "*Suplemento sobre cableado estructurado*".
URL: http://www.espoch.edu.ec/Descargas/noticias/dacee2_CCNA1_CS_Structured_Cabling_es.pdf

[23] **HASSAN**, Yusuf; **ASATI**, Rajiv. "*Troubleshooting Mpls Networks*". Cisco Systems. 2004.
URL: http://www.Cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/prod_presentation0900aecd80312051.pdf

[24] **ANÓNIMO**. "*Cisco IOS XR Troubleshooting Guide Troubleshooting MPLS Services*". Cisco Systems.
URL: http://www.Cisco.com/en/US/docs/routers/asr9000/software/asr9k_r4.0/ troubleshooting/guide/tr40mpl.pdf

INTERNET

[25] **ANÓNIMO**. "*Implementing IS-IS on Cisco IOS XR Software*"
URL: http://www.Cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.0/routing/configuration/guide/rc3isis.html

[26] **ANÓNIMO**. "*IP Routing Protocol-Independent Commands : redistribute (IP) Through traffic-share min*"

URL: http://www.Cisco.com/en/US/docs/ios/12_2/ iproute/command/ reference/1rfindp2.html

[27] **ANÓNIMO**. ” *IP Routing Protocols Commands: K through M*”
URL: http://www.Cisco.com/en/US/docs/ios/12_3t/ip_route/command/ reference/ip2_k1gt.html

[28] **ANÓNIMO** ”*How to block one or more networks from BGP peer*”
URL: http://www.cisco.com/en/US/tech/tk365/technologies_tech_ note09186a00801310cb.shtml

[29] **ANÓNIMO**. “*Implementing BGP on Cisco IOS XR Software*”.
URL: http://www.Cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/routing/ configuration/guide/rc37bgp.html#wp1197962

[30] **ANÓNIMO** “*Routing Policy Commands on Cisco IOS XR Software*“.
URL: http://www.Cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/routing/ command/reference/rr37plcy.html#wp1135677.

[31] **ANÓNIMO** “*Any Transport over MPLS*”.
URL: http://www.Cisco.com/en/US/docs/ios/12_0s/feature/guide/ fsatom28.html.

[32] **ANÓNIMO** “*MPLS DiffServ Tunneling Modes*”.
URL: http://www.Cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ ftdtmode.html#wp1154997.

[33] **ANÓNIMO** “*Configuring Layer 1 and Layer 2 Features*”.
URL: http://www.Cisco.com/en/US/docs/routers/7600/install_config/ ES40_config_guide/es40_chap4.html#wp1627009

[34] **ANÓNIMO** “*Configuring the Cisco 7600 Series Ethernet Services 20G Line Card*”
URL: http://www.Cisco.com/en/US/docs/routers/7600/install_config/ ES20_config_guide/baldcfg.html#wp1507850

[35] **ANÓNIMO** “Gabinete net-access”
URL: http://www.gruposaytel.com.mx/detalles.php?id=6

[36] **ANÓNIMO** “*Accesorio bajada de cables escalerilla*”
URL: http://www.enavar.com/images/productos/dev100gs.jpg

[37] **ANÓNIMO** “Organizador de cables”
URL: http://images2.cableorganizer.com/panduit/fiber-runner-system/ FRIV45_inside-corner_cables-s.jpg

[38] **ANÓNIMO**. “*How to Troubleshoot the MPLS VPN*”. Cisco Systems.
URL: http://www.Cisco.com/en/US/tech/tk436/tk428/ technologies_tech_note09186a0080093fcd.shtml#routeinfo

[39] **ANÓNIMO**. "*Cisco IOS XR MPLS Configuration Guide, Release 3.7*". Cisco Systems.
URL: http://www.Cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/mpls/configuration/guide/gc37book.html

[40] **MILIVOJEVIC**, Marko. "*Multicast MPLS VPNs*". Blog IPExpert.
URL: http://blog.ipexpert.com/2010/06/07/multicast-mpls-vpns/

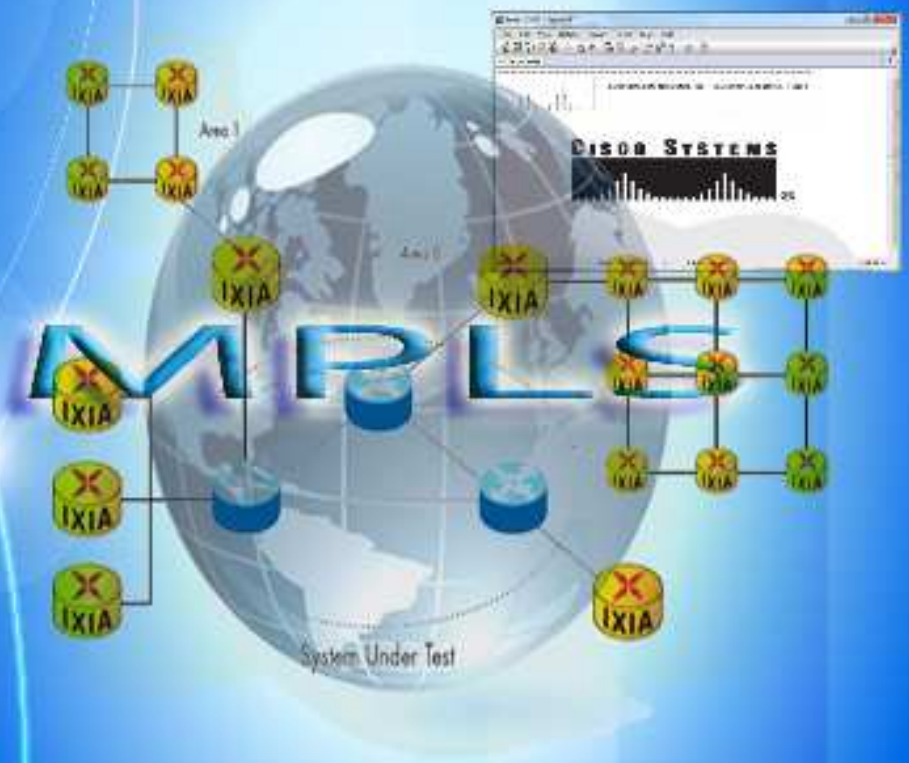
[41] **ANÓNIMO**. "*Multicast Quick-Start Configuration Guide*". Cisco System.
URL: http://www.Cisco.com/en/US/tech/tk828/technologies_tech_note09186a0080094821.shtml

[42] **ANÓNIMO**, "*Cisco IOS Switching Services Command Reference, Release 12.2*". Cisco Systems.
URL: http://www.Cisco.com/en/US/docs/ios/12_2/switch/command/reference/fswtch_r.html

[43] **ANÓNIMO**. "*Multicast-VPN -- IP Multicast Support for MPLS VPNs*". Cisco Systems.
URL: http://www.Cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_mvpn.html#wp1048025

CAPÍTULO 4

PRUEBAS Y RESULTADOS DE LOS ESCENARIOS DISEÑADOS



Este capítulo se enfoca en la presentación de las diferentes configuraciones y los resultados de las pruebas realizadas.

Se desarrolla un plan de pruebas de simulación de troubleshooting de servicios VPN capa 2 y capa 3, así como el establecimiento de las mejores prácticas para lograr optimizar el desempeño en redes de Service Provider.

CAPÍTULO 4

PRUEBAS Y RESULTADOS DE LOS ESCENARIOS DISEÑADOS

4.1 COMPROBACIÓN Y PRUEBAS DE HABILITACIÓN DE MPLS

El procedimiento para comprobar el adecuado funcionamiento de MPLS es: comprobar el funcionamiento de CEF, corroborar que el protocolo de enrutamiento IGP IS-IS esté funcionando de manera adecuada, observar si la habilitación de LDP es la adecuada y comprobar que se esté realizando el envío de paquetes con etiquetas MPLS.

4.1.1 COMPROBACIÓN DE CEF [32] [33]

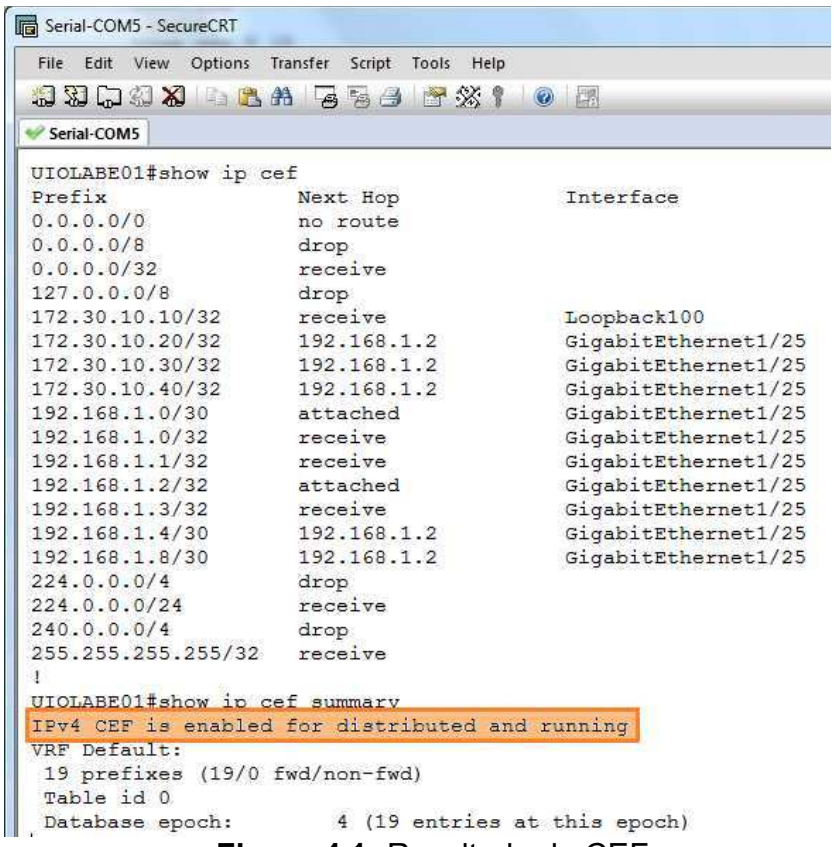


Figura 4.1: Resultado de CEF.

Para verificar si la funcionalidad CEF se encuentra en funcionamiento se utiliza el comando ***show ip cef***, desplegando la información contenida en la tabla FIB (*Forwarding Information Base*).

En la figura 4.1 se observa un ejemplo de la salida obtenida cuando el comando se aplica en el router UIOLABE01, se muestra los prefijos IP aprendidos, el siguiente salto para alcanzar el prefijo IP (red) y la interfaz de salida.

El comando ***show ip cef summary*** permite ver un resumen de las entradas contenidas en la tabla FIB, muestra el número de prefijos IP aprendidos e ingresados en la tabla FIB, además de mostrar si el funcionamiento de CEF se encuentra habilitado, esto se muestra en la sección resaltada en la figura 4.1, con lo que se concluye que la conmutación CEF se encuentra activa.

Otro de los comandos que ayuda en la verificación del funcionamiento de CEF es el comando ***show ip cef detail***, mostrado en la figura 4.2; el cual muestra en detalle cada una de las entradas que se encuentran en la tabla FIB, la sentencia mostrada puede ser utilizada tanto en un sistema IOS como en el IOS XR.

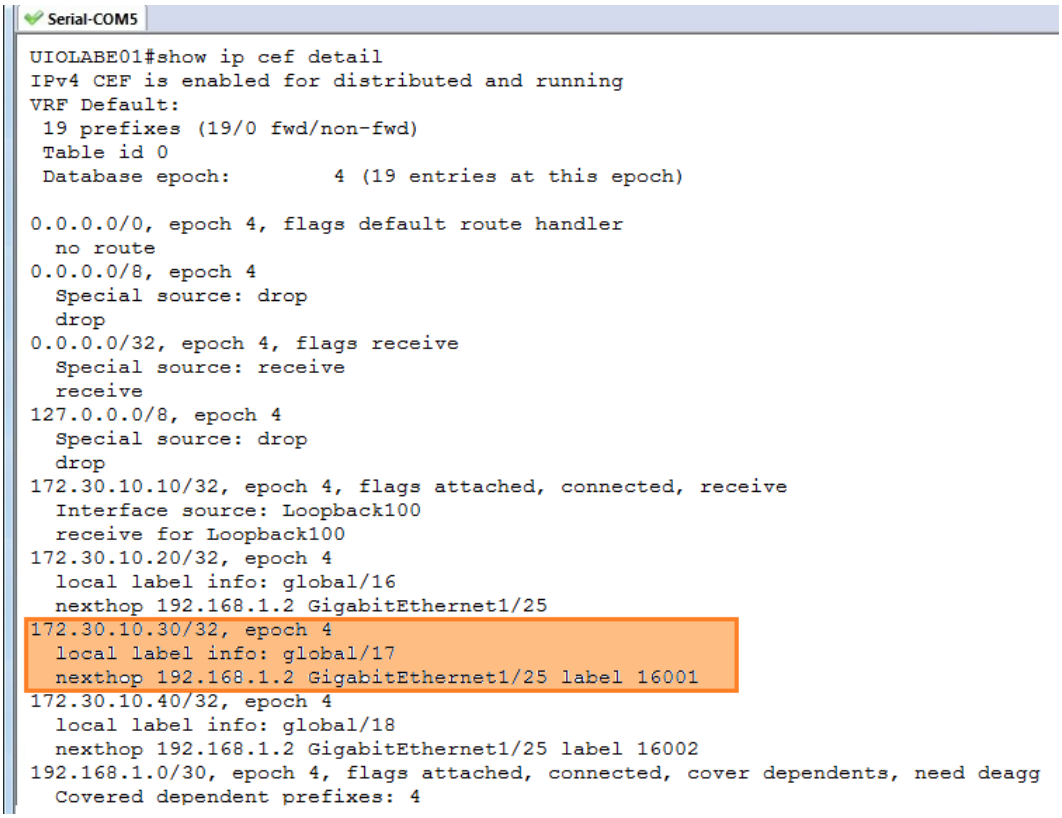


Figura 4.2: Resultado de CEF detallado.

Por ejemplo en la figura 4.2 se muestra el resultado del comando ***show ip cef detail*** cuando se aplica en el router de frontera "UIOLABPE01", donde para cada una de las entradas de la tabla FIB, se muestra en detalle la información del siguiente salto para alcanzar la red, la interfaz de reenvío, y la información de etiquetamiento que se le asignan a los paquetes dirigidos hacia dicho prefijo de red. En donde la etiqueta local identificará los paquetes entrantes al router que son dirigidos hacia una red remota, usando el router como un salto intermedio, mientras que la etiqueta de salida reemplaza a la etiqueta local permitiendo el reenvió de los paquetes hacia el siguiente salto.

En el caso del prefijo de red "172.30.10.30/32" resaltado en la figura 4.2, se tiene como etiqueta local el valor de 17, y todo router que quiera enviar paquetes hacia dicho prefijo de red por medio del router UIOLABPE01 debe etiquetarlos con la etiqueta 17, para que el router UIOLABPE01 los distinga a su ingreso y los reenvíe intercambiando la etiqueta local por la etiqueta de salida 16001, a través de la interfaz Gi1/25 para alcanzar el próximo salto (192.168.1.2).

4.1.2 COMPROBACIÓN DEL FUNCIONAMIENTO DE ISIS. [1] [2] [9] [10] [11] [17]

Para comprobar el adecuado funcionamiento de IS-IS, el primer paso es verificar si el protocolo se encuentra activo, para esto se dispone de la sentencia ***show ip protocols*** que mostrará los protocolos de enrutamiento IP activos, se utiliza tanto para el IOS como para el IOS XR. En la figura 4.3 se observa el resultado obtenido al aplicarlo en el router UIOLABE02 que utiliza un sistema IOS.

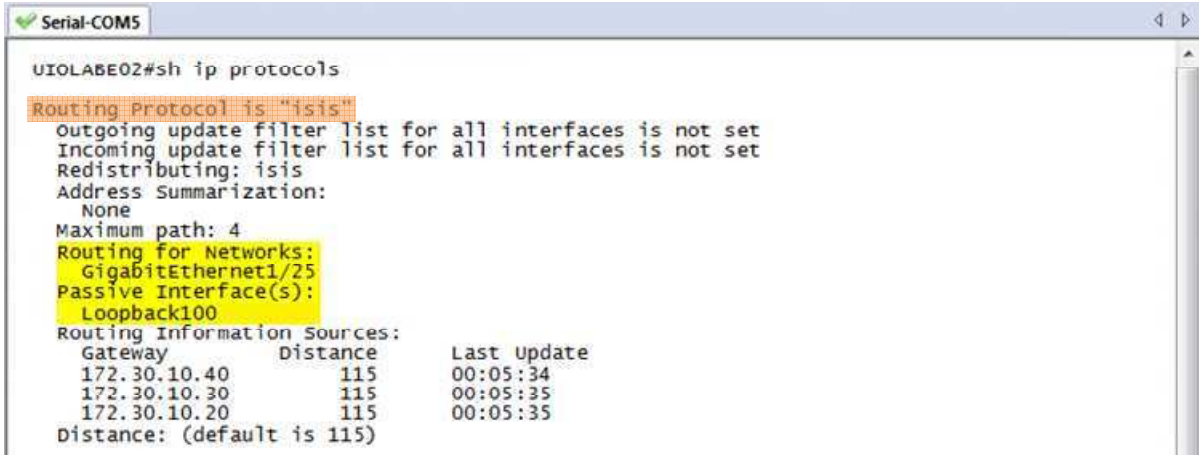


Figura 4.3: Protocolos activos en UIOLABE02 IOS.

En la figura 4.3 se observa que el protocolo de enrutamiento habilitado es IS-IS, que no se tienen filtros de rutas en las interfaces, el "*redistributing"* especifica que no redistribuye las rutas en otro protocolo, únicamente maneja rutas ISIS, el parámetro "*Address Summarization: none*" indica que no se está haciendo sumarización, el parámetro "*maximun path"* indica que se pueden utilizar hasta 4 rutas de igual costo por las que se puede realizar balanceo de carga, en la sección resaltada se muestra las interfaces que son parte de IS-IS (GigabitEthernet 1/25 y loopback100), a continuación se muestra una lista de todos los equipos de los que obtiene información para construir la tabla de enrutamiento, para cada fuente se muestra la dirección IP, la distancia administrativa y el tiempo en que se recibió la última actualización.

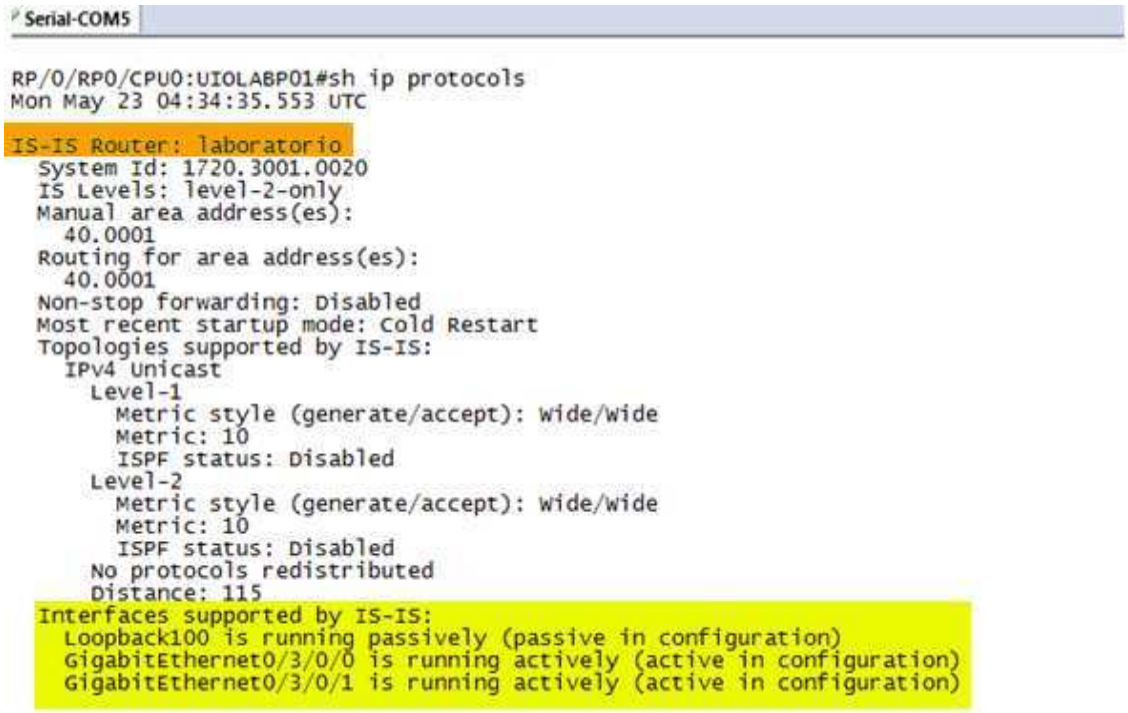


Figura 4.4: Resultado "*show ip protocols"* en UIOLABP01 IOS XR.

En la figura 4.4 se muestra el resultado del comando ***show ip protocols*** al aplicarlo en el router UIOLABP01 que utiliza el sistema IOS XR, las diferencias con el resultado obtenido en el IOS es que adicionalmente muestra la información del "*System ID"*, 6 octetos de la dirección CLNS que identifican al sistema; el "*IS Levels"* muestra los niveles de enrutamiento soportados, en este caso nivel 2 únicamente; "*manual area addresss"* es la dirección del área configurada, "*routing for area addresss"* identifica al área para la que el router provee enrutamiento, el

estado del "*Non-stop forwarding"* NFS[1] es desactivado, en "*Topologies supported by IS-IS"* se muestran las familias de direcciones configuradas, IPv4 *unicast* en este caso, dentro de la familia de direcciones se observa el valor y el estilo de las métricas configuradas para cada uno de los niveles de enrutamiento IS-IS.

Como se observa en la figura 4.3 y figura 4.4 resaltado en anaranjado se muestra que el protocolo de enrutamiento activo es IS-IS, adicionalmente resaltado en amarillo se observan las diferentes interfaces que son parte del proceso de enrutamiento IS-IS, con lo que se concluye que el protocolo de enrutamiento IS-IS se encuentra funcionando y que tiene interfaces asociadas al proceso.

Lo siguiente es comprobar si se establecieron las adyacencias con los vecinos directamente conectados, para esto se usa la sentencia ***show isis neighbors*** valido para el IOS como para el IOS XR**,** los resultados que se obtienen al usar este comando en UIOLABE02 se muestran en la figura 4.5.

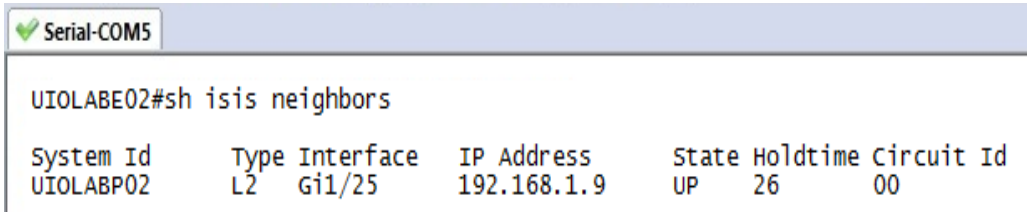
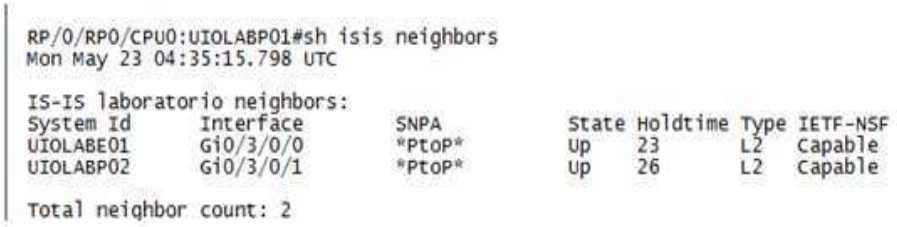


Figura 4.5: Adyacencias en el router UIOLABE02 IOS.

En la figura 4.5 se observa el nombre (*System Id*) del vecino con el que UIOLABE02 establece la adyacencia, en este caso UIOLABP02; el tipo de adyacencia, de nivel 2 (L2); la interfaz, Gi1/25 por la que aprendió la información de este sistema; la dirección IP del router vecino, 192.168.1.9 que es la dirección de UIOLABP02; el estado de la adyacencia, activa (UP); la cantidad de tiempo (*Holdtime*) que el paquete LSP-ISIS continua siendo válido, 26 segundos; y el "*circuit ID"* que identifica a cada conexión establecida sobre un medio compartido tipo broadcast, no aplica porque se especifica que la adyacencia es punto a punto y su valor es 00.

[1] Nop-stop Forwarding es una técnica de software que asegura que los paquetes IP se envíen continuamente en caso que no se pueda procesar las rutas.

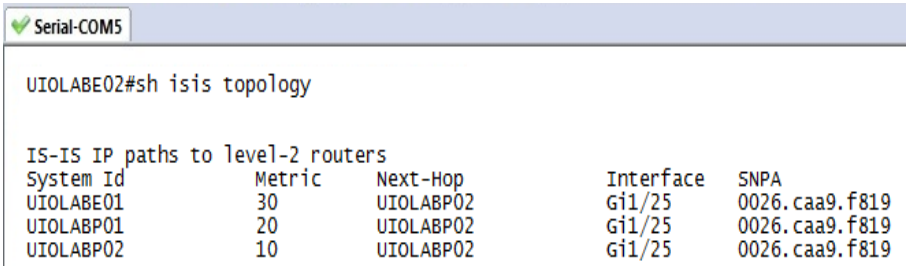


```
RP/0/RP0/CPU0:UIOLABP01#sh isis neighbors
Mon May 23 04:35:15.798 UTC

IS-IS laboratorio neighbors:
System Id      Interface        SNPA           State Holdtime Type IETF-NSF
UIOLABE01      Gi0/3/0/0        *PtoP*         Up    23       L2   Capable
UIOLABP02      Gi0/3/0/1        *PtoP*         Up    26       L2   Capable

Total neighbor count: 2
```

Figura 4.6: Adyacencias en UIOLABP01 IOS XR.

En la figura 4.6 se observa el resultado del comando ***show isis neighbors*** en el IOS XR, comparándolo con lo observado en el IOS se muestra que se eliminan los campos "*IP address"* y "*Circuit Id"*, y se aumentan el campo "*SNPA"* que es la dirección de la capa enlace de datos, *PtoP* indica un medio tipo broadcast Ethernet y finalmente el campo "IETF-NSF" indica si ese equipo soporta NSF. Se observa que UIOLABP01 establece dos sesiones una con UIOLABP02 y otra con UIOLABE01.

Una vez que se comprueba el correcto establecimiento de las adyacencias, lo siguiente es comprobar que se tiene conocimiento de todos los routers conectados en la topología. Para esto se usa la sentencia ***show isis topology***, que provee una vista de la localización relativa de todos los routers conocidos, se puede usar tanto en IOS como en IOS XR. La salida de este comando al aplicarlo en el router UIOLABE02 se observa en la figura 4.7.



Serial-COM5

```
UIOLABE02#sh isis topology


IS-IS IP paths to level-2 routers
System Id           Metric     Next-Hop            Interface   SNPA
UIOLABE01           30         UIOLABP02           Gi1/25      0026.caa9.f819
UIOLABP01           20         UIOLABP02           Gi1/25      0026.caa9.f819
UIOLABP02           10         UIOLABP02           Gi1/25      0026.caa9.f819
```

Figura 4.7: Lista de routers conocidos por UIOLABE02 IOS.

En la figura 4.7 se tiene una lista de los routers que integran la topología ISIS; por lo que se tiene un conocimiento total de la red. El campo "*System Id"* corresponde al nombre que identifica al equipo, "*Metric"* es el costo de la adyacencia entre el router UIOLABE02 y el que se muestra en el *System ID*, el campo "*Next-Hop"* muestra el router de siguiente salto por el que se puede

alcázar el *System ID*, la interfaz por la que se aprendió ese sistema y la dirección de la capa enlace de datos SNPA.

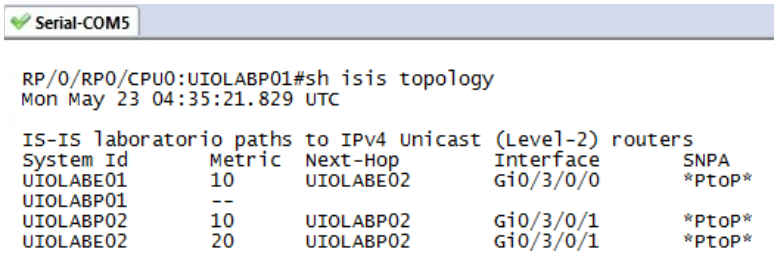


Figura 4.8: Lista de routers conocidos por UIOLABP01 IOS XR.

En la figura 4.8 se observa el resultado del comando *show isis topology* para el IOS XR, se observa una lista de los routers que integran la topología. Lo que cambia respecto al IOS es que se aumenta el *System Id* (UIOLABP01) del router en el que se aplica la sentencia y que en el campo "SNPA" se observa la sentencia *PtoP*.

Al observar que se establecen las adyacencias entre los routers que conforman la topología, y que todos estos tienen conocimiento del resto de equipos que conforman la red y son parte del proceso de enrutamiento IS-IS, se establece que el protocolo de enrutamiento se encuentra correctamente habilitado y listo para el intercambio de rutas. Finalmente se debe comprobar el intercambio de rutas, y que se tiene conocimiento de todas las redes configuradas en la topología. Para esto se usa el comando ***show ip route*** que muestra la tabla de enrutamiento con todas las rutas aprendidas por el router; se puede usar tanto en el IOS como en el IOS XR.

```
UIOLABE02#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.30.0.0/32 is subnetted, 4 subnets
C       172.30.10.40 is directly connected, Loopback100
i L2    172.30.10.30 [115/10] via 192.168.1.9, GigabitEthernet1/25
i L2    172.30.10.20 [115/20] via 192.168.1.9, GigabitEthernet1/25
i L2    172.30.10.10 [115/30] via 192.168.1.9, GigabitEthernet1/25
     192.168.1.0/30 is subnetted, 3 subnets
i L2    192.168.1.0 [115/30] via 192.168.1.9, GigabitEthernet1/25
i L2    192.168.1.4 [115/20] via 192.168.1.9, GigabitEthernet1/25
C       192.168.1.8 is directly connected, GigabitEthernet1/25
```

Figura 4.9: Tabla de enrutamiento de PE2.

En la figura 4.9 se observa la tabla de enrutamiento de UIOLABE02, donde se aprecian todas las redes de la topología, se distinguen dos grupos de prefijos, los aprendidos por ISIS que se los distingue por la letra i, y los que están directamente conectados que se las distingue por la letra C, el L2 observado en las rutas aprendidas por ISIS indica que son de nivel 2.

En las siguientes columnas se observa la dirección de la red remota aprendida, la distancia administrativa, el costo de alcázar la ruta, la dirección del siguiente salto, y la interfaz por la que se envía los paquetes que tengan como destino dicha red.

Se puede asegurar que las configuraciones de ISIS se realizaron de manera adecuada, ya que se aprenden todas las rutas publicadas por los otros routers que integran la topología, esto se verifica al comparar la tabla de enrutamiento con el plan de direccionamiento IP que se muestra en la figura 3.7 del capítulo 3.

En la figura 4.10 se observa la tabla de enrutamiento que se obtiene en el UIOLABP02 que utiliza IOS XR, la diferencia con un sistema IOS es que se observa un valor de tiempo junto a las rutas aprendidas, este es el tiempo que ha trascurrido desde que la ruta fue instalada en la tabla RIB, adicionalmente en la primera columna de las rutas, se observa que las direcciones IP configuradas en este router se distinguen con la letra L.

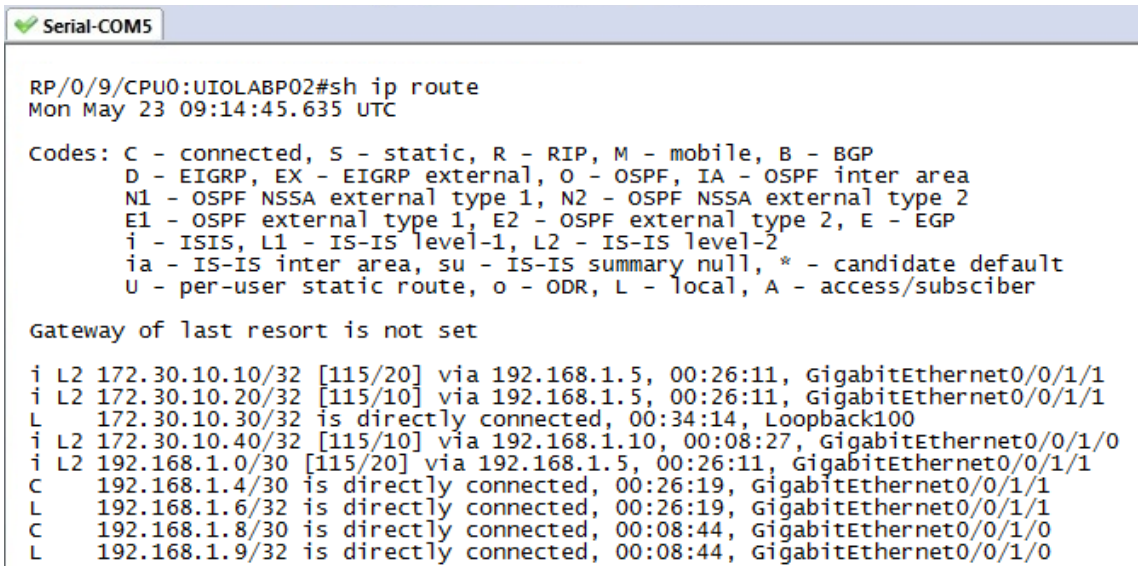


Figura 4.10: Tabla de enrutamiento IOS XR

4.1.3 COMPROBACIÓN DEL FUNCIONAMIENTO DE MPLS Y LDP[32]

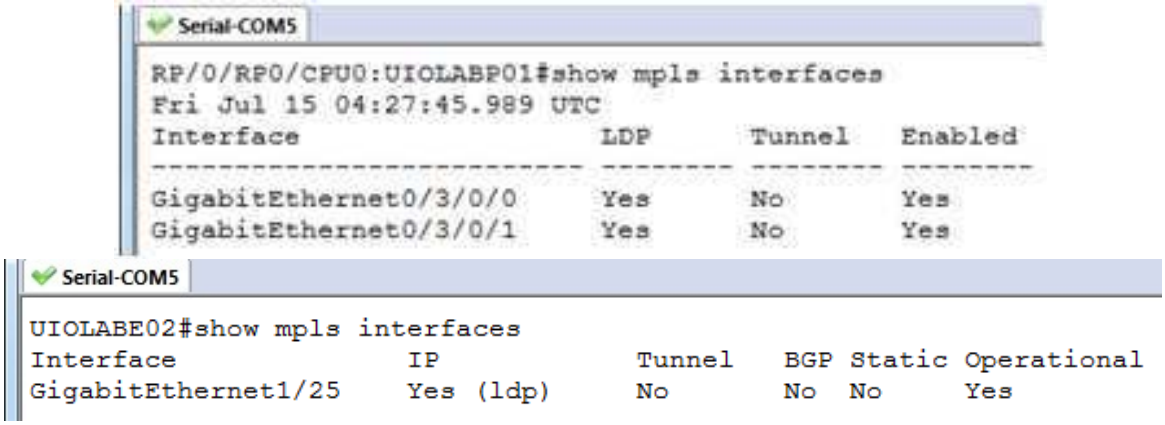


Figura 4.11: Interfaces habilitadas para MPLS

El siguiente paso es comprobar el reenvío MPLS, lo primero es verificar que las interfaces adecuadas estén habilitas para el reenvío de paquetes con MPLS, para lo cual se aplica en cada uno de los routers P y PE el comando ***show mpls interfaces***, En la figura 4.11 se muestran las salidas de estos comandos al ser aplicadas tanto en un sistema IOS como en un IOS XR.

En la figura 4.11 se puede comprobar que para el router "P" UIOLABP01 las interfaces habilitadas para el reenvío de paquetes MPLS son las interfaces "GigabitEthernet0/3/0/0 y GigabitEthernet0/3/0/1", mientras que para el router PE "UIOLABPE02" la interfaz "GigabitEthernet1/25". Donde la columna "LDP" para el P router con sistema IOS XR y columna "IP" para el caso del PE router con sistema IOS, informan si el mapeo de etiquetas a destinos IP se encuentra habilitado, y cuál es el protocolo que lo implementa , la columna "Tunnel" especifica si el etiquetamiento LSP en modo túnel se encuentra habilitado, y por último la columna "Enabled y Operational" para el "P" y "PE" router respectivamente, indica si la interfaz se encuentra habilitada para etiquetar paquetes.

Lo siguiente en verificar será el protocolo de distribución de etiquetas "LDP", verificando su estado y las adyacencias establecidas con los routers vecinos.

Entre los comandos que nos permiten verificar su estado se encuentra el comando "***show mpls ldp discovery***", el cual verifica el estado del proceso de

descubrimiento LDP, muestra la información de los vecinos LDP descubiertos, así como las interfaces sobre las cuales se tiene en ejecución el proceso de descubrimiento LDP.

En la figura 4.12 se muestra la salida de la ejecución del comando tanto en el sistema IOS como IOS XR, para el primer caso se observa que el router de frontera "UIOLABE01" tiene como identificador LDP la IP de la loopback 100 (loopback compartida), luego se muestran los vecinos LDP descubiertos, la interfaz por la cual se descubrió el vecino LDP y se mantiene el proceso de descubrimiento, en el caso del router "UIOLABE01", este descubrió un vecino LDP a través de la interfaz "Gi1/25" con un identificador LDP "172.30.10.20", el campo xmit/recv indica que la interfaz se encuentra transmitiendo y recibiendo paquetes LDP Hello de descubrimiento.

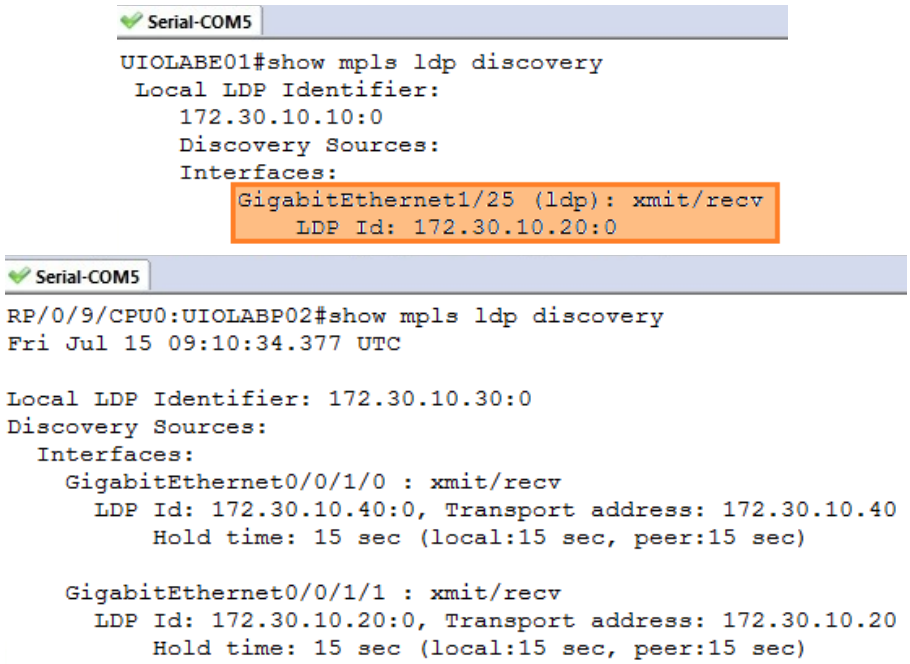


Figura 4.12: Descubrimiento de vecinos LDP.

Para el caso del IOS XR se tiene el mismo análisis, por ejemplo en el router "UIOLABP02" con LDP ID "172.30.10.30" se observa que encontró dos vecinos LDP uno por la interfaz Gi0/0/1/0 "172.30.10.40" y el otro por la interfaz Gi0/0/1/1 "172.30.10.20", donde ambas interfaces intercambian mensajes de descubrimiento LDP Hello.

Para verificar el plano de control y de envío se tienen los comandos “**show mpls ldp bindings**” y “**show mpls ldp forwarding-table**” respectivamente, el primero de estos muestra la tabla de etiquetas que el router está manejando, la cual es propagada a sus router vecinos, para que estos envíen los paquetes a dicho router con las etiquetas debidas de una forma vinculante.

En la figura 4.13 se observa la salida del comando ejecutado en el router “UIOLABP02”, se observa que este router traspasa a sus vecinos LDP “172.30.10.20 y 172.30.10.40” las etiquetas que deben ser impuestas de manera obligatoria en el envío de paquetes según la red que se desee alcanzar por medio de él; por ejemplo si los routers vecinos desean comunicarse con la red “172.30.10.10” a través de UIOLABP02, estos deben etiquetar el paquete con el valor “16002”, y en el caso de que el router “UIOLABP02” envíe tráfico hacia dicha red por medio de su router vecino con el LDP ID “172.30.10.20” este debe etiquetar el paquete con un valor “16000”, mientras que si lo envía por medio del router con LDP ID “172.30.10.40” queriendo alcanzar la misma red debe etiquetarlo con el valor “19”.

Serial-COM5

```
RP/0/9/CPU0:UIOLABP02#sh mpls ldp bindings
Fri Jul 15 09:10:40.508 UTC

172.30.10.10/32, rev 13
        Local binding: label: 16002
        Remote bindings: (2 peers)
            Peer                 Label
            -----------------    --------
            172.30.10.20:0       16000
            172.30.10.40:0       19
172.30.10.20/32, rev 12
        Local binding: label: 16001
        Remote bindings: (2 peers)
            Peer                 Label
            -----------------    --------
            172.30.10.20:0       IMP-NULL
            172.30.10.40:0       18
172.30.10.30/32, rev 2
        Local binding: label: IMP-NULL
        Remote bindings: (2 peers)
            Peer                 Label
            -----------------    --------
            172.30.10.20:0       16001
            172.30.10.40:0       16
```

Figura 4.13: Plano se control y envío.

Para el caso en el que se quiere alcanzar la IP “172.30.10.30” configurada en el router “UIOLABP02”, este les comunica a sus vecinos que la etiqueta a imponer es una IMP-NULL, lo que significa que sus routers vecinos funcionarán como el penúltimo router para alcanzar la red y estos deben realizar la operación de PHP (“Penultimate Hop Popping”) para ahorrar recursos, realizando la operación de POP en el envío de datos, evitando una doble búsqueda en el último router “UIOLABP02”.

En la figura 4.14 se tiene una salida de la ejecución del comando “**show mpls forwarding-table**” en IOS y “**show mpls forwarding**” para IOS XR, el cual muestra la tabla de envío e imposición de etiquetas para alcanzar cada uno de los prefijos (redes).

Serial-COM5

```
UIOLABE01#sh mpls forwarding-table
Local      Outgoing   Prefix           Bytes Label   Outgoing    Next Hop
Label      Label      or Tunnel Id     Switched      interface
16         Pop Label  172.30.10.20/32  0             Gi1/25      192.168.1.2
17         16001      172.30.10.30/32  0             Gi1/25      192.168.1.2
18         16002      172.30.10.40/32  0             Gi1/25      192.168.1.2
19         Pop Label  192.168.1.4/30   0             Gi1/25      192.168.1.2
20         16003      192.168.1.8/30   0             Gi1/25      192.168.1.2
```

Serial-COM5

```
RP/0/9/CPU0:UIOLABP02#sh mpls forwarding
Fri Jul 15 09:11:24.425 UTC
Local  Outgoing    Prefix            Outgoing     Next Hop        Bytes
Label  Label       or ID             Interface                    Switched
------ ----------- ----------------- ------------ --------------- ---------
16000  Pop         172.30.10.40/32   Gi0/0/1/0    192.168.1.10    36360
16001  Pop         172.30.10.20/32   Gi0/0/1/1    192.168.1.5     16308
16002  16000       172.30.10.10/32   Gi0/0/1/1    192.168.1.5     0
16003  Pop         192.168.1.0/30    Gi0/0/1/1    192.168.1.5     0
```

Figura 4.14: Tabla de envío MPLS.

En el ejemplo de la figura 4.14 para que el router “UIOLABP02” pueda alcanzar la red “172.30.10.10/32”, los paquetes dirigidos a este destino debe llegar al router UIOLABP02 con una etiqueta “16002”, donde este realiza la operación SWAP sobre la etiqueta de dichos paquetes, intercambiándola por la etiqueta de salida “16000” y enviándola por el camino asociado a la etiqueta, que para este caso es la interfaz Gi0/0/1/1, que tiene como siguiente salto la IP 192.168.1.5 que es la entrada al siguiente router “UIOLABP01”. Para el resto de prefijos contenidos en

la tabla se observa que las etiquetas a imponer a su salida son “Pop” ya que para alcanzar dichos prefijos, el router “UIOLABP02” se comporta como el penúltimo router y aplica la función de PHP.

Al comprobar la existencia e intercambio de etiquetas en el plano de control se verifica el adecuado funcionamiento del protocolo LDP, así como el establecimiento de los diferentes caminos LSP que se forman para cada uno de los prefijos de red.

A continuación se realizan pruebas de conectividad con la ayuda de **ping** y **traceroute** además de algunas capturas de paquetes con la ayuda de wireshark, en la figura 4.15 se muestra un ejemplo de las pruebas mencionadas.

En la figura 4.15 se observa en el recuadro amarillo que se tiene conectividad entre los routers de frontera UIOLABE01 con el router ID 172.30.10.10 y UIOLABE02 con el router ID 172.30.10.40, mediante el uso del comando “ping 172.30.10.40” ejecutado en el router UIOLABE01, donde no se tiene pérdida de paquetes.

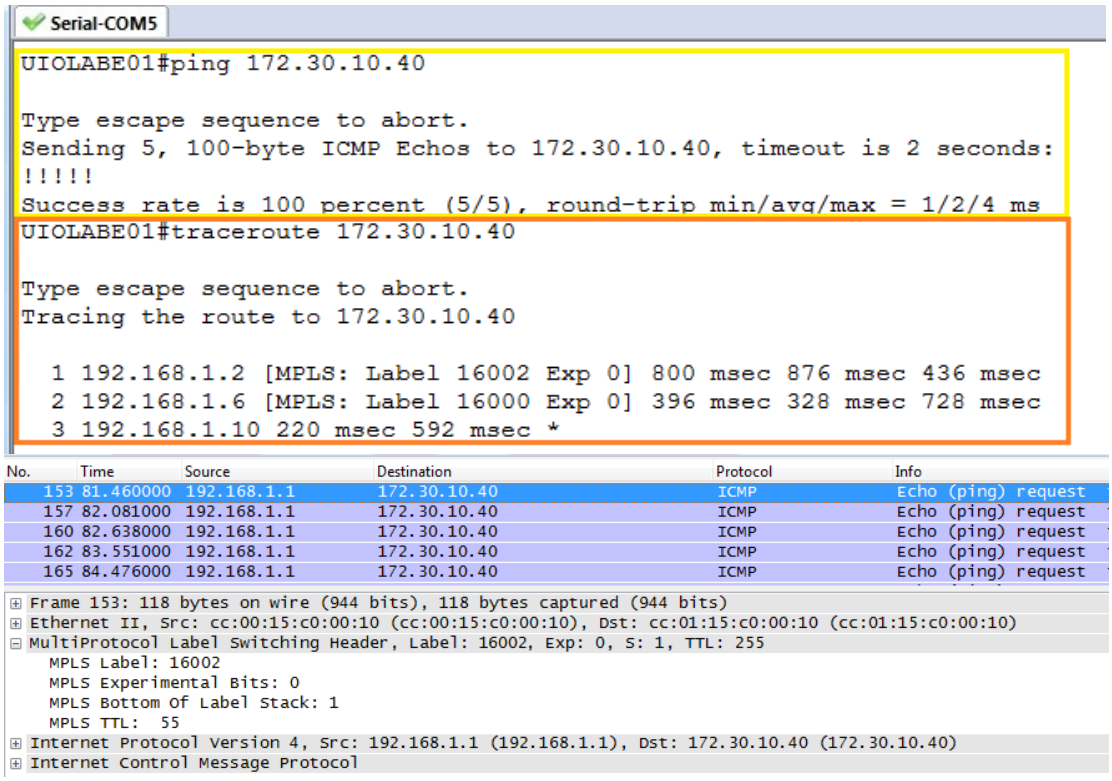


Figura 4.15: Pruebas de conectividad y capturas Wireshark.

Luego en el mismo router se utiliza el comando “traceroute 172.30.10.40” en el que se verifican los saltos de los paquetes para alcanzar el destino, y el etiquetamiento de los mismos en cada uno de los saltos, esto se puede observar en el recuadro anaranjado de la figura 4.15.

Donde se observa que para el envío de paquetes desde el router UIOLABE01 hacia el router UIOLABE02, los paquetes en su primer salto hacia el router UIOLABP01, van con la etiqueta 16002, donde se realiza la operación SWAP, intercambiando dicha etiqueta por una nueva de valor 16000, para reenviar el paquete hacia el próximo salto el router UIOLABP02, éste al recibir dichos paquetes con la etiqueta 16000 realiza la operación de POP, quitando dicha etiqueta del paquete y reenviándolo hacia su destino, debido a que este es el penúltimo salto antes de alcanzar la red 172.30.10.40.

A continuación se observa una captura de los paquetes en la interfaz Gigabitehternet 1/25 del router UIOLABE01, en la que se verifica que los paquetes dirigidos hacia el router UIOLABP01, con destino a la red 172.30.10.40 tienen asociado la etiqueta 16002.

En la figura 4.16 se demuestra el intercambio de los mensajes de descubrimiento LDP Hello entre el router “UIOLABE01” y “UIOLABP01”

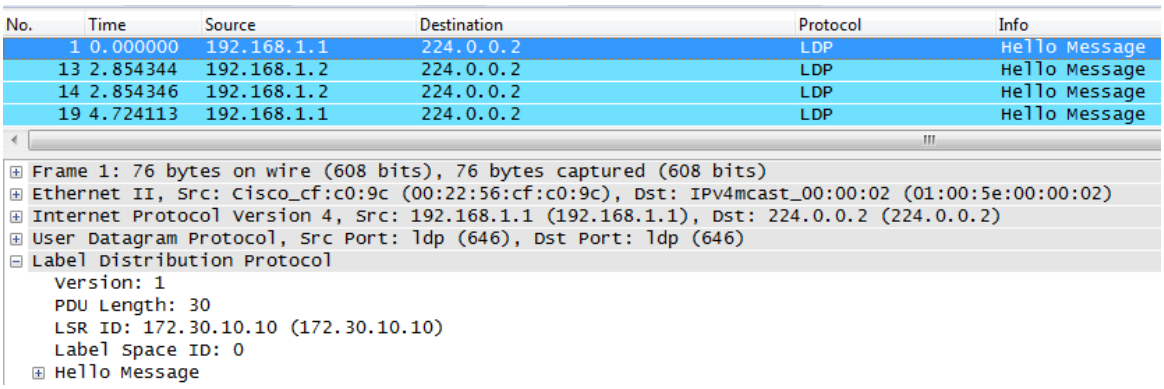


Figura 4.16: Intercambio de mensajes de descubrimiento.

Las pruebas mostradas en esta sección han sido tomadas como una demostración y ejemplo de las pruebas y resultados que se aplicaron y obtuvieron en cada uno de los routers pertenecientes al backbone MPLS.

Una vez comprobado que el protocolo de enrutamiento IS-IS, intercambia los prefijos de red; el protocolo de distribución de etiquetas LDP, asigna las etiquetas para los diferentes LSP; que las interfaces de los routers están habilitadas para el reenvío MPLS; y que las pruebas de conectividad fueron exitosas, se concluye que el funcionamiento de MPLS es el adecuado.

4.2 PRUEBAS Y RESULTADOS DE BGP [5] [12]

A continuación se procede a detallar las pruebas realizadas y los resultados obtenidos. Para observar el funcionamiento de las diferentes configuraciones se utilizarán los diferentes comandos, disponibles tanto en el IOS como en el IOS XR.

En la parte inicial se comprobará el funcionamiento de las configuraciones básicas de las topologías. Después se realizará las diferentes modificaciones y configuraciones adicionales necesarias para cada una de las pruebas, se comprobará el funcionamiento de las mismas y se verifica que los cambios obtenidos sean los esperados. Las configuraciones finales obtenidas se detallan en el anexo 1.

4.2.1 PRIMER ESCENARIO

Antes de realizar las pruebas es necesario establecer si las configuraciones iniciales se realizaron de manera adecuada, para realizar las comprobaciones básicas se observó el adecuado funcionamiento de ISIS y MPLS que se detallan a continuación en las figuras 4.17 y 4.18.

```
RP/0/9/CPU0:R2#sh isis neighbors
Wed Jun 15 09:05:25.083 UTC

IS-IS laboratorio neighbors:
System Id      Interface        SNPA           State Holdtime Type IETF-NSF
R1             Gi0/0/1/1        *PtoP*         Up    29       L2   Capable

R3>enable
R3#show isis neighbors

Tag null:
System Id      Type Interface   IP Address      State Holdtime Circuit Id
R4             L2   Gi9/1       192.168.0.1     UP    26       00

R5>enable
R5#show isis neighbors

System Id      Type Interface   IP Address      State Holdtime Circuit Id
R6             L2   Gi1/1       172.31.0.2      UP    29       00
```

Figura 4.17: Adyacencias IS-IS.

En la figura 4.17 se observa que se han establecido las adyacencias IS-IS dentro de los sistemas autónomos; estas son en el recuadro amarillo, R1 con R2; en el recuadro anaranjado, R3 con R4 y en el recuadro verde, R5 con R6. En el estado de todas las adyacencias se observa “UP” lo que indica que se establecieron de manera adecuada y que se pueden intercambiar las rutas dentro del SA, con lo que se comprueba el adecuado funcionamiento básico de IS-IS.

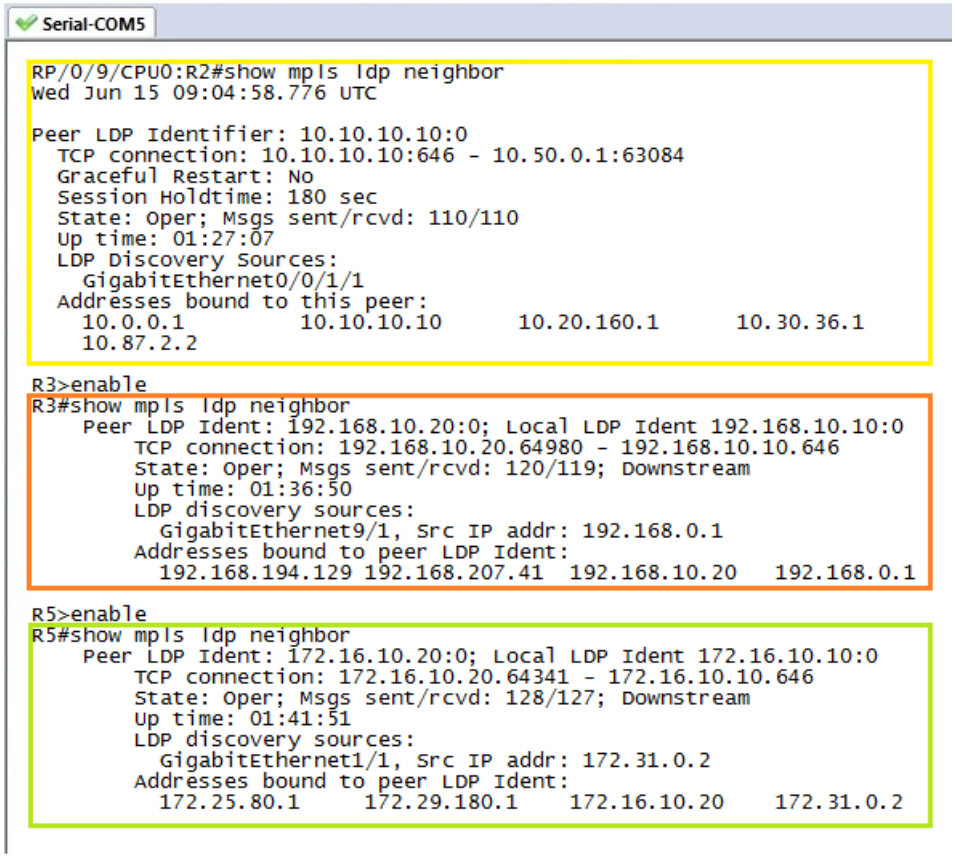


Figura 4.18: Sesiones LDP.

En la figura 4.18 se observa que las sesiones LDP se establecieron de las siguiente manera: en el recuadro amarillo, R2 con R1 (10.10.10.10); en el recuadro anaranjado R3 con R4 (192.16.10.20), y en el recuadro verde R5 con R6 (172.16.10.20), las sesiones se encuentran en estado “oper” (Operacional), en “Msgs sent/rcvd” se observa que se está produciendo el intercambio de mensajes LDP, con esto se comprueba el adecuado funcionamiento de MPLS, que permite el envío de paquetes etiquetados dentro del SA.

Con las configuraciones básicas funcionando adecuadamente, se procede a comprobar si el protocolo BGP funciona de manera adecuada, para eso se debe observar si se establecieron las sesiones con sus vecinos. La sentencia ***show ip bgp neighbors*** brinda información de las conexiones BGP que se establecen con los vecinos y el estado en que se encuentran las sesiones.

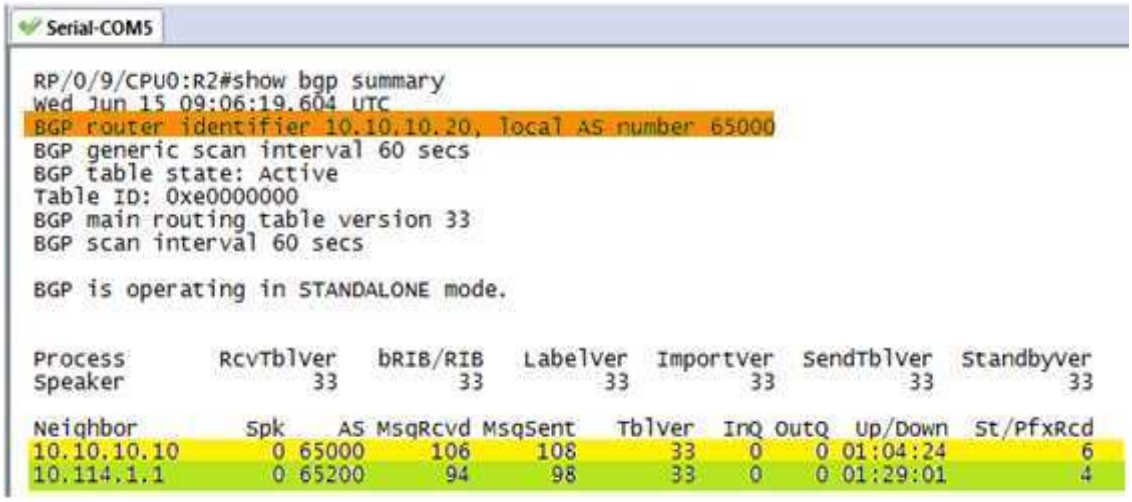


Figura 4.19: Sesiones BGP de R2 en IOS XR.

En la figura 4.19 observa que R2 (10.10.10.20) ha establecido dos sesiones una IBGP con R1 señalado en amarillo, cuya dirección IP 10.10.10.10 es la asignada como router id, es la dirección de la loopback 100 y se usa como origen para las actualizaciones. Se determina que es una sesión IBGP debido a que R2 pertenece al SA 65000 como se observa en lo resaltado en anaranjado, y en la información de la sesión se observa que R1 pertenece al mismo SA.

La otra sesión resaltada en verde, es una EBGP, se establece con R5 con la dirección IP 10.114.1.1 que es la dirección de la interfaz directamente conectada con la que se puede establecer una conexión sin necesidad de un protocolo de enrutamiento. Se determina que es una sesión EBGP debido a que R2 pertenece al SA 65000, y en la información de la sesión se observa que R5 pertenece al SA 65200.

Se establece que las sesiones BGP están arriba porque en el campo UP/DOWN se muestra el tiempo que estas han estado activas.

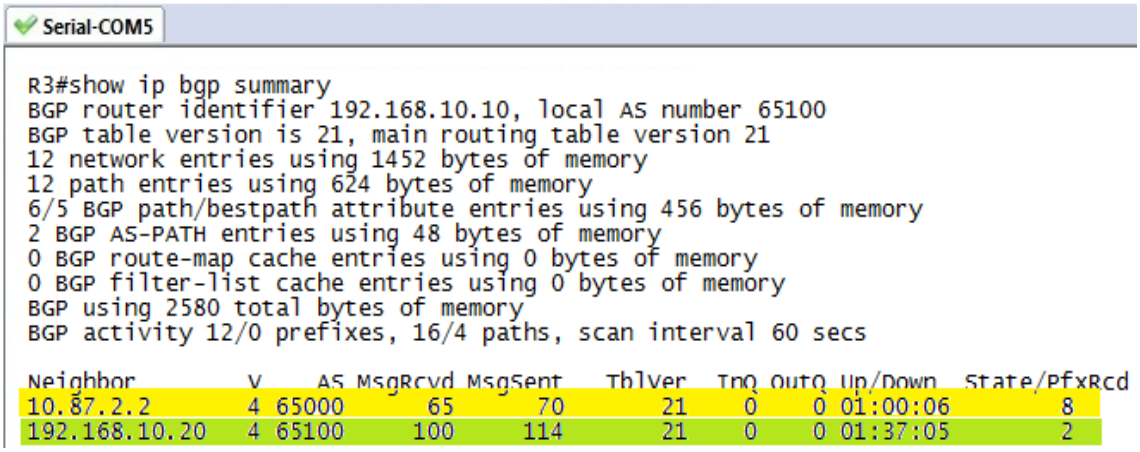


Figura 4.20: Sesiones BGP de R3

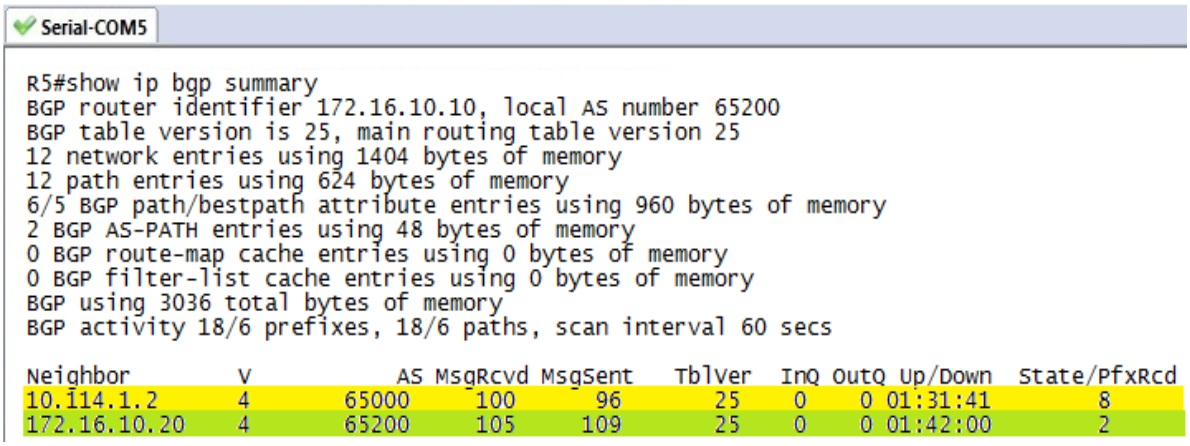


Figura 4.21: Sesiones BGP de R5

Para la figura 4.20 se observa que R3 “192.168.10.20” establece una sesión IBGP con R4 (resaltado de verde) y una EBGP con R1 “10.87.2.2” (resaltado en amarillo), de la misma manera en la figura 4.21 se muestra que R5 establece una sesión IBGP con R6 “172.16.10.20” (resaltado en verde) y una sesión EBGP con R2 “10.114.1.2” (resaltado en amarillo), las sesiones para ambos routers se establecieron con las mismas caracterizas descritas para R2. No se detalla las sesiones formadas por los otros tres routers pues con estos tres se observan todas las sesiones establecidas dentro de la topología.

Lo siguiente es comprobar que las rutas se estén intercambiando de manera adecuada dentro del SA y con los SA vecinos, para lo que se debe observar las tablas de enrutamiento de los routers. La sentencia **show ip bgp** nos muestra la tabla de enrutamiento BGP de un equipo, los campos que despliega este comando, se observa en la figura 4.22.

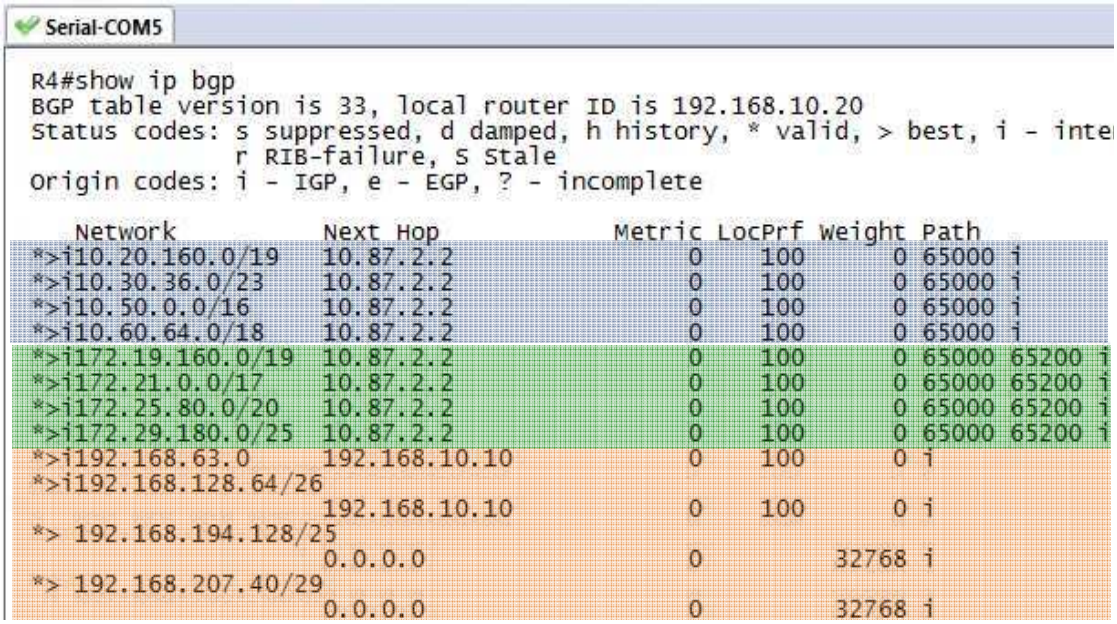


Figura 4.22: Tabla de enrutamiento de BGP en R4.

La interpretación de los campos de la tabla de enrutamiento es: el código de estatus se muestra en la primera columna. Los códigos de estatus son "*" ruta valida, "s" ruta eliminada, "d" indica intermitencia de la ruta y por lo tanto no se publica, "h" histórico indica que la ruta es invalida e inalcanzable, "r" una falla en la RIB (Routing information Base) por lo que la ruta no se instaló y "s" indica una ruta vieja. En la figura 4.22 se observa que todas las rutas son validas, por lo que se asegura que el intercambio de rutas es adecuado.

El símbolo ">" de la segunda columna indica que ha sido seleccionado como el mejor camino, la tercera columna indica con una "i" que fue aprendida de un vecino IBGP, si está en blanco en cambio la aprendió de un vecino externo, la cuarta columna son las redes aprendidas, la quinta columna lista las direcciones de siguiente salto; para todas las rutas en caso de mostrarse 0.0.0.0 el router originó la ruta, las siguientes tres columnas son los atributos BGP MED, *local-preference* y *weigth*; la columna *path* contiene una secuencia de SA; de izquierda a derecha el primero es el SA adyacente y el último es el origen de la ruta. Los valores del origen pueden ser: "i" significa que la entrada fue originada por un IGP y se publica con el comando *network,"*e" indica que la entrada fue originada por EGP, y "?" significa que el origen de ruta no está claro (*incomplete*), este origen se da cuando se redistribuyen rutas de un IGP en BGP.

En la figura 4.22 se visualizan doce rutas aprendidas por BGP, las cuatro primeras rutas son originadas en el SA 65000, las cuatro siguientes las origina el SA 65200 y las cuatro últimas se originan en el SA local; de estas últimas las dos primeras se originaron en el vecino IBGP y las 2 últimas son direcciones de redes directamente conectadas que serán publicadas por R4. Todas las rutas son aprendidas de un vecino IBGP, son rutas seleccionadas como el mejor camino y se instalarán en la tabla de enrutamiento IP.

Al comparar la tabla de enrutamiento BGP de R4 de la figura 4.22 con la figura 3.8 del capítulo 3, se observa que las direcciones de red de las loopback 10 y 20 de todos los router de la topología, que se publican por BGP se encuentran en la tabla BGP de R4, por lo que se concluye que todos los routers se encuentran publicando los prefijos de red dispuestos verificándose que las sesiones IBGP y EBGP funcionan adecuadamente.

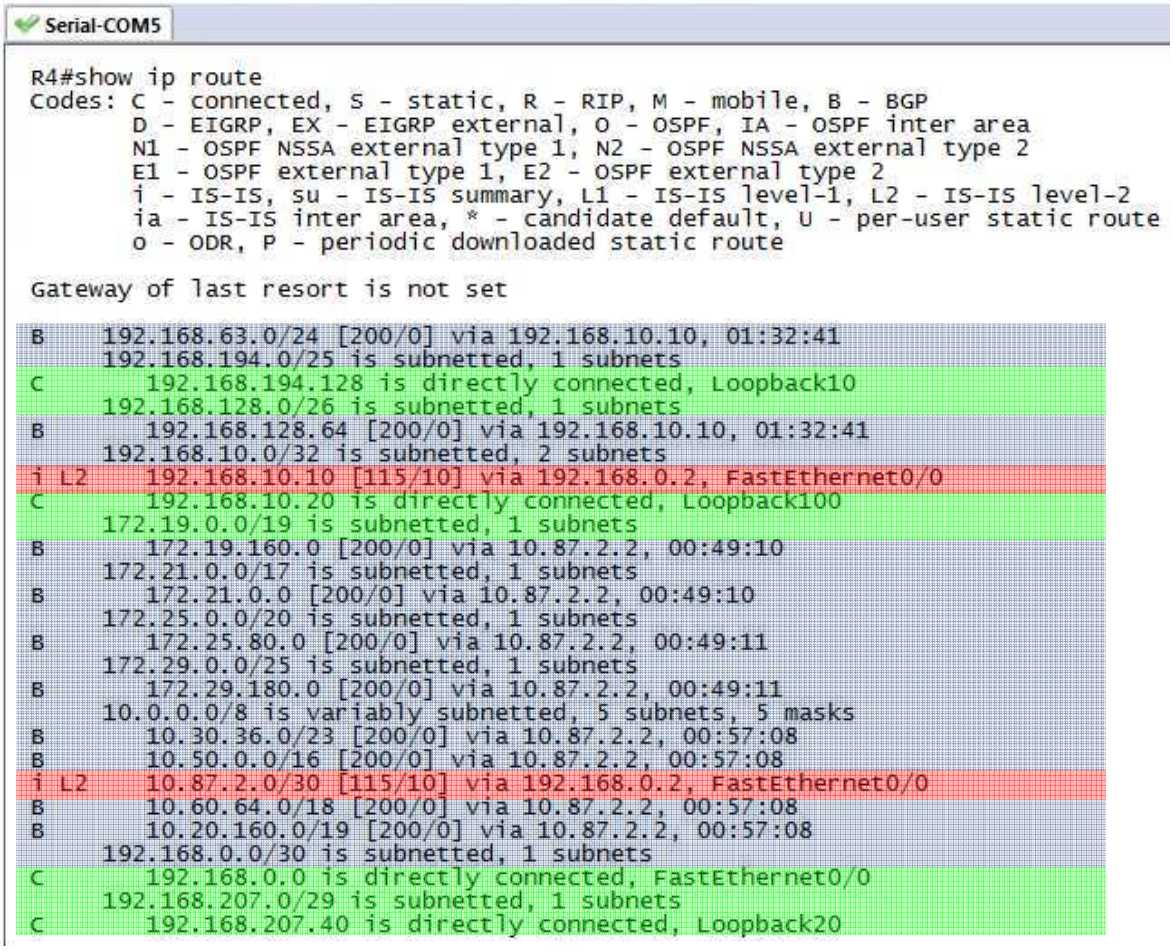


Figura 4.23: Tabla de enrutamiento IP.

Al comparar la tabla de enrutamiento IP de R4 de la figura 4.23 con la figura 3.8 del capítulo 3, se observa que las direcciones de red instaladas en dicha tabla son: las directamente conectadas, las aprendidas por IS-IS y las aprendidas por BGP, con lo que se establece que el intercambio de rutas por el IGP y el EGP es correcta.

Serial-COM5

```
R6#show ip bgp
BGP table version is 25, local router ID is 172.16.10.20
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*>i10.20.160.0/19   10.114.1.2               0    100      0 65000 i
*>i10.30.36.0/23    10.114.1.2               0    100      0 65000 i
*>i10.50.0.0/16     10.114.1.2               0    100      0 65000 i
*>i10.60.64.0/18    10.114.1.2               0    100      0 65000 i
*>i172.19.160.0/19  172.16.10.10             0    100      0 i
*>i172.21.0.0/17    172.16.10.10             0    100      0 i
*> 172.25.80.0/20   0.0.0.0                  0         32768 i
*> 172.29.180.0/25  0.0.0.0                  0         32768 i
*>i192.168.63.0     10.114.1.2               0    100      0 65000 65100 i
*>i192.168.128.64/26
                    10.114.1.2               0    100      0 65000 65100 i
*>i192.168.194.128/25
                    10.114.1.2               0    100      0 65000 65100 i
*>i192.168.207.40/29
                    10.114.1.2               0    100      0 65000 65100 i
```

Figura 4.24: Tabla de enrutamiento BGP en R6.

Serial-COM5

```
R6#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

B    192.168.63.0/24 [200/0] via 10.114.1.2, 01:11:17
     192.168.194.0/25 is subnetted, 1 subnets
B       192.168.194.128 [200/0] via 10.114.1.2, 01:11:17
     192.168.128.0/26 is subnetted, 1 subnets
B       192.168.128.64 [200/0] via 10.114.1.2, 01:11:17
     172.16.0.0/32 is subnetted, 2 subnets
C       172.16.10.20 is directly connected, Loopback100
i L2    172.16.10.10 [115/10] via 172.31.0.1, FastEthernet0/0
     172.19.0.0/19 is subnetted, 1 subnets
B       172.19.160.0 [200/0] via 172.16.10.10, 01:28:06
     172.21.0.0/17 is subnetted, 1 subnets
B       172.21.0.0 [200/0] via 172.16.10.10, 01:45:26
     172.25.0.0/20 is subnetted, 1 subnets
C       172.25.80.0 is directly connected, Loopback10
     172.29.0.0/25 is subnetted, 1 subnets
C       172.29.180.0 is directly connected, Loopback20
     172.31.0.0/30 is subnetted, 1 subnets
C       172.31.0.0 is directly connected, FastEthernet0/0
     10.0.0.0/8 is variably subnetted, 5 subnets, 5 masks
B       10.30.36.0/23 [200/0] via 10.114.1.2, 01:11:19
B       10.50.0.0/16 [200/0] via 10.114.1.2, 01:35:55
B       10.60.64.0/18 [200/0] via 10.114.1.2, 01:35:55
i L2    10.114.1.0/30 [115/10] via 172.31.0.1, FastEthernet0/0
B       10.20.160.0/19 [200/0] via 10.114.1.2, 01:11:19
     192.168.207.0/29 is subnetted, 1 subnets
B       192.168.207.40 [200/0] via 10.114.1.2, 01:11:19
```

Figura 4.25: Tabla de enrutamiento IP en R6.

En la figura 4.24 y 4.25 se observan las tablas de enrutamiento BGP e IP de R6 respectivamente, se tienen características similares a las descritas, la diferencia es que las rutas internas del SA, las que están directamente conectadas, y las aprendidas por IS-IS cambian. También cambian las direcciones de siguiente salto por las que se puede alcanzar las redes. Se observa que se mantienen las doce redes aprendidas por BGP y que se instalan correctamente en la tabla de enrutamiento IP.

No se colocan las tablas de enrutamiento de todos los routers de la topología, ya que al considerar que R4 y R6 son los extremos de la topología, y que todas las redes configuradas en BGP se encuentran en sus tablas de enrutamiento, implica que todas las rutas han pasado por los routers intermedios y estos las han publicado de manera adecuada, por lo que se concluye que las rutas BGP en los otros equipos serán las mismas.

4.2.1.1 Pruebas de Mapas de Ruta. [4] [18] [19]

Una vez comprobado el funcionamiento de las configuraciones de BGP y que las rutas se intercambian de manera adecuada entre los diferentes sistemas autónomos se procederá a realizar el filtrado de rutas, para esto en R1 se aplicará un mapa de ruta como política de salida, que evitará que se publiquen las redes 172.25.80.0/20 y 172.21.0.0/17 a R3, la configuración aplicada en R1 es:

```
! Listas de acceso
access-list 1 permit 172.25.80.0 0.0.15.255
access-list 1 permit 172.21.0.0 0.0.127.255
!
! Mapa de ruta
route-map rutas_salida deny 0
 match ip address 1
!
route-map rutas_salida permit 10
!
! Asociación del mapa de ruta
router bgp 65000
neighbor 10.87.2.1 route-map rutas_salida out
!
```

En la configuración se crea una lista de acceso que será la encarga de identificar las rutas a filtrar, el mapa de ruta rutas-salida en base a la lista de acceso negará

que se publiquen estas rutas. La segunda sentencia *route-map* permitirá el envío de todas las demás rutas, es importante colocar esta sentencia para evitar una denegación completa, la misma que evitará que se publique cualquier ruta. La tabla de enrutamiento BGP de R3 antes de aplicar la política se muestra en la figura 4.26, donde se observa que todas las rutas están presentes.

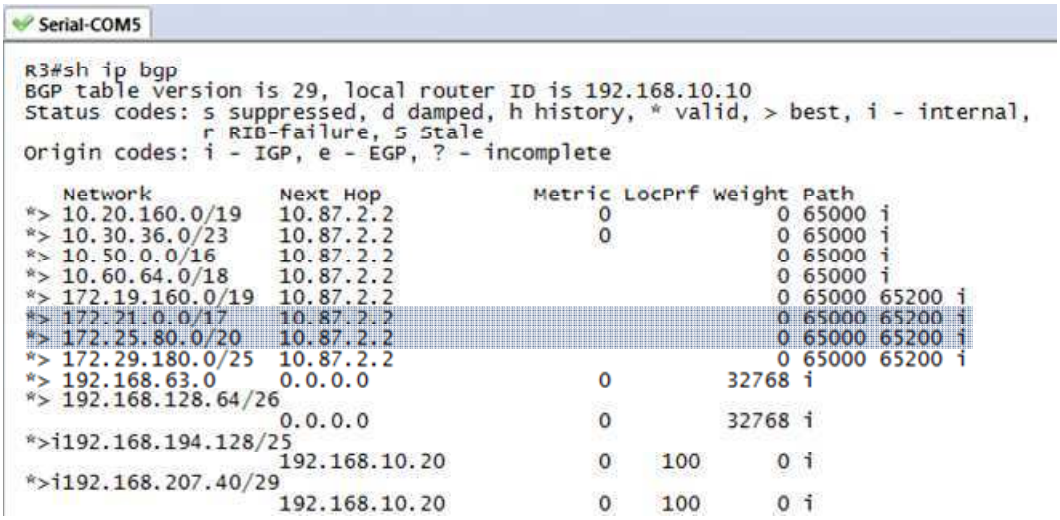


Figura 4.26: Tabla de enrutamiento de R3.

Una vez configurado el mapa de ruta en R1 se lo aplica como política de salida en las rutas a publicar a R3. Para observar los cambios es necesario reiniciar la sesión BGP con el comando "*clear ip bgp * ",* para que de esta manera las nuevas políticas tengan efecto, la tabla de enrutamiento de R3 una vez aplicada la política se muestra en la figura 4.27 donde se observa que no se encuentran los prefijos 172.25.80.0/20 y 172.21.0.0/17 comprobándose la correcta configuración y funcionamiento del mapa de ruta.

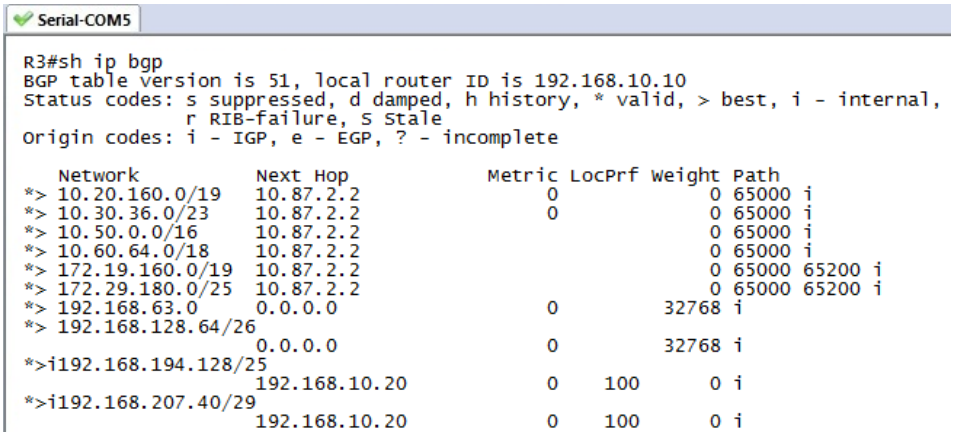


Figura 4.27: Tabla de enrutamiento R3 después de aplicar la política.

Adicional al filtrado, los mapas de ruta se pueden utilizar para alterar los valores de las métricas de BGP que cambian la elección de la ruta preferida, lo que permite por ejemplo realizar balanceo de carga que se mostrará más adelante, para cambiar el valor del atributo MED en el R1 se añadieron las configuraciones mostradas a continuación:

```
access-list 2 permit 10.50.0.0 0.0.255.255
access-list 2 permit 10.20.160.0 0.0.31.255
route-map rutas_salida permit 5
 match ip address 2
 set metric 55
```

Con estas configuraciones se aumenta una acción en el mapa de ruta "rutas-salida", esta se ejecutará a continuación del filtrado realizado anteriormente. Al aumentar esta sentencia se comprueba la flexibilidad de los mapas de ruta, que permiten el aumento de sentencias, sin tener que eliminar las configuraciones anteriores, para volver a crear la nueva política. La sentencia mostrada altera el valor por defecto del atributo MED publicado por R1 y enviado R3, en los prefijos 10.20.160.0/19 y 10.50.0.0/16, este cambio se observa en la figura 4.28 donde el valor por defecto de 0 ha sido cambiado por 55.

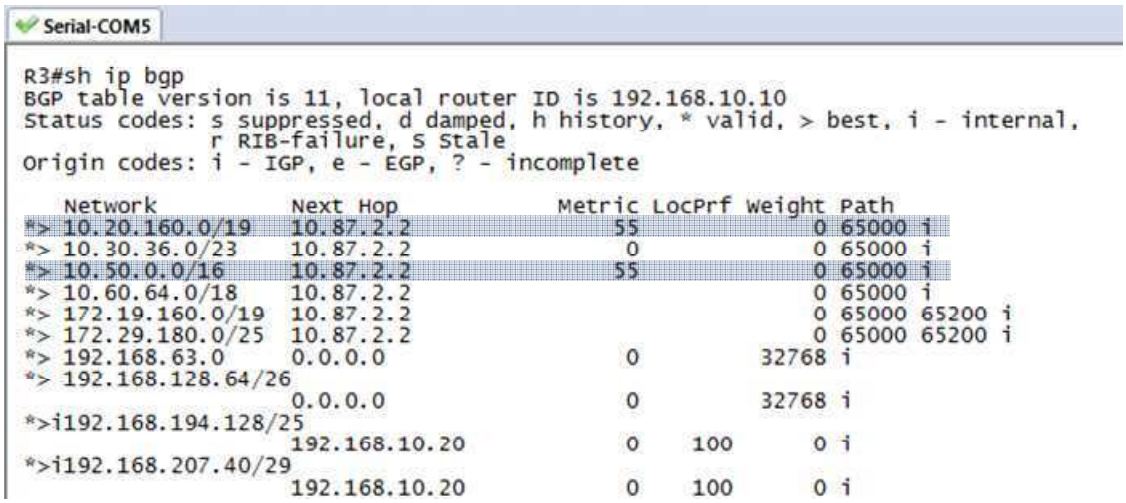


Figura 4.28: Tabla de R3 alterado el atributo MED.

En el mapa de ruta anterior se creó una política que filtraba las rutas especificadas y permitía el resto de rutas, se la aplicó como política de salida. A continuación en cambio se creará una política que permita las redes especificadas y filtre el resto de las rutas. Se la aplicará en R5 como política de entrada para las rutas recibidas de R2. Para crearla en el R5 se añadió la siguiente configuración:

```
access-list 1 permit 192.168.63.0 0.0.0.255
access-list 1 permit 192.168.207.40 0.0.0.7
!
route-map rutas_entrada permit 10
 match ip address 1
!
router bgp 65200
 neighbor 10.114.1.2 route-map rutas_entrada in
!
```

Mediante la configuración anterior se permitirán las redes 192.168.63.0/24 y 192.168.207.40/29, el resto de redes publicadas por R2 no se instalarán en la tabla de R5, las redes directamente conectadas a R5 y las aprendidas de R6 se instalarán correctamente, esto se puede observar en la figura 4.30, mientras que en la figura 4.29 se observa la tabla de enrutamiento de R5 antes de aplicar la política, donde se observa como todas las rutas se encuentran presentes.

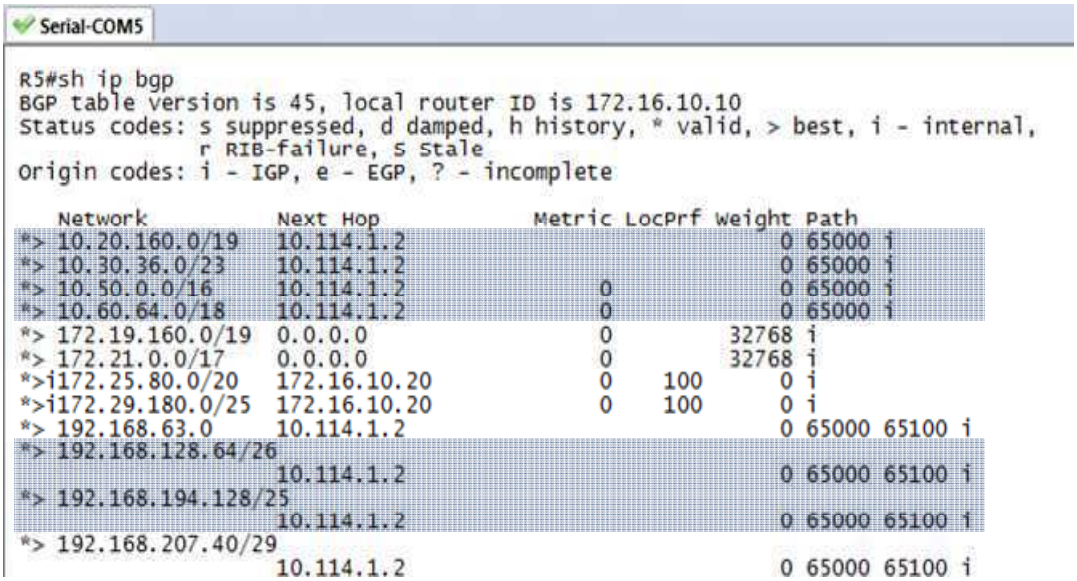


Figura 4.29: Tabla de enrutamiento de R5 antes de aplicar la política.

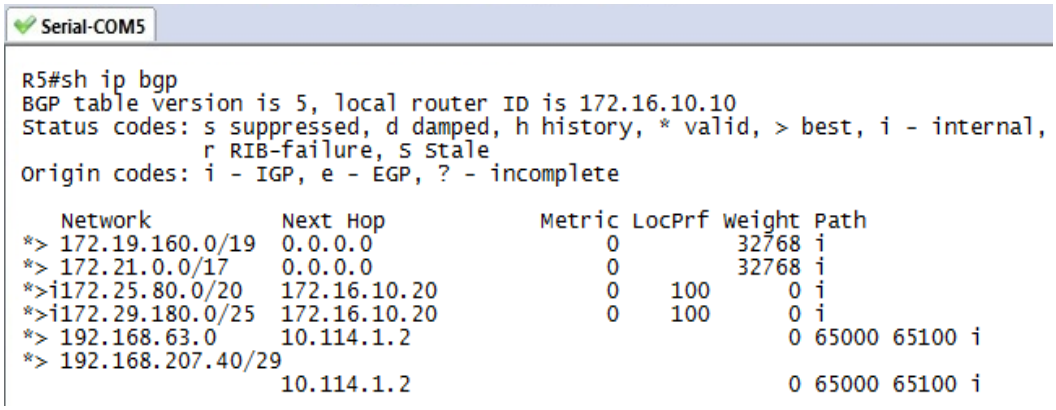


Figura 4.30: Tabla de enrutamiento R5.

4.2.1.2 Pruebas de Listas de Prefijos. [4] [5]

Una opción alterna para filtrar las rutas a ser publicadas, son las listas de prefijos, estas se pueden configurar para filtrar las rutas que se instalan en la tabla de enrutamiento, o para filtrar las rutas que se publican a un par BGP.

Para probar las listas de prefijos se parte de la configuración inicial, en la que se publican todas las redes a todos los routers, sin ninguna política configurada, a excepción de la configurada en R2 que es un prerrequisito para enviar y recibir todas las rutas en el IOS XR. La configuración aumentada en R5 para colocar una lista de prefijos es la siguiente:

```
ip prefix-list in_R5 seq 5 deny 192.0.0.0/6 ge 24 le 30
ip prefix-list in_R5 seq 10 deny 10.20.160.0/19
ip prefix-list in_R5 seq 15 permit 0.0.0.0/0 le 32
!
router bgp 65200
 neighbor 10.114.1.2 prefix-list in_R5 in
!
```

En las configuraciones anteriores se crea una lista de prefijos “in_R5”, que filtrará el rango 192.0.0.0/24 a 192.0.0.152/30 y la red 10.20.160.0/19 , la seq 15 permite que se instalen las demás redes. Esto se puede observar en la figura 4.31 donde se nota la ausencia de las redes señaladas, comparándola con la tabla de enrutamiento original antes de aplicar la política que se muestra en la figura 4.29.

Serial-COM5

```
R5#sh ip bgp
BGP table version is 8, local router ID is 172.16.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.30.36.0/23    10.114.1.2                           0 65000 i
*> 10.50.0.0/16     10.114.1.2               0           0 65000 i
*> 10.60.64.0/18    10.114.1.2               0           0 65000 i
*> 172.19.160.0/19  0.0.0.0                  0       32768 i
*> 172.21.0.0/17    0.0.0.0                  0       32768 i
*>i172.25.80.0/20   172.16.10.20             0    100      0 i
*>i172.29.180.0/25  172.16.10.20             0    100      0 i
```

Figura 4.31: Tabla de enrutamiento R5.

Similar a los mapas de ruta las listas de prefijos se pueden aplicar como política de entrada o de salida, pero con la restricción de que realizan únicamente el filtrado de las rutas, sin alterar los atributos de BGP.

4.2.1.3 Pruebas de *Routing Policy.* [11] [21] [22]

Las pruebas del *routing policy* se realizan en el R2 que es el router que tiene el IOS XR. Es necesario utilizar este IOS debido a que las *routing policy* son una nueva característica introducida en este sistema operativo, se pueden aplicar como política de entrada o de salida.

En la figura 4.32 se muestra la tabla de enrutamiento BGP de R2, antes de la aplicación de las políticas, la topología tendrá únicamente las configuraciones iniciales, por lo que todas las rutas serán aprendidas sin ninguna modificación en sus atributos.

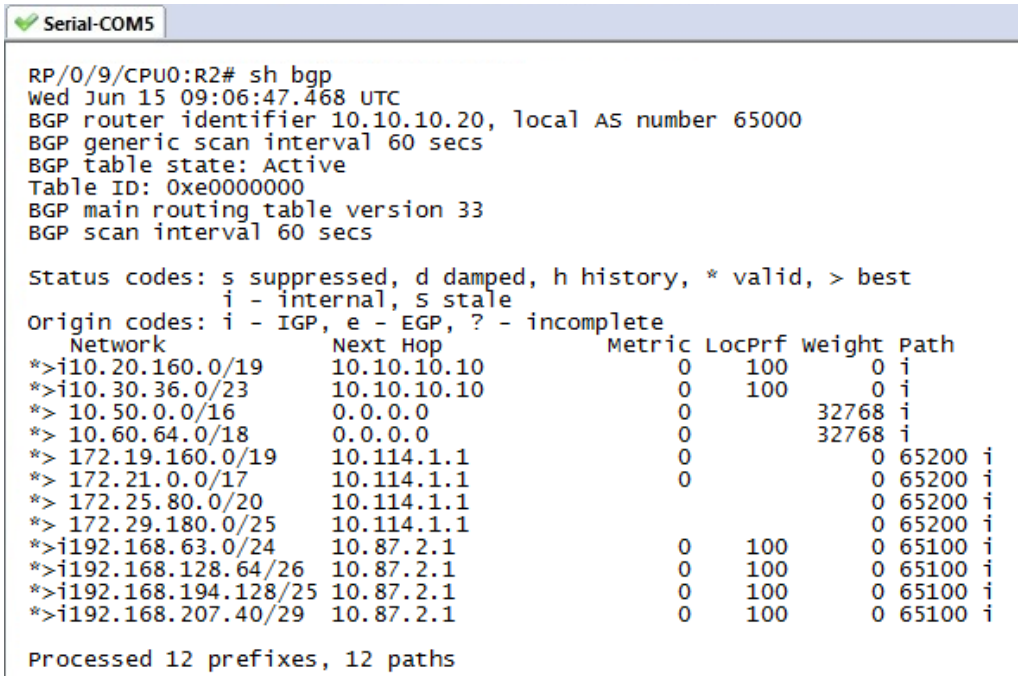


Figura 4.32: Tabla de enrutamiento R2.

Para realizar las pruebas se crearon dos *routing policy,* una se aplicará como política de entrada y otra como política de salida en R2. Las configuraciones aplicadas para crear la política de entrada se muestran a continuación:

```
route-policy permitir_in
  if destination in(172.29.180.0/25) then
    set origin incomplete
  elseif med eq 30 then
    drop
  elseif next-hop in(10.114.1.1) then
    set local-preference 300
```

```
  else
    pass
  endif
end-policy
!
router bgp 65000
neighbor 10.114.1.1
  address-family ipv4 unicast
   route-policy permitir_in in
```

En las configuraciones anteriores se crea una política "*permitir_in"* colocada como política de entrada para las rutas recibidas de R5, esta se encarga de colocar el origen en *incomplete,* para el prefijo 172.29.180.0/25; elimina aquellos prefijos con el atributo MED en 30; coloca el atributo *local-preference* en 300, en los prefijos que tengan como dirección del siguiente salto 10.114.1.1, el resto de prefijos los deja pasar sin ningún inconveniente.

Los cambios realizados por esta política al aplicarlos en R3 se observan en la figura 4.33, donde se muestra que para la red 172.29.180.0/25 (señalada en azul) que tiene como dirección de siguiente salto 10.114.1.1, el atributo *local-preference* no se coloca en 300, esto se debe a que coincide con el primer criterio que coloca el origen de ruta en *incomplete* (?), por lo que no se aplicarán el resto de criterios configurados en la política, este es el comportamiento por defecto de los routing policy, donde se aplica la acción del primer criterio coincidente, siendo el resto de acciones de la política ignoradas.

Para completar la prueba en R5 se cambió el atributo MED de la red 172.19.0.0/17 por 30, para que de esta manera se tenga una coincidencia con el criterio "*med eq 30",* usado en la política *permitir_in* aplicada en R2. Lo cual se puede verificar en la tabla de enrutamiento BGP de R2 mostrada en la figura 4.33, donde se observa la ausencia de este prefijo comparándolo con lo obtenido en la figura 4.32. La configuración en R5 fue la siguiente:

```
access-list 1 permit 172.19.0.0 0.0.231.255
!
route-map rutas_salida permit 10
 match ip address 1
 set metric 30
!
route-map rutas_salida permit 20
!
```

```
router bgp 65200
 neighbor 10.114.1.2 route-map rutas_salida out
!
```

Serial-COM5

```
RP/0/9/CPU0:R2#sh bgp
Fri Jun 17 08:00:38.752 UTC
BGP router identifier 10.10.10.20, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000
BGP main routing table version 80
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i10.20.160.0/19   10.10.10.10              0    100      0 i
*>i10.30.36.0/23    10.10.10.10              0    100      0 i
*> 10.50.0.0/16     0.0.0.0                  0         32768 i
*> 10.60.64.0/18    0.0.0.0                  0         32768 i
*> 172.21.0.0/17    10.114.1.1               0    300      0 65200 i
*> 172.25.80.0/20   10.114.1.1               0    300      0 65200 i
*> 172.29.180.0/25  10.114.1.1                           0 65200 ?
*>i192.168.63.0/24  10.87.2.1                0    100      0 65100 i
*>i192.168.128.64/26 10.87.2.1               0    100      0 65100 i
*>i192.168.194.128/25 10.87.2.1              0    100      0 65100 i
*>i192.168.207.40/29 10.87.2.1               0    100      0 65100 i

Processed 11 prefixes, 11 paths
```

Figura 4.33: Tabla de enrutamiento BGP en R2 después de aplicar la política.

A continuación se muestran las configuraciones aplicadas en R2 para crear la política de salida:

```
prefix-set permitidas_salida
  192.168.0.0/16 le 30,
  10.30.36.0/23,
  10.50.0.0/16
end-set
!
route-policy permitir_out
  if destination in permitidas_salida then
    done
  else
    drop
  endif
end-policy
!
router bgp 65000
neighbor 10.114.1.1
  address-family ipv4 unicast
   route-policy permitir_out out
!
!
```

En las configuraciones mostradas se crea un prefix-set llamado permitidas_salida, éste es un criterio de coincidencia con las redes 10.30.36.0/23, 10.50.0.0/16 y con el rango 192.168.0.0/16 a 192.168.255.152/30. Se lo utiliza en la política permitir_out como criterio de coincidencia para los prefijos que se permiten enviar a R5.

En la figura 4.34, se observan los prefijos de las redes directamente conectados, los prefijos aprendidos de R6 y los prefijos aprendidos de R2 filtrados por la política permitir_out, lo que se comprueba al compararla con la figura 4.29 que contiene la tabla antes de aplicar la política.

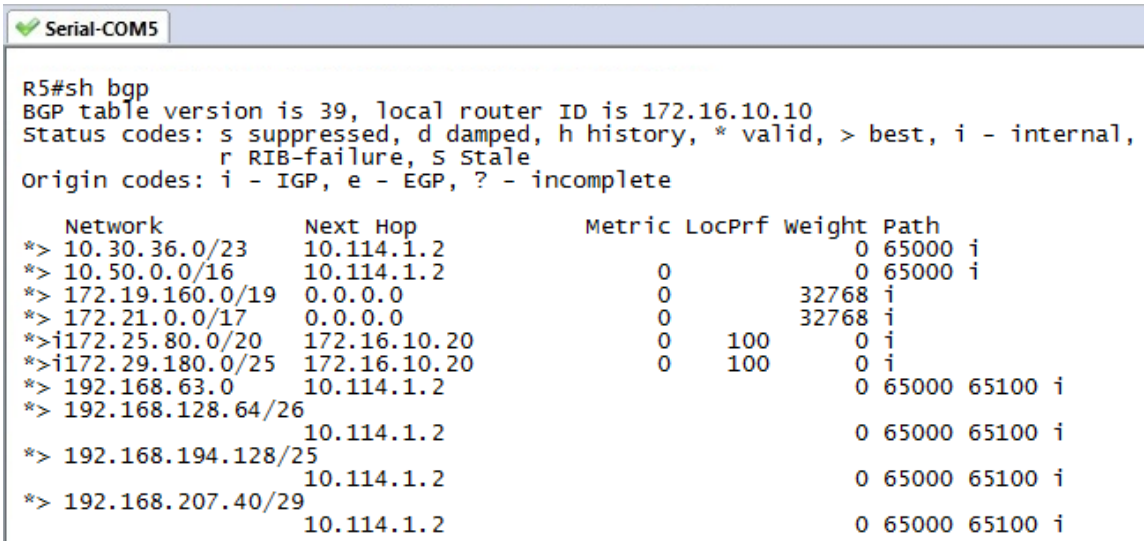


Figura 4.34: Tabla de enrutamiento de R5 después de aplicar la política.

4.2.2 SEGUNDO ESCENARIO

Para crear el segundo escenario se realizaron cambios a la topología del primer escenario, aumentando dos enlaces uno entre R3 con R2 y otro entre R1 con R5, se mantienen la configuraciones iniciales, y se aumentan sesiones EBGP en estos enlaces. Las pruebas para observar el adecuado funcionamiento inicial se centrarán en observar que las nuevas sesiones EBGP se establezcan de manera adecuada.

En la figura 4.35 se observa las tres sesiones BGP establecidas por R1, estas son: una sesión IBGP con R2 y dos sesiones EBGP una con R3 y la nueva sesión

que se establece con R5; con esto se comprueba que la sesión BGP se estableció con éxito en el nuevo enlace entre R1 y R5.

Serial-COM5

```
R1#sh ip bgp summary
BGP router identifier 10.10.10.10, local AS number 65000
BGP table version is 93, main routing table version 93
12 network entries using 1404 bytes of memory
20 path entries using 1040 bytes of memory
11/6 BGP path/bestpath attribute entries using 1760 bytes of memory
2 BGP AS-PATH entries using 48 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 4252 total bytes of memory
BGP activity 24/12 prefixes, 59/39 paths, scan interval 60 secs

Neighbor        V           AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
10.10.10.20     4        65000     177     157       93    0    0 00:42:43        10
10.87.2.1       4        65100     158     158       93    0    0 00:18:34         4
10.114.1.6      4        65200      23      24       93    0    0 00:07:34         4
```

Figura 4.35: Sesiones BGP en R1

En la figura 4.36 se muestra que R2 establece tres sesiones BGP una IBGP con R1 y dos EBGP una con R5 y la nueva con R3; con esto se comprueba que las sesiones en el nuevo enlace se establecieron con éxito.

Serial-COM5

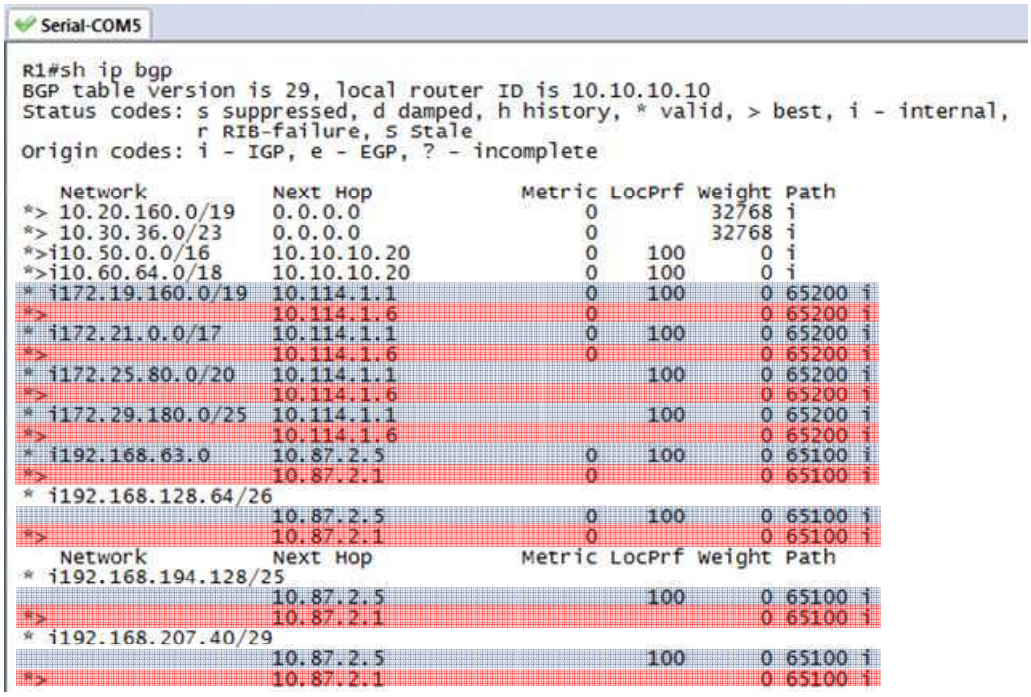
```
RP/0/9/CPU0:R2#sh bgp summary
Fri Jun 17 08:45:05.936 UTC
BGP router identifier 10.10.10.20, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000
BGP main routing table version 125
BGP scan interval 60 secs

BGP is operating in STANDALONE mode.


Process       RcvTblVer   bRIB/RIB   LabelVer  ImportVer  SendTblVer  StandbyVer
Speaker             125        125        125        125         125         125

Neighbor        Spk    AS MsgRcvd MsgSent   TblVer  InQ OutQ  Up/Down  St/PfxRcd
10.10.10.10       0 65000     155     175      125    0    0 00:40:19         10
10.87.2.5         0 65100      24      21      125    0    0 00:03:06          4
10.114.1.1        0 65200     164     182      125    0    0 00:40:19          4
```

Figura 4.36: Sesiones BGP en R2

Antes de cambiar los valores del atributo MED, y mostrar cómo se realiza el balanceo de carga es necesario mostrar las tablas de enrutamiento de R1, R2, R3 y R5 antes de aplicar los cambios, las figuras 4.37, 4.38, 4.39 y 4.40 muestran las tablas de enrutamiento antes de realizar el balanceo de carga.

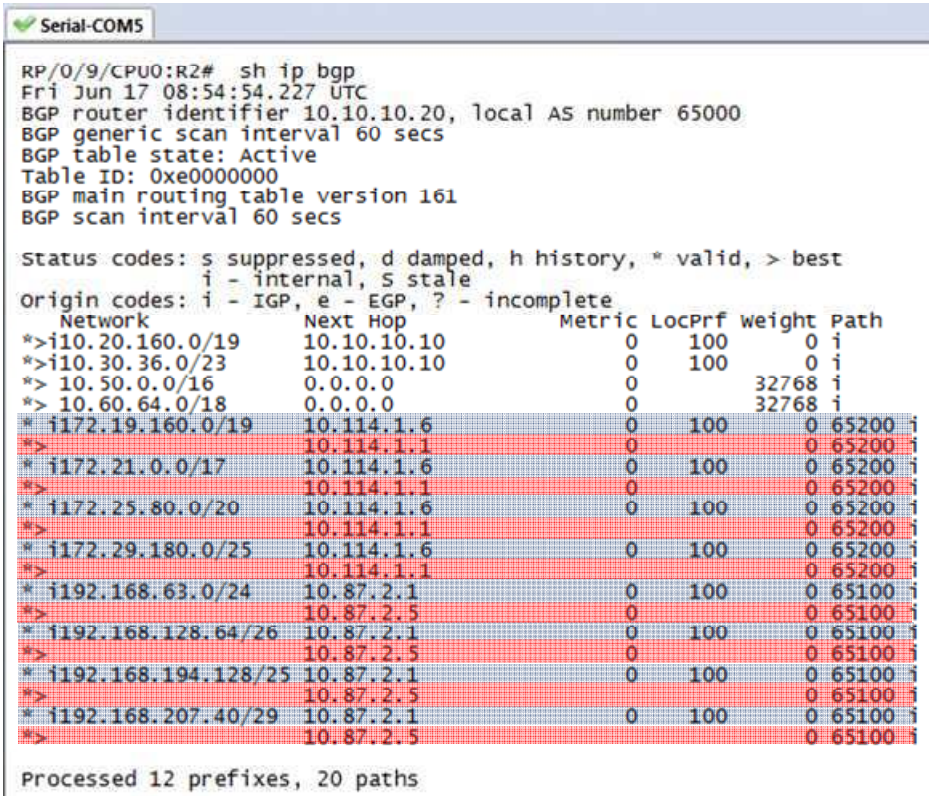
En la figura 4.37 se observa que para las redes 172.0.0.0 y 192.168.0.0 el proceso BGP no escoge como mejor camino a R2 cuyo *next hop* es 10.114.1.1 y 10.87.2.5 (señalado en azul). Para las redes 172.0.0.0 escoge a R5 con *next hop*

10.114.1.6 y para las redes 192.168.0.0 a R3 con *next hop* 10.87.2.1 (señalado en rojo), esta selección se realiza debido a que en el proceso de decisión BGP prefiere las rutas aprendidas por EBGP sobre las rutas aprendidas por IBGP.



```
Serial-COM5

R1#sh ip bgp
BGP table version is 29, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.20.160.0/19   0.0.0.0                  0         32768 i
*> 10.30.36.0/23    0.0.0.0                  0         32768 i
*>i10.50.0.0/16     10.10.10.20              0    100      0 i
*>i10.60.64.0/18    10.10.10.20              0    100      0 i
* i172.19.160.0/19  10.114.1.1              0    100      0 65200 i
*>                  10.114.1.6              0             0 65200 i
* i172.21.0.0/17    10.114.1.1              0    100      0 65200 i
*>                  10.114.1.6              0             0 65200 i
* i172.25.80.0/20   10.114.1.1                   100      0 65200 i
*>                  10.114.1.6                            0 65200 i
* i172.29.180.0/25  10.114.1.1                   100      0 65200 i
*>                  10.114.1.6                            0 65200 i
* i192.168.63.0     10.87.2.5                0    100      0 65100 i
*>                  10.87.2.1                0             0 65100 i
* i192.168.128.64/26
                    10.87.2.5                0    100      0 65100 i
*>                  10.87.2.1                0             0 65100 i
   Network          Next Hop            Metric LocPrf Weight Path
* i192.168.194.128/25
                    10.87.2.5                      100      0 65100 i
*>                  10.87.2.1                               0 65100 i
* i192.168.207.40/29
                    10.87.2.5                      100      0 65100 i
*>                  10.87.2.1                               0 65100 i
```

Figura 4.37: Tabla de enrutamiento R1.



```
Serial-COM5

RP/0/9/CPU0:R2#  sh ip bgp
Fri Jun 17 08:54:54.227 UTC
BGP router identifier 10.10.10.20, local AS number 65000
BGP generic scan interval 60 secs
BGP table state: Active
Table ID: 0xe0000000
BGP main routing table version 161
BGP scan interval 60 secs

Status codes: s suppressed, d damped, h history, * valid, > best
              i - internal, S stale
Origin codes: i - IGP, e - EGP, ? - incomplete
   Network          Next Hop            Metric LocPrf Weight Path
*>i10.20.160.0/19   10.10.10.10              0    100      0 i
*>i10.30.36.0/23    10.10.10.10              0    100      0 i
*> 10.50.0.0/16     0.0.0.0                  0         32768 i
*> 10.60.64.0/18    0.0.0.0                  0         32768 i
* i172.19.160.0/19  10.114.1.6              0    100      0 65200 i
*>                  10.114.1.1              0             0 65200 i
* i172.21.0.0/17    10.114.1.6              0    100      0 65200 i
*>                  10.114.1.1              0             0 65200 i
* i172.25.80.0/20   10.114.1.6              0    100      0 65200 i
*>                  10.114.1.1                            0 65200 i
* i172.29.180.0/25  10.114.1.6              0    100      0 65200 i
*>                  10.114.1.1                            0 65200 i
* i192.168.63.0/24  10.87.2.1               0    100      0 65100 i
*>                  10.87.2.5                0             0 65100 i
* i192.168.128.64/26  10.87.2.1             0    100      0 65100 i
*>                  10.87.2.5                0             0 65100 i
* i192.168.194.128/25 10.87.2.1             0    100      0 65100 i
*>                  10.87.2.5                             0 65100 i
* i192.168.207.40/29  10.87.2.1             0    100      0 65100 i
*>                  10.87.2.5                             0 65100 i

Processed 12 prefixes, 20 paths
```

Figura 4.38: Tabla de enrutamiento R2.

En R2 el proceso de decisión BGP no escoge como mejor camino para les redes 172.0.0.0 y 192.168.0.0 a R1 con *next hop* 10.114.1.6 y 10.87.2.1 (señalado en azul), sino que escoge las rutas aprendidas por EBGP, es decir para redes 172.0.0.0 escoge a R5 con *next hop* 10.114.1.1 y para las redes 192.168.0.0 a R3 con *next hop* 10.87.2.5 (señalado en rojo). Esta selección de rutas se observa en la figura 4.38.

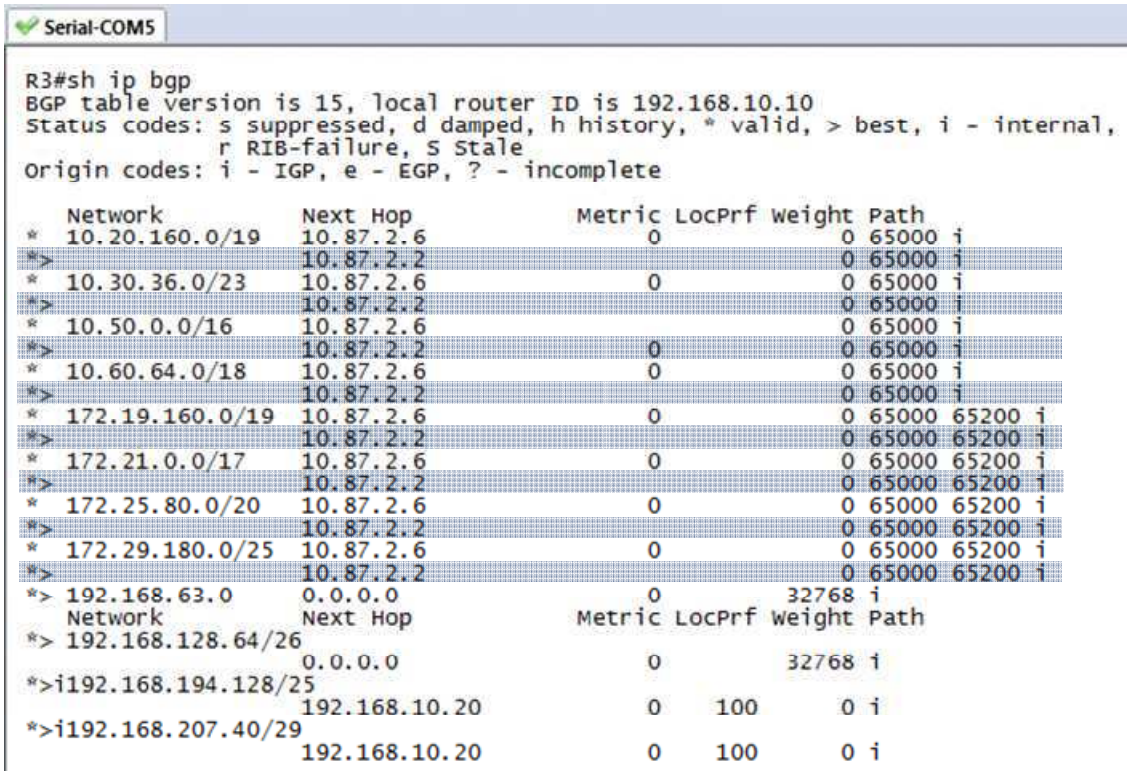


Figura 4.39: Tabla de enrutamiento R3.

En la tabla de enrutamiento BGP de R3 mostrada en la figura 4.39 se observa que para alcanzar las redes 10.0.0.0 y 172.0.0.0, se escoge como mejor camino a R1 con next hop 10.87.2.2. BGP elije esta ruta basándose en el proceso de decisión, el cual prefiere la ruta cuyo parámetro ROUTER_ID sea el más bajo, para el caso de la prueba R1 tiene un ROUTER_ID menor a R2.

En la figura 4.40 se observa la tabla de enrutamiento BGP de R5, donde el mejor camino para las redes 10.0.0.0 y 192.168.0.0 es R1 (10.114.1.5). En la tabla de enrutamiento BGP de R3 y de R5 se puede apreciar que la configuración de dos enlaces no es útil, ya que todo el tráfico se envía por un único enlace, siendo subutilizado el otro enlace.

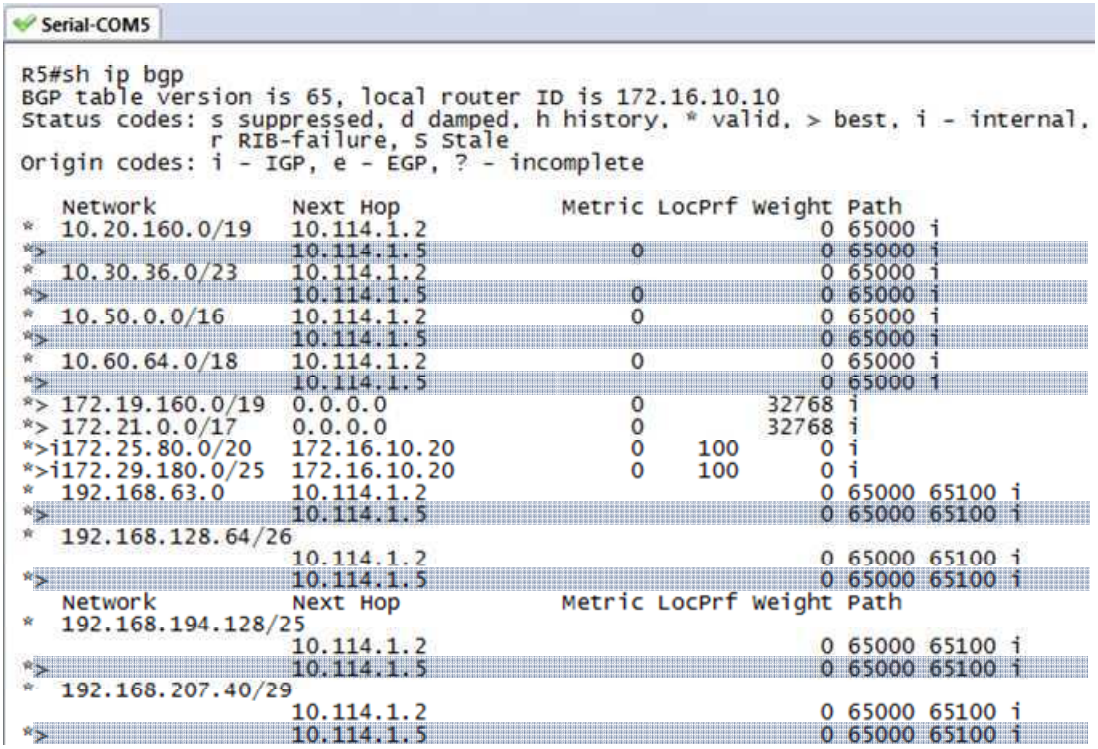


Figura 4.40: Tabla de enrutamiento R5.

Para corregir la subutilización de los enlaces se ve la necesidad de hacer balanceo de carga, las configuraciones que permiten realizar el balanceo mediante el cambio del valor del atributo MED se muestran a continuación:

En R1 se realiza las siguientes configuraciones:

```
!
! Listas de acceso que seleccionan las rutas
!
access-list 1 permit 172.21.0.0 0.0.127.255
access-list 1 permit 172.19.160.0 0.0.31.255
access-list 2 permit 172.25.80.0 0.0.15.255
access-list 2 permit 172.29.180.0 0.0.0.127
!
! Mapa de ruta que coloca el valor de 200 en el atributo MED de
! las rutas que coinciden con la lista de acceso 1 y 100 en las
! que coinciden con la lista de acceso 2
!
route-map salida_R1_al_R3 permit 10
 match ip address 1
 set metric 200
!
route-map salida_R1_al_R3 permit 20
 match ip address 2
 set metric 100
!
route-map salida_R1_al_R3 permit 30
!
```

```
route-map entrada_R1_del_R5 permit 10
 match ip address 1
 set metric 200
!
route-map entrada_R1_del_R5 permit 20
 match ip address 2
 set metric 100
!
route-map entrada_R1_del_R5 permit 30
!
! Asociación de las políticas a un vecino
!
router bgp 65000
 neighbor 10.87.2.1 route-map salida_R1_al_R3 out
 neighbor 10.114.1.6 route-map entrada_R1_del_R5 in
!
```

En R2 se realiza las siguientes configuraciones:

```
!
! Especifica un conjunto de prefijos sobre los que se realizara
! una acción
!
prefix-set listaA
  172.21.0.0/17,
  172.19.160.0/19
end-set
!
prefix-set listaB
  172.25.80.0/20,
  172.29.180.0/25
end-set
!
! Routing policy que colocará el valor de 100 en el atributo MED
! de los prefijos especificados en listaA y 200 en los
! especificados por listaB
!
route-policy salida_R2_al_R3
  if destination in listaA then
    set med 100
  elseif destination in listaB then
    set med 200
  else
    pass
  endif
end-policy
!
route-policy entrada_R2_del_R5
  if destination in listaA then
    set med 100
  elseif destination in listaB then
    set med 200
  else
    pass
```

```
  endif
end-policy
!
! Asociación de las políticas a un vecino
!
router bgp 65000
  address-family ipv4 unicast
   route-policy pass-all in
   route-policy salida_R1_al_R3 out
  !
 !
 neighbor 10.114.1.1
   address-family ipv4 unicast
   route-policy entrada_R1_del_R5 in
   route-policy pass-all out
  !
 !
!
```

En R3 se realiza las siguientes configuraciones:

```
!
! Listas de acceso que seleccionan las rutas
!
access-list 1 permit 192.168.63.0 0.0.0.255
access-list 1 permit 192.168.194.128 0.0.0.127
access-list 2 permit 192.168.128.64 0.0.0.63
access-list 2 permit 192.168.207.40 0.0.0.7
!
! Mapa de ruta que coloca el valor de 100 en el atributo MED de
! las rutas que coinciden con la lista de acceso 1 y 200 en las
! que coinciden con la lista de acceso 2
!
route-map salida_R3_al_R2 permit 10
 match ip address 1
 set metric 100
!
route-map salida_R3_al_R2 permit 20
 match ip address 2
 set metric 200
route-map salida_R3_al_R2 permit 30
!
!
! Mapa de ruta que coloca el valor de 200 en el atributo MED de
! las rutas que coinciden con la lista de acceso 1 y 100 en las
! que coinciden con la lista de acceso 2
!
route-map salida_R3_al_R1 permit 10
 match ip address 1
 set metric 200
!
route-map salida_R3_al_R1 permit 20
 match ip address 2
 set metric 100
```

```
!
route-map salida_R3_al_R1 permit 20
!
! Asociación de las políticas a un vecino
!
router bgp 65100
 neighbor 10.87.2.2 route-map salida_R3_al_R1 out
 neighbor 10.87.2.6 route-map salida_R3_al_R2 out
!
```

En R5 se realiza las siguientes configuraciones:

```
!
! Listas de acceso que seleccionan las rutas
!
access-list 1 permit 192.168.63.0 0.0.0.255
access-list 1 permit 192.168.194.128 0.0.0.127
access-list 2 permit 192.168.128.64 0.0.0.63
access-list 2 permit 192.168.207.40 0.0.0.7
!
! Mapa de ruta que coloca el valor de 100 en el atributo MED de
! las rutas que coinciden con la lista de acceso 1 y 200 en las
! que coinciden con la lista de acceso 2
!
route-map entrada_R5_del_R2 permit 10
 match ip address 1
 set metric 100
!
route-map entrada_R5_del_R2 permit 20
 match ip address 2
 set metric 200
!
route-map entrada_R5_del_R2 permit 30
!
!
! Mapa de ruta que coloca el valor de 200 en el atributo MED de
! las rutas que coinciden con la lista de acceso 1 y 100 en las
! que coinciden con la lista de acceso 2
!
route-map entrada_R5_del_R1 permit 10
 match ip address 1
 set metric 200
!
route-map entrada_R5_del_R1 permit 20
 match ip address 2
 set metric 100
!
route-map entrada_R5_del_R1 permit 30
!
! Asociación de las políticas a un vecino
!
router bgp 65200
 neighbor 10.114.1.2 route-map entrada_R5_del_R2 in
 neighbor 10.114.1.5 route-map entrada_R5_del_R1 in
```

Una vez creadas las políticas, se procede a observar los cambios que estas produjeron en la selección del mejor camino, para que estas tengan efecto se procede al reinicio de las sesiones BGP. Las tablas de enrutamiento BGP que se obtuvieron se muestran en las figuras 4.41, 4.42, 4.43 y 4.44, en las que se observa el cambio del valor del atributo MED y la elección de la mejor ruta en base a este parámetro.

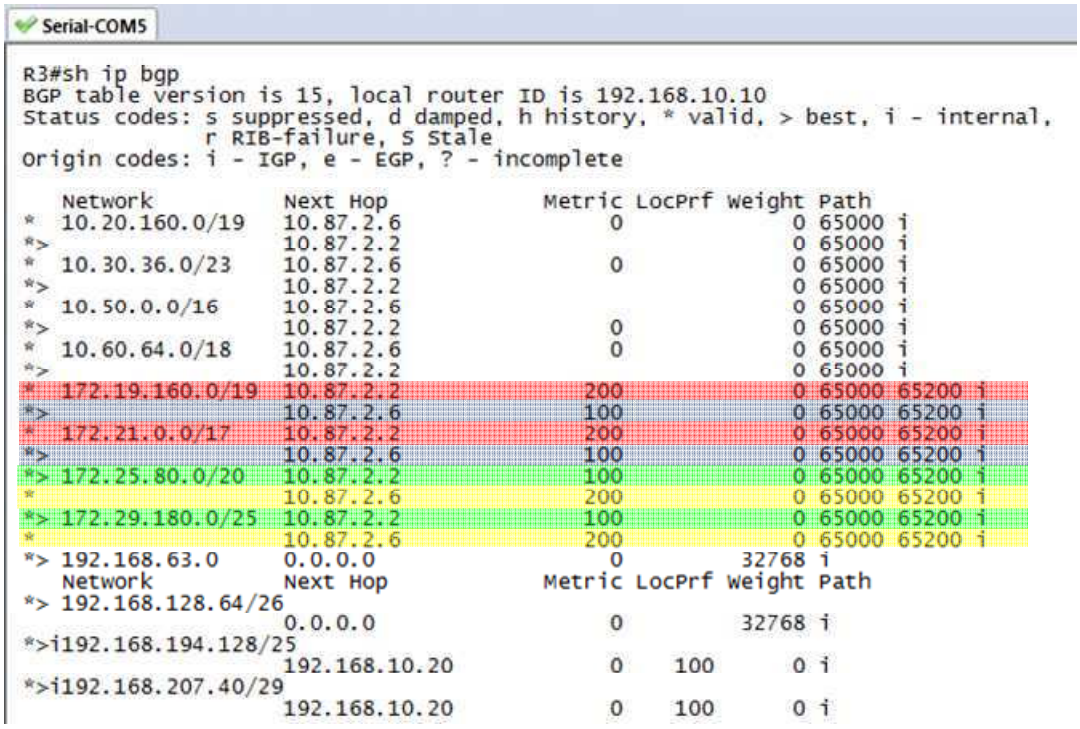


Figura 4.41: Tabla de enrutamiento R3 después de aplicar las políticas.

En la figura 4.41 se puede observar que los paquetes cuyos destinos son las redes 172.19.160.0/19 y 172.21.0.0/17 (señalado en rojo) son enviados a R2 con *next hop* 10.87.2.6, siendo elegido este camino porque el valor del atributo MED es menor para las rutas aprendidas de R2 (señaladas en azul). El cambió de los valores de MED se lo realiza con la política "*salida_R2_al_R3*" configurada en el R2, asignando un valor de 100 para estas rutas y 200 para las rutas 172.25.80.0/20 y 172.29.180.0/25 que publica R2.

De las misma manera para los paquetes que tengan como destino la red 172.25.80.0/20 y 172.29.180.0/25 (señaladas en verde) son enviados a R1 con *next hop* 10.87.2.2, pues tiene el valor MED más bajo para las rutas aprendidas

de R1 (señalado en amarrillo), el cambio de valor del atributo MED para estas rutas se lo realiza con la política “salida_R1_al_R3”.

Con esto se comprueba que se realiza el balanceo de carga en R3, ya que el tráfico cuyo destino sean las redes 172.25.80.0/20 y 172.29.180.0/25 van por el enlace entre R3 y R1, y el tráfico cuyo destino sean las redes 172.19.160.0 /19 y 172.21.0.0/17 va por enlace entre R3 y R2, de esta manera se usa los dos enlaces disponibles.

Al comparar la tabla de enrutamiento mostrada en la figura 4.39 con la tabla mostrada en la figura 4.41 se observa que en esta última la elección de la mejor ruta, se realiza en base al atributo MED de menor valor.

De manera similar en R5 se realiza balanceo de carga para las redes 192.168.0.0, el resultado obtenido al aplicar las políticas se observa en la figura 4.42. En este caso para las redes 192.168.63.0/24 y 192.168.194.128/25 (subrayado en rojo) se elije a R2 con *next hop* 10.114.1.2, ya que las rutas aprendidas de este router tienen una métrica MED menor, el cambio de valor se lo realiza con la política entrada_R5_del_R2 configurada en R5.

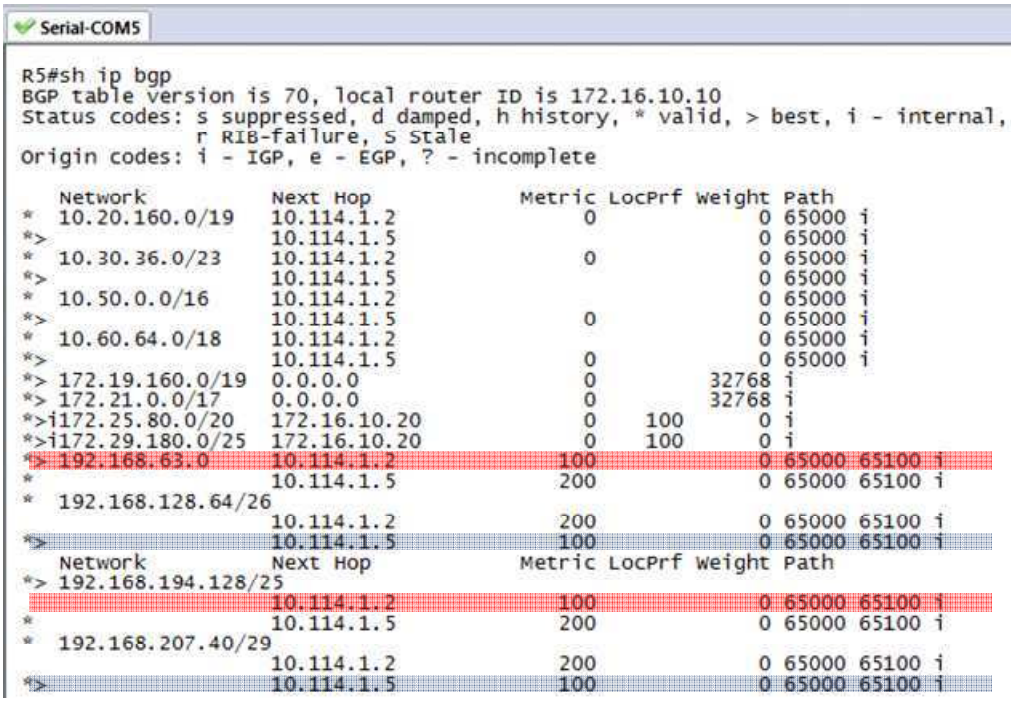


Figura 4.42: Tabla de enrutamiento R5 después de aplicar las políticas.

Las redes 192.168.128.64/26 y 192.168.207.40/29 (señaladas en azul) escogen como dirección de siguiente salto a 10.144.1.5 configurada en R1, ya que las rutas aprendidas de este router tienen el MED más bajo, el cambio del valor se lo realiza con la política “entrada_R5_del_R2” configurada en R5, con esto se realiza balanceo de carga para las redes 192.168.0.0 en R5.

Al comparar la tabla de enrutamiento mostrada en la figura 4.40 con la tabla mostrada en la figura 4.42 se observa que en esta última la elección de la mejor ruta, se realiza en base al atributo MED de menor valor.

Para completar el balanceo de carga es necesario realizarlo en el SA 65000, el resultado obtenido al realizar balanceo de carga en R1 se muestra en la figura 4.43, donde para las redes 172.19.160.0/19 y 172.21.0.0/17 (señaladas en rojo) se tiene como dirección de siguiente salto preferida a R5 (10.114.1.6), se escogen las rutas aprendidas de R5 por tener el atributo MED más bajo que las aprendidas por R2, el cambio de este valor se lo realizó con la política “entrada_R1_del_R5” configurada en R1.

Serial-COM5

```
R1#sh ip bgp
BGP table version is 29, local router ID is 10.10.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
*> 10.20.160.0/19   0.0.0.0                  0         32768 i
*> 10.30.36.0/23    0.0.0.0                  0         32768 i
*>i10.50.0.0/16     10.10.10.20              0    100      0 i
*>i10.60.64.0/18    10.10.10.20              0    100      0 i
*>i172.19.160.0/19  10.114.1.6             100    100      0 65200 i
*                   10.114.1.1             200             0 65200 i
*>i172.21.0.0/17    10.114.1.6             100    100      0 65200 i
*                   10.114.1.1             200             0 65200 i
* i172.25.80.0/20   10.114.1.6             200    100      0 65200 i
*>                  10.114.1.1             100             0 65200 i
* i172.29.180.0/25  10.114.1.6             200    100      0 65200 i
*>                  10.114.1.1             100             0 65200 i
*>i192.168.63.0     10.87.2.5              100    100      0 65100 i
*                   10.87.2.1              200             0 65100 i
*  192.168.128.64/26
                    10.87.2.5              200    100      0 65100 i
*>                  10.87.2.1              100             0 65100 i
*>i192.168.194.128/25
   Network          Next Hop            Metric LocPrf Weight Path
                    10.87.2.5              100    100      0 65100 i
*                   10.87.2.1              200             0 65100 i
*  192.168.207.40/29
                    10.87.2.5              200    100      0 65100 i
*>                  10.87.2.1              100             0 65100 i
```

Figura 4.43: Tabla de enrutamiento R1 después de aplicar las políticas.

Mientras que los paquetes que se tienen que enviar a las redes 172.25.80.0/20 y 172.29.180.0/25 (señalado en azul) se envían primero a R2, a través de este alcanzan a R5, esto se da por que el valor MED aprendido de R2 es menor que el aprendido de R5, el cambio del valor se lo realiza con la política “entrada_R2_del_R5” aplicada en el R2.

Con esto se comprueba que el atributo MED se envía en las actualizaciones IBGP; ya que tiene significado dentro del SA. A pesar que la ruta hacia 172.25.80.0/20 y 172.29.180.0/25 con menor número de saltos seria a través de R3 no se la utiliza ya que el objetivo es utilizar el enlace existente entre R2 y R3.

Para los paquetes dirigidos a las redes 192.168.63.0/24 y 192.168.194.128/25, primero se envían a R2, a través de esta alcanzarán a R3. Se escogen las rutas aprendidas de R2 por tener una métrica MED menor, para alterar este valor se usó la política “salida_R3_al_R1”, configurada en R3.

Para alcanzar las redes 192.168.128.64/26 y 192.168.207.40/29 los paquetes se enviarán directamente a R3 pues el atributo MED es menor para este camino, el cambio en el valor se lo realiza con la política “salida_R3_al_R2” configurada en R1.

Al comparar la tabla de enrutamiento mostrada en la figura 4.37 con la tabla mostrada en la figura 4.43 se observa que en esta última la elección de la mejor ruta, se realiza en base al atributo MED de menor valor.

En la tabla de enrutamiento de R2 mostrada en la figura 4.44 se observa un resultado similar al obtenido en R1, la diferencia está en el camino por el que se envían los paquetes a su destino esto es: para alcanzar las redes 172.19.160.0 /19 y 172.21.0.0/17 se la enviará a R1, a través de este alcanzarán a R5; en cambio para las redes 172.25.80.0/20 y 172.29.180.0/25 los paquetes se enviarán directamente a R5

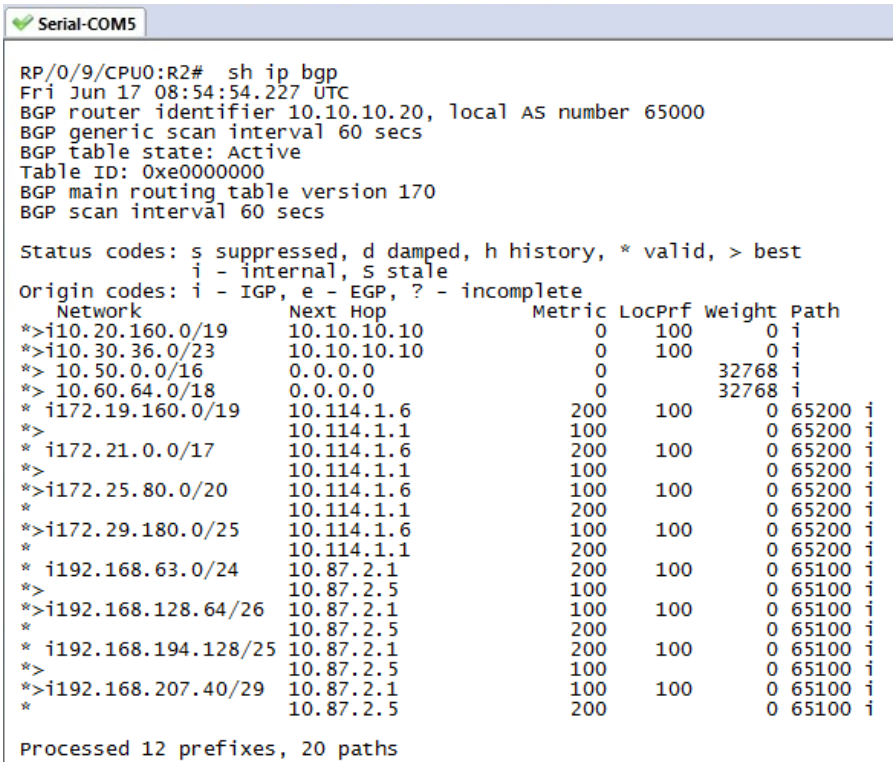


Figura 4.44: Tabla de enrutamiento de R2 después de aplicar las políticas.

En las redes clase C el envío en R2 se lo realizará así: para llegar a las redes 192.168.63.0/24 y 192.168.194.128/25 los paquetes se envían directamente a R3; en cambio para las redes 192.168.128.64/26 y 192.168.207.40/29, el camino para alcanzar el destino es a través de R1.

Al comparar la tabla de enrutamiento mostrada en la figura 4.38 con la tabla mostrada en la figura 4.44 se observa que en esta última la elección de la mejor ruta, se realiza en base al atributo MED de menor valor.

En el escenario se muestran dos formas de realizar balanceo de carga, la primera se la utiliza para las redes 172.0.0.0, en este caso todas las políticas se configuran y aplican en el SA 65000, se utilizan políticas de entrada que modifican los atributos MED en las rutas que ingresan al SA, y políticas de salida que modifican los atributos MED en las rutas que se envían a los SA vecinos, de esta manera se altera las rutas que selecciona BGP.

Los caminos que se crearon con las dos políticas son: para alcanzar 172.19.160.0 /19 y 172.21.0.0/17 desde el SA 65100 se lo hace a través del R2, para alcanzar 172.25.80.0/20 y 172.29.180.0/25 se lo realiza a través de R1.

Una segunda opción se la utilizó para las rutas 192.168.0.0, en este caso las configuraciones se realizan en el SA 65100 y SA 65200; en el SA 65100 que publica las redes 192.168.0.0, se la configura como políticas de salida que alteran los valores del atributo MED, de esta manera se influye sobre la decisión de que ruta prefiere el SA 65000.

En el SA 65200 se configuran políticas de entrada, que afectan a las rutas aprendidas desde del SA 65000, de esta manera se cambia los enlaces por los que se envían los paquetes. Los caminos para alcanzar el SA 65100 desde el SA 65200 son: para los paquetes que tengan como destino las redes 192.168.63.0/24 y 192.168.194.128/25 se los envía por R2 y para los paquetes que se envían a 192.168.128.64/26 y 192.168.207.40/29 por R1.

4.3 PRUEBAS DE VPNS CAPA 2 [6] [23]

4.3.1 PRIMER ESCENARIO

Para realizar las pruebas de las VPNs capa dos se parte de las configuraciones iniciales mostradas para la topología base en la que se habilita un backbone MPLS para un proveedor de servicios, por esta razón se omite la comprobación de su adecuado funcionamiento inicial, las pruebas de este se detallan en la primera sección de este capítulo, las configuraciones que permiten crear una VPN capa 2 punto a punto se muestran a continuación:

En UIOLABPE01:

```
interface GigabitEthernet1/3
 description conexion CustomerA a site2
 no ip address
 xconnect 172.30.10.40 1234 encapsulation mpls
 no shutdown
```

En UIOLABPE02

```
interface GigabitEthernet1/3
 description conexion CustomerA a site1
 no ip address
 xconnect 172.30.10.10 1234 encapsulation mpls
 no shutdown
```

Las configuraciones mostradas anteriormente crean un túnel capa 2 entre las interfaces Gi1/3 de UIOLABE01 y Gi1/3 de UIOLABE02, se usa el vcid 1234 y se

define como encapsulación para enviar el tráfico dentro de la red del proveedor de servicios a MPLS, para comprobar su adecuado funcionamiento se usa el comando ***sh mpls l2transport vc 1234 detail,*** el resultado de la salida obtenida al aplicarlo en UIOLABE02 se muestra en la figura 4.45.

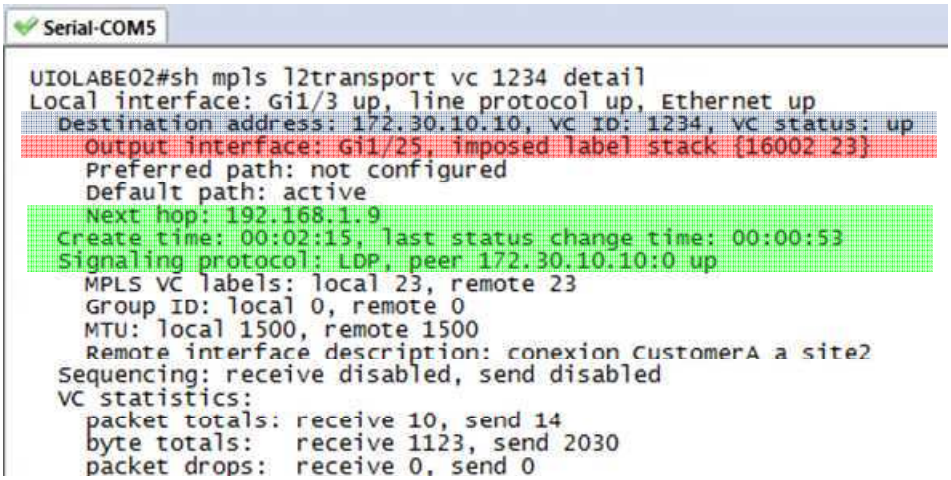


Figura 4.45: Comprobación del funcionamiento de túnel.

En la figura 4.45 se observa el estado de la VPN, los parámetros que se muestran son: la dirección del router remoto que es el destino, en este caso 172.30.10.10; el vcid que es 1234; el estado de la VPN en este caso UP (señalado en azul), este estado indica que el tráfico se puede enviar sin ningún problema; la interfaz de salida que es gi1/25; la pila de etiquetas impuesta (subrayada en rojo), en este caso se tiene la etiqueta 16002 que es la más externa, se la considera como la asignada por el IGP, y permite la conmutación del paquete por el LSP. La etiqueta 23 es la etiqueta mas interna es la última en retirarse, y se utiliza para identificar al túnel capa 2 en ambos PEs; también se muestra la dirección del siguiente salto en este caso 192.168.1.9; el protocolo de señalización de etiquetas es LDP y algunas estadísticas del tráfico del túnel (mostrado en verde).

Una variante del comando mostrado anteriormente es colocar únicamente ***sh mpls l2transport vc 1234,*** este muestra únicamente la interfaz local, el tipo de circuito en este caso Ethernet, la dirección de destino y el estado de la VPN. En la figura 4.46 se observa el resultado de este comando al aplicarlo en los dos PEs, con esto se comprueba que el túnel se encuentra activo y que se puede enviar tráfico extremo a extremo.

```
UIOLABE01#show mpls l2transport vc

Local intf     Local circuit              Dest address    VC ID      Status
-------------  -------------------------- --------------- ---------- ----------
Gi1/3          Ethernet                   172.30.10.40    1234       UP

UIOLABE02#sh mpls l2transport vc 1234

Local intf     Local circuit        Dest address    VC ID      Status
-------------  -------------------- --------------- ---------- ----------
Gi1/3          Ethernet             172.30.10.10    1234       UP
```

Figura 4.46: Estado de la VPN.

Para comprobar que una VPN de capa 2 puede enviar el tráfico del cliente y ofrecer una conexión transparente para el usuario, en la que se tiene la percepción de que no existe una red WAN entre las ubicaciones remotas, sino que existe un enlace LAN se conectaron los routers CE1 y CE2 en los respectivos nodos PEs extremos de la topología. Se configuraron las direcciones de red y el protocolo de enrutamiento OSPF, se observa en las figuras 4.47 y 4.48 el establecimiento de adyacencias e intercambio de rutas respectivamente.

```
CE1#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.1.2         1   FULL/DR         00:00:36    10.10.1.2       FastEthernet0/0

CE2#sh ip ospf neighbor

Neighbor ID     Pri   State           Dead Time   Address         Interface
10.10.1.1         1   FULL/BDR        00:00:39    10.10.1.1       FastEthernet0/0
```

Figura 4.47: Establecimiento de sesiones OSPF.

En la figura 4.47 se observa el establecimiento de las sesiones OSPF entre CE1 y CE2. Las direcciones que identifican a los routers que establecen las adyacencias OSPF son las configuradas en los equipos del cliente, y no se establecen adyacencias con los router intermedios de la red MPLS, comprobándose que la existencia de red del proveedor de servicios es transparente para los equipos del cliente.

Los parámetros observados son: el router ID del vecino, la prioridad del router designado, el estado OSPF en este caso FULL, indica total establecimiento de la adyacencia; el tiempo que debe trascurrir antes de declarar a un vecino muerto (dead time); la dirección de siguiente salto y el nombre de la interfaz por la que se formó la adyacencia.

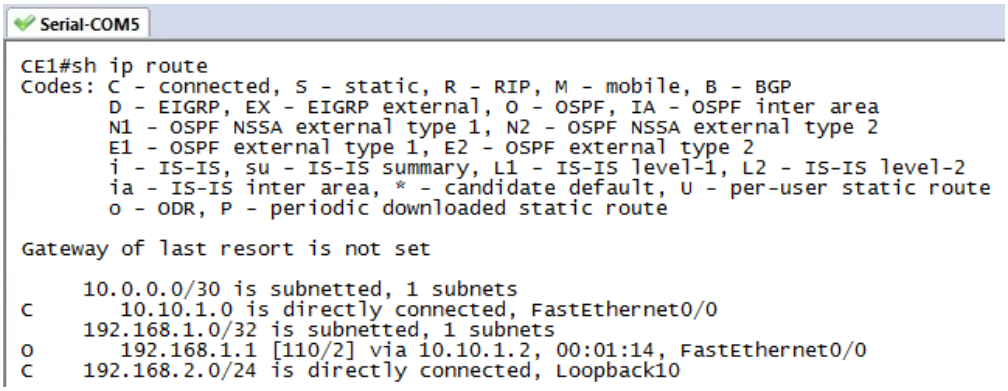


Figura 4.48: Tabla de enrutamiento de CE1.

En la figura 4.48 se muestra la tabla de enrutamiento de CE1. Se observa que todas las redes configuradas en CE1 y CE2 se encuentran en la tabla, por lo que se concluye que todas las redes se han intercambiado y aprendido mediante OSPF, asegurado que el cliente tendrá una conectividad total entre sus localidades.

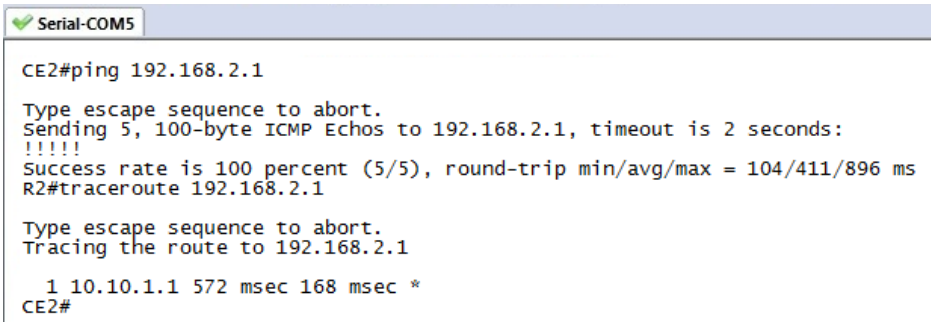


Figura 4.49: Pruebas de ping y tracert.

El la figura 4.49 se observa que al realizar un ping se puede alcanzar la red del otro extremo del cliente comprobándose la conectividad. También se muestra un traceroute en el que se observa que entre los routers CEs solo se tiene un salto por lo que se tiene la sensación de que la red WAN de proveedor de servicios no existe.

4.3.2 SEGUNDO ESCENARIO

Para el segundo escenario se cambia la topología por lo que es necesario comprobar que las configuraciones iniciales de MPLS, LDP e IS-IS se hayan realizado de manera adecuada, las configuraciones finales se adjuntan en los anexos. La comprobación del funcionamiento se muestra a continuación:

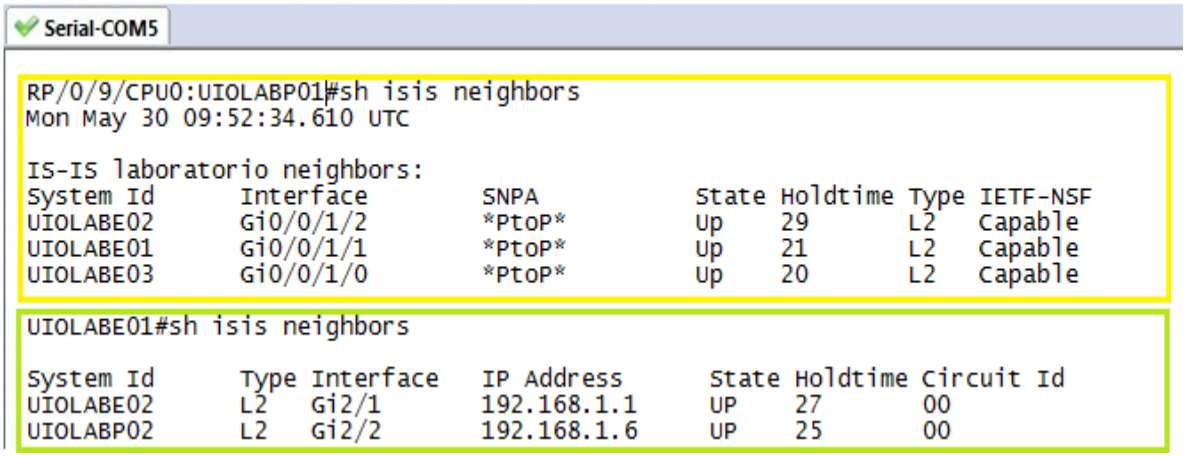


Figura 4.50: Adyacencias IS-IS del segundo escenario.

En la figura 4.50 se muestran todas las adyacencias IS-IS establecidas en la topología. Para UIOLABP01 (en amarillo) se establecieron sesiones con UIOLABE01, UIOLABE02 y UIOLABE03. El UIOLABE01 (en verde) establece una sesión adicional con UIOLABE02, todas las adyacencias tienen como estado UP por lo que se encuentran activas, comprobándose el adecuado funcionamiento de IS-IS.

En la figura 4.51 se muestra la tabla de enrutamiento de UIOLABP01, se observa que se tiene un entrada para cada una de las redes configuradas en la topología, se tiene conocimiento de las redes de los todos enlaces, y de la loopback 100 de cada router en la red, con esto se comprueba que se tiene una ruta para alcanzar cualquier destino en la red mostrando que IS-IS converge.

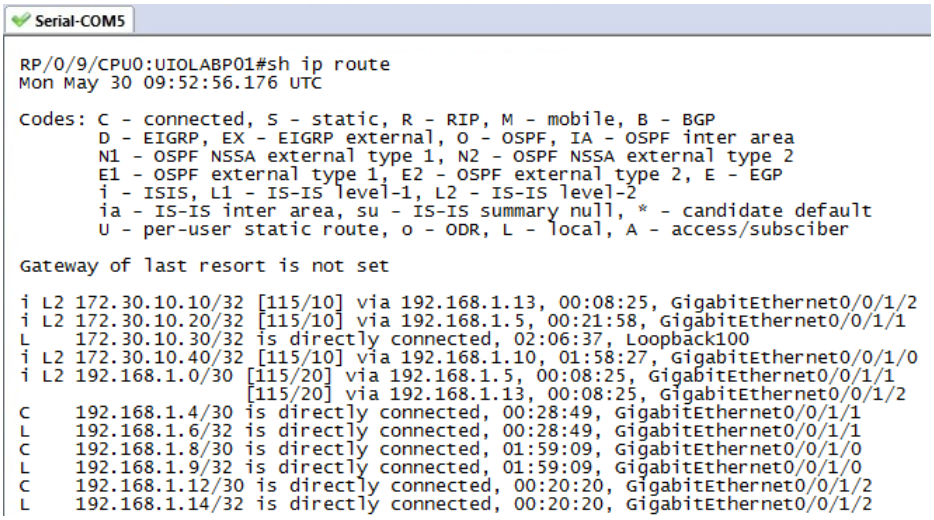


Figura 4.51: Tabla de enrutamiento de UIOLABP01.

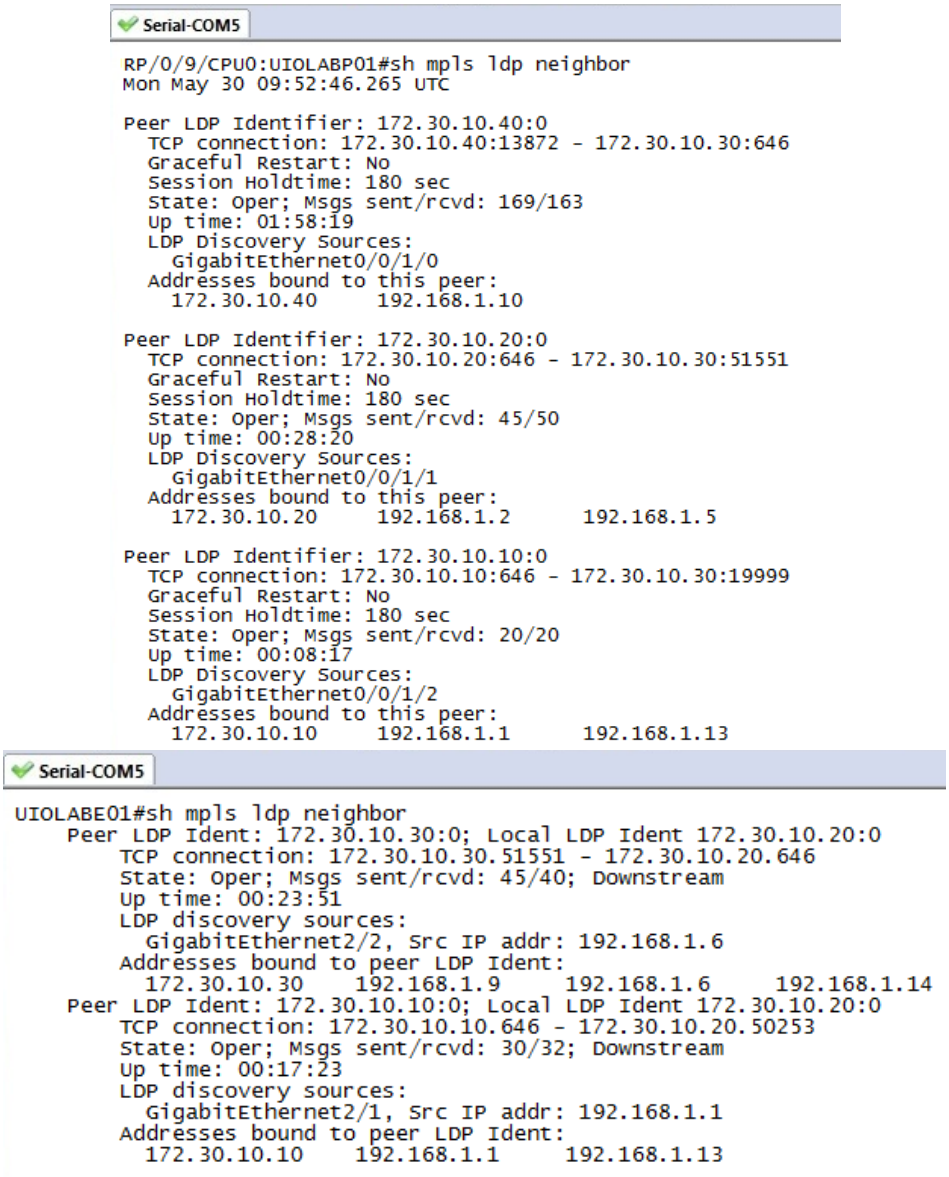


Figura 4.52: Sesiones LDP.

En la figura 4.52 se comprueba el adecuado funcionamiento de LDP pues se observan que UIOLABP01 (mostrado en la primera parte) ha establecido sesiones con UIOLABE01, UIOLABE02 y UIOLABE03. UIOLABE01 (mostrado en la segunda parte) también establece una sesión adicional con UIOLABE02, con esto se comprueba que los routers establecen sesiones LDP con todos sus vecinos, permitiendo realizar el intercambio de etiquetas, necesario para establecer la conmutación MPLS dentro de la red.

Una vez que se comprueba el adecuado funcionamiento de las configuraciones básicas de la red se procede a configurar los túneles necesarios para crear una

estructura HUB and SPOKE, para de esta manera ofrecer conectividad entre las tres ubicaciones remotas del cliente; las configuraciones realizadas son:

EN UIOLABE01

```
interface GigabitEthernet9/1
 no ip address
 xconnect 172.30.10.10 1000 encapsulation mpls
!
```

EN UIOLABE02

```
interface GigabitEthernet1/1.1000
 encapsulation dot1Q 1000
 xconnect 172.30.10.20 1000 encapsulation mpls
!
interface GigabitEthernet1/1.2000
 encapsulation dot1Q 2000
 xconnect 172.30.10.40 2000 encapsulation mpls
!
```

EN UIOLABE03

```
interface GigabitEthernet1/1
 no ip address
 xconnect 172.30.10.10 2000 encapsulation mpls
!
```

Las configuraciones mostradas crean dos VPNs capa 2, una entre UIOLABE02 y UIOLABE01 y otra en entre UIOLABE03 y UIOLABE01, el tráfico que se genera en los routers spoke no necesita ningún encapsulamiento adicional, mientras que al generado por el HUB se le añade un etiqueta VLAN, para distinguir el tráfico que pertenece al túnel 1000, del que pertenece al túnel 2000; los equipos del proveedor de servicios se encargan de realizar la traducción entre el tráfico etiquetado y el no etiquetado.

Por ejemplo un paquete originado en CE1 se etiquetará con la VLAN 2000, esto indicará a UIOLABE02 que el paquete debe ser enviado por túnel 2000 hacia el UIOLABE03, en donde este envía el tráfico a CE3 sin asociar ninguna etiqueta a los paquetes. En la dirección contraria en cambio CE3 envía los paquetes a UIOLABE03 sin etiquetar, como existe un único túnel en la interfaz, el tráfico se

envía UIOLABE02, en donde se lo etiqueta con la VLAN 2000 y se lo envía a CE1, la etiqueta permite distinguir que el flujo viene de CE3.

A continuación, se comprobará si los procesos OSPF configurados en las tres localidades establecen adyacencias e intercambian rutas entre ellos, las configuraciones de las localidades de los clientes son:

En CE1:

```
interface Loopback10
 ip address 192.168.10.1 255.255.255.0
 ip ospf network point-to-point
!
interface FastEthernet0/0
 ip address 192.168.1.6 255.255.255.252
 ip ospf network point-to-point
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.4 0.0.0.3 area 0
 network 192.168.10.0 0.0.0.255 area 0
!
```

En CE2:

```
interface Loopback100
 ip address 192.168.30.1 255.255.255.0
 ip ospf network point-to-point
!
interface GigabitEthernet1/1.1000
 encapsulation dot1Q 1000
 ip address 192.168.1.5 255.255.255.252
 ip ospf network point-to-point
!
interface GigabitEthernet1/1.2000
 encapsulation dot1Q 2000
 ip address 192.168.1.1 255.255.255.252
 ip ospf network point-to-point
!
router ospf 1
 log-adjacency-changes
 passive-interface Loopback100
 network 192.168.1.0 0.0.0.3 area 0
 network 192.168.1.4 0.0.0.3 area 0
 network 192.168.30.0 0.0.0.255 area 0
!
```

En CE3

```
interface Loopback30
 ip address 192.168.20.1 255.255.255.0
 ip ospf network point-to-point
!
interface FastEthernet0/0
 ip address 192.168.1.2 255.255.255.252
 ip ospf network point-to-point
 duplex auto
 speed auto
!
router ospf 1
 log-adjacency-changes
 network 192.168.1.0 0.0.0.3 area 0
 network 192.168.20.0 0.0.0.255 area 0
!
```

Las configuraciones anteriores habilitan el proceso OSPF y el intercambio de rutas entre las tres localidades de los clientes, se crea una dirección de loopback para simular una red LAN conectada a cada router y se procede a verificar su correcto funcionamiento:

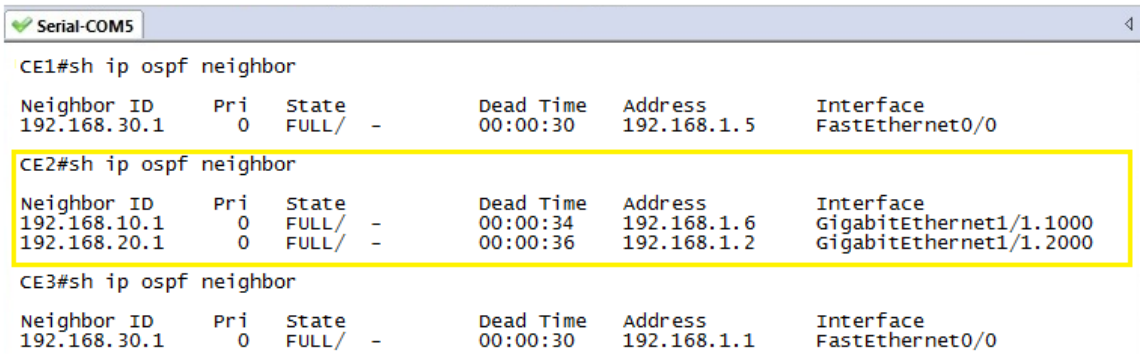


Figura 4.53: Establecimiento de adyacencia OSPF

En la figura 4.53 se observa que se establecieron adyacencias OSPF entre CE1 con CE2 y CE3 con CE2, todas están en estado full, las adyacencias muestran únicamente las direcciones asignadas por el cliente, la existencia de la red MPLS es transparente, también se demuestra que las subinterfaces tienen las mismas características que una interfaz física, ya que por estas se puede establecer adyacencias OSPF sin ningún problema, finalmente se nota que las etiquetas VLANs añadidas para identificar los flujos de tráfico cumplen con el objetivo de identificar el tráfico entre CE2 y PE2, pues no afectan el correcto funcionamiento de OSPF.

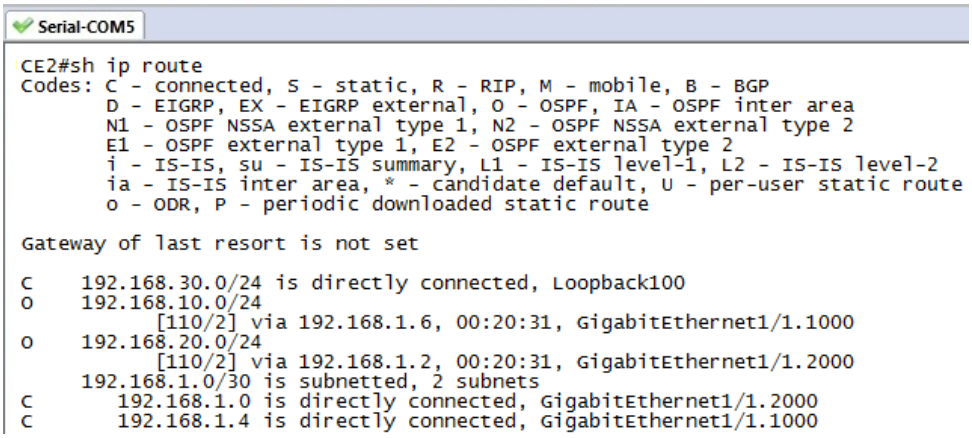


Figura 4.54: Tabla de enrutamiento de CE2.

En la figura 4.54 se muestra la tabla de enrutamiento de CE2, donde se observa que se tienen entradas para cada una de las redes configuradas en las localidades del cliente, con esto se demuestra el adecuado intercambio de las rutas entre los diferentes routers que componen la red del cliente.

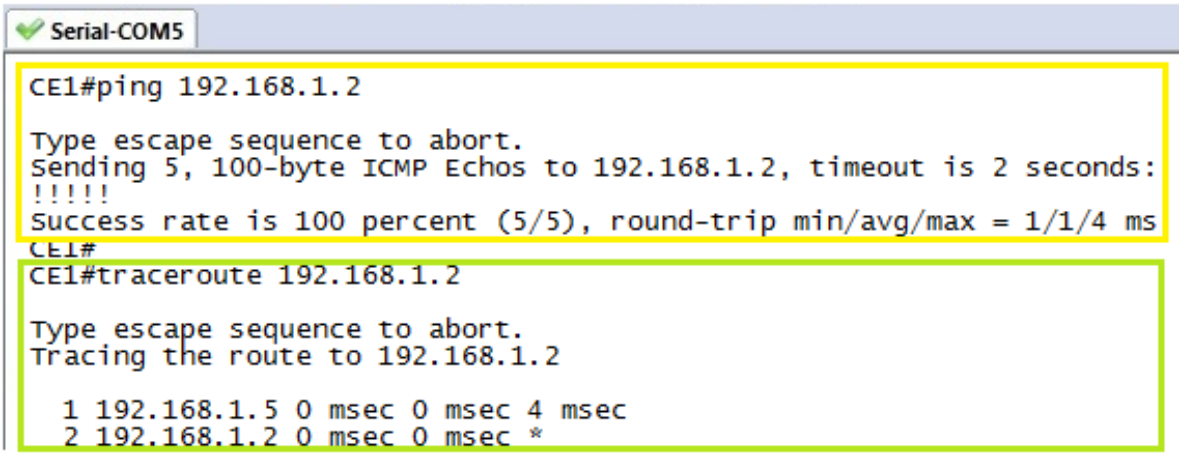


Figura 4.55: Comandos ping y tracert en CE1.

Para la figura 4.55 con el comando ping (mostrado en amarillo) se comprueba que el cliente tiene conectividad total entre sus LANs, con tracert (mostrado en verde) se muestra que para alcanzar las redes de CE2 desde CE1 es necesario que el tráfico pase primero por CE3 (192.168.1.5), comprobándose que es una topología HUB and SPOKE, al observar que solo se tiene como saltos los routers del cliente, nuevamente se observa la transparencia de la red del proveedor de servicios.

4.4 PRUEBAS DE VPN CAPA 3 "VRF" [32] [33][36] [37]

Una vez que el backbone MPLS se encuentra configurado y probado su funcionamiento, para realizar la prueba de las VPN capa 3 se crearon dos instancias VRF para dos clientes, la configuración se muestra a continuación.

Configuración PE1 "UIOLABE01"

```
ip vrf customerA
rd 1:500
route-target export 1:500
route-target import 1:100
!
ip vrf customerB
rd 1:600
route-target export 1:600
route-target import 1:200
```

Configuración PE2 "UIOLABE02"

```
ip vrf customerA
 rd 1:100
 route-target export 1:100
 route-target import 1:500
!
ip vrf customerB
 rd 1:200
 route-target export 1:200
 route-target import 1:600
```

Los siguientes comandos permiten verificar el funcionamiento de las configuraciones realizadas para las VPN *Routing and Forwarding* "VRF" establecidas en los routers de frontera.

El comando ***show ip vrf*** muestra el conjunto de instancias VRF configuradas, sus correspondientes *route-distinguishers* (RD) y las interfaces asociadas a dichas instancias.

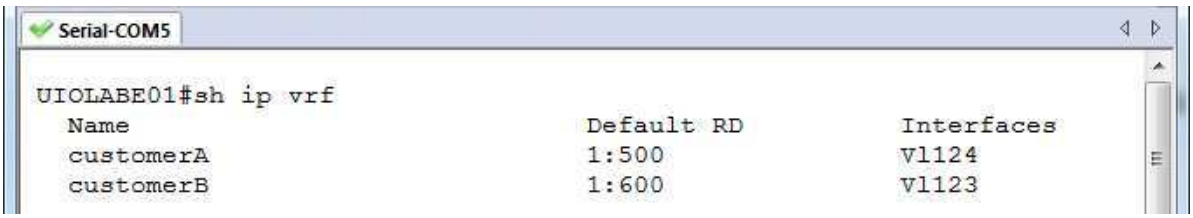


Figura 4.56: Salida del comando "show ip vrf"

En el ejemplo de la figura 4.56 se puede observar que en el router UIOLABE01, se encuentran configuradas dos instancias VRF "customerA y customerB", con un *route-distinguisher* "1:500 y 1:600" respectivamente, además se informa que cada instancia está asociada a una interfaz vlan 124 y 123 respectivamente.

Esta misma información puede ser ampliada con la ayuda del comando ***show ip vrf detail***

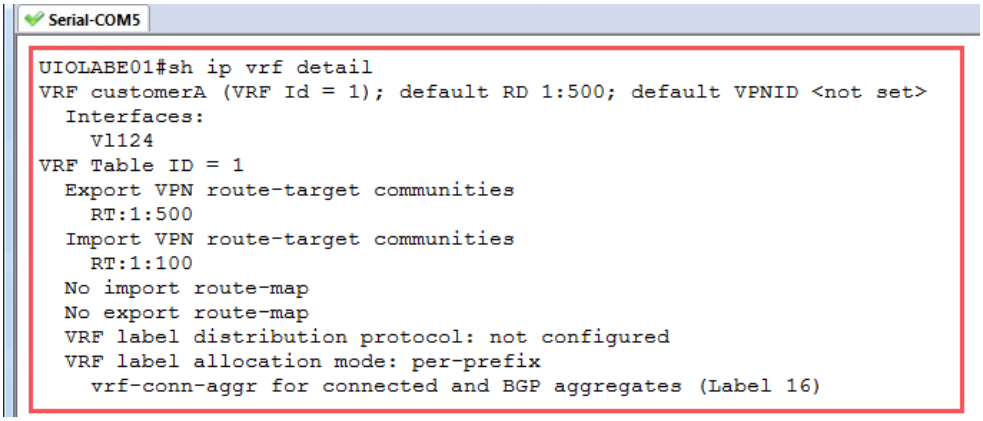


Figura 4.57: Salida del comando "show ip vrf detail"

En la figura 4.57 se verifica los atributos de enrutamiento individual para cada VRF, las tablas de enrutamiento que se importan o exportan, por ejemplo para la VRF CustomerA, además del RD 1:500, el comando proporciona información de las rutas que se exportarán e importarán por MP-BGP para un cliente en especifico.

Para la VRF CustomerA, las rutas a ser exportadas, son aquellos prefijos configurados en la localidad del cliente, a los que se les añade el atributo *Route Target* de exportación 1:500. Al momento de convertirse en un prefijo VPNv4, dentro de las comunidades extendidas de BGP, usa el valor del *route target* como un atributo en sus actualizaciones, este permite que el prefijo sea reconocido en los sitios remotos, donde se lo requiere importar.En cambio para la importación de rutas en la VRF CustomerA, se buscará la coincidencia del atributo de los prefijos VPNv4, con el route target de importación 1:100, y todas aquellas coincidencias serán instaladas dentro de la tabla de la VRF.

El comando ***show ip vrf interfaces*** muestra las asociaciones entre interfaces e instancias VRF configuradas en el router, adicionalmente muestra el estatus y la dirección IP configurada para la misma, las cuales no son parte de la tabla de enrutamiento global.

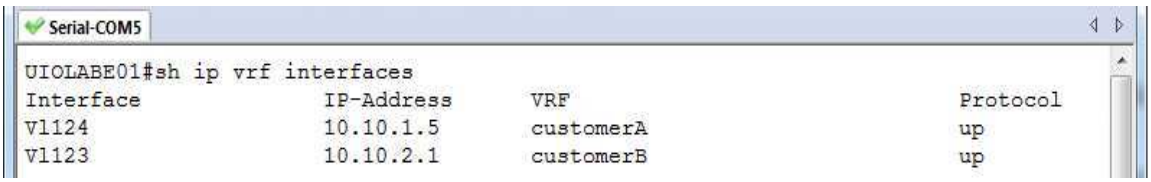


Figura 4.58: Salida del comando "show ip vrf interfaces"

En este caso se observa en la figura 4.58 las dos VRFs customerA y customerB configuradas en el Router “UIOLABE01” están asociadas cada una a una interfaz vlan “124 y 123” respectivamente, las dos se encuentran operativas (UP) y sus IP configuradas en cada interfaz, no forman parte de las tablas de enrutamiento global, sino de cada una de las tablas de enrutamiento propias de cada una de las VRFs.

Los siguientes comandos permiten realizar una verificación de enrutamiento, tanto a nivel de PE-PE como entre CE-PE, revisando las tablas de enrutamiento o bases de datos de los protocolos de enrutamiento. Donde a nivel de enrutamiento entre PE-PE, el comando ***sh ip route vrf [****vrf-name****]*** permite verificar el estado de las tablas de enrutamiento independientes para cada una de las instancias VRF.

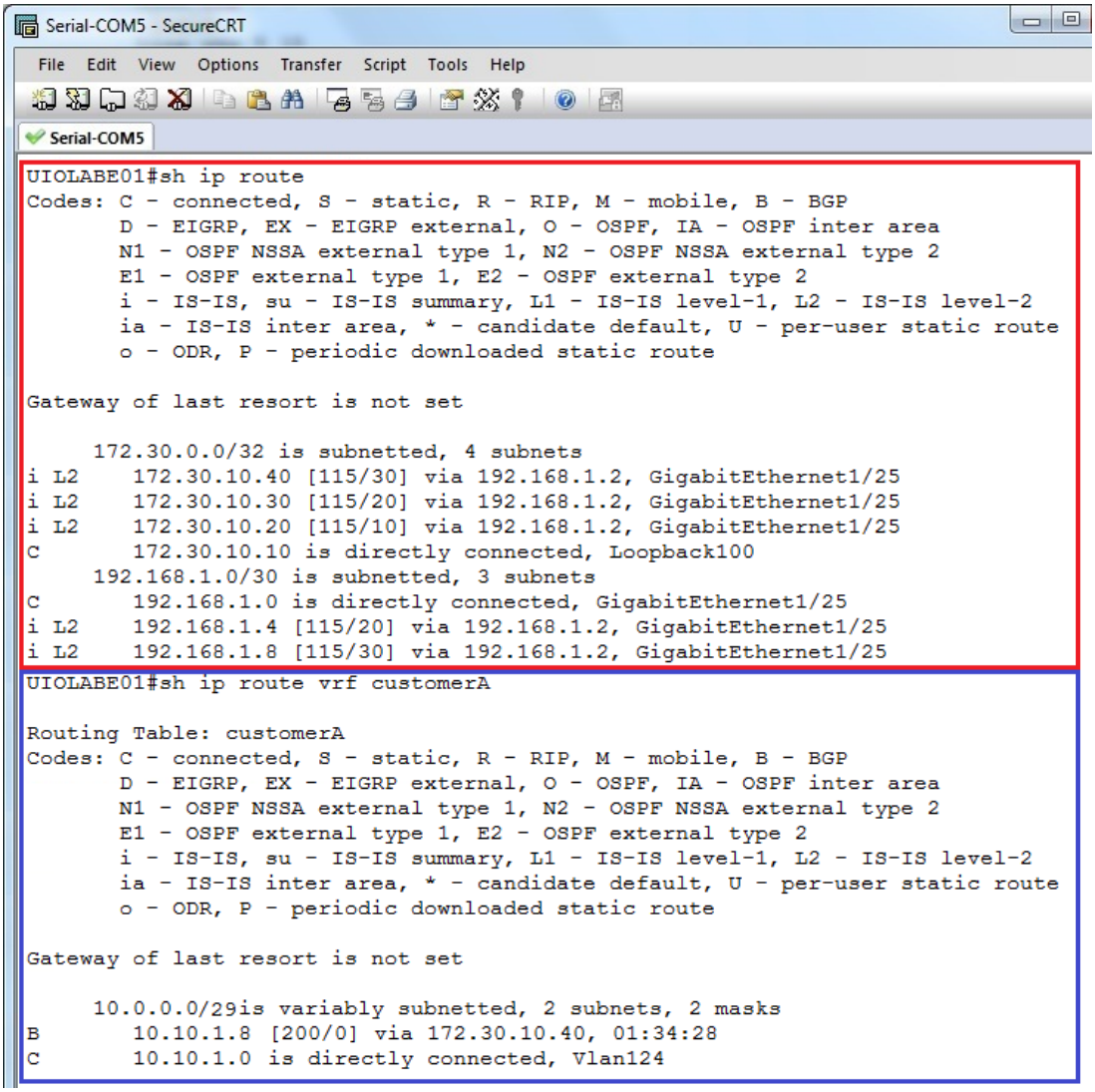


Figura 4.59: Salida del comando “sh ip route vrf [vrf-name]”

En el ejemplo de la figura 4.59 se puede observar la tabla de enrutamiento global enmarcada en rojo, en la que las rutas de las instancias VRF no forman parte de esta tabla, y que estas se encuentran en cada una de las tablas de enrutamiento correspondientes a cada instancia VRF, la tabla de enrutamiento para la instancia VRF “customerA” enmarcada en azul, en la que aparecen dos rutas, la una es la red conectada directamente al router “UIOLABE01” (10.10.1.8), y la ruta aprendida del sitio remoto por medio de MP-BGP (10.10.1.0), configurada en el router “UIOLABE02”, y aprendida vía “172.30.10.40” que es la dirección de la loopback compartida de “UIOLABE02”, y es la interfaz fuente de las actualizaciones de MP-BGP de este router.

El comando ***sh ip bgp vpnv4 [****vrf-name****]*** muestra la información de direcciones VPNv4 en la tabla de BGP “Border Gateway Protocol” para una VRF en especifico.

En el caso del ejemplo de la figura 4.60 se tienen de igual manera dos entradas en la tabla de direcciones VPNv4 de BGP para la VRF “customerB”, donde la una representa la red local del cliente conectada al router “UIOLABE01”, mientras que la segunda entrada representa la red del sitio remoto ubicado en el otro PE router “UIOLABE02”, que para ser alcanzada tiene como siguiente salto la IP de la loopback compartida “172.30.10.40” del router PE remoto.

```
UIOLABE01#sh ip bgp vpnv4 vrf customerB
BGP table version is 29, local router ID is 172.30.10.10
Status codes: s suppressed, d damped, h history, * valid, > best, i - internal,
              r RIB-failure, S Stale
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop            Metric LocPrf Weight Path
Route Distinguisher: 1:600 (default for vrf customerB)
*> 10.10.2.0/29     0.0.0.0                  0         32768 ?
*>i10.10.2.8/29     172.30.10.40             0    100      0 ?
```

Figura 4.60: Salida del comando “ip bgp vpnv4 [vrf-name]”

Para verificar el enrutamiento entre PE-CE dependerá del protocolo de enrutamiento utilizado en el lado del cliente; en el caso de la prueba se ha escogido como protocolos de enrutamiento para los clientes “customerA y

customerB", OSPF y RIP v2 respectivamente, las configuraciones se muestra a continuación.

```
router ospf 1 vrf customerA
log-adjacency-changes
redistribute connected
redistribute static
redistribute bgp 65000 subnets
network 10.10.1.0 0.0.0.7 area 0
```

```
router rip
version 2
 !
address-family ipv4 vrf
customerB
redistribute bgp 65000 metric 0
network 10.0.0.0
no auto-summary
version 2
exit-address-family
```

En esta configuración se puede observar resaltado cómo se realiza la redistribución de protocolos, los protocolos de enrutamiento OSPF y RIP v2, solo son conocidos entre los routers de frontera que participan de la instancia VRF, tanto del lado del cliente como del proveedor de servicios, y no así los routers de core "P", para los cuales las VRFs son transparentes.

Considerando que el protocolo de enrutamiento manejado en el backbone MPLS es el IGP "ISIS", las actualizaciones de OSPF y de RIP v2 no podrían ser transportadas o manejadas normalmente dentro del backbone del Proveedor de Servicios, por lo que es necesario el empleo de MP-BGP para llevar las actualizaciones de los protocolos mencionados, los comandos que ayudan a verificar su funcionamiento son:

El comando ***show ip rip database [****vrf vrf-name****]*** muestra la información completa contenida en la base de datos de RIP para una VRF en específico, de igual manera el comando ***show ip ospf*** *process-id* ***database*** muestra la información completa contenida en la base de datos de OSPF del proceso respectivo asociado a una VRF.

En el ejemplo de la figura 4.61 los comandos fueron ejecutados en el router PE "UIOLABE02" donde la VRF "customerB" se encuentra corriendo el protocolo de enrutamiento RIPv2, para mostrar su base de datos se aplicó el comando ***show ip rip database vrf customerB***. Que se observa en la sección resaltada de azul, en la cual existen dos entradas, la red 10.10.2.0 que se ha obtenido por redistribución de protocolos vía "172.30.10.10", es la IP utilizada como

identificador del router PE remoto “UIOLABE01”, en donde se conecta otra sucursal del cliente, la otra entrada es la red 10.10.2.8 asignada a la sucursal del cliente, que se conecta directamente al router “UIOLABE02” en la interfaz Gi1/2.

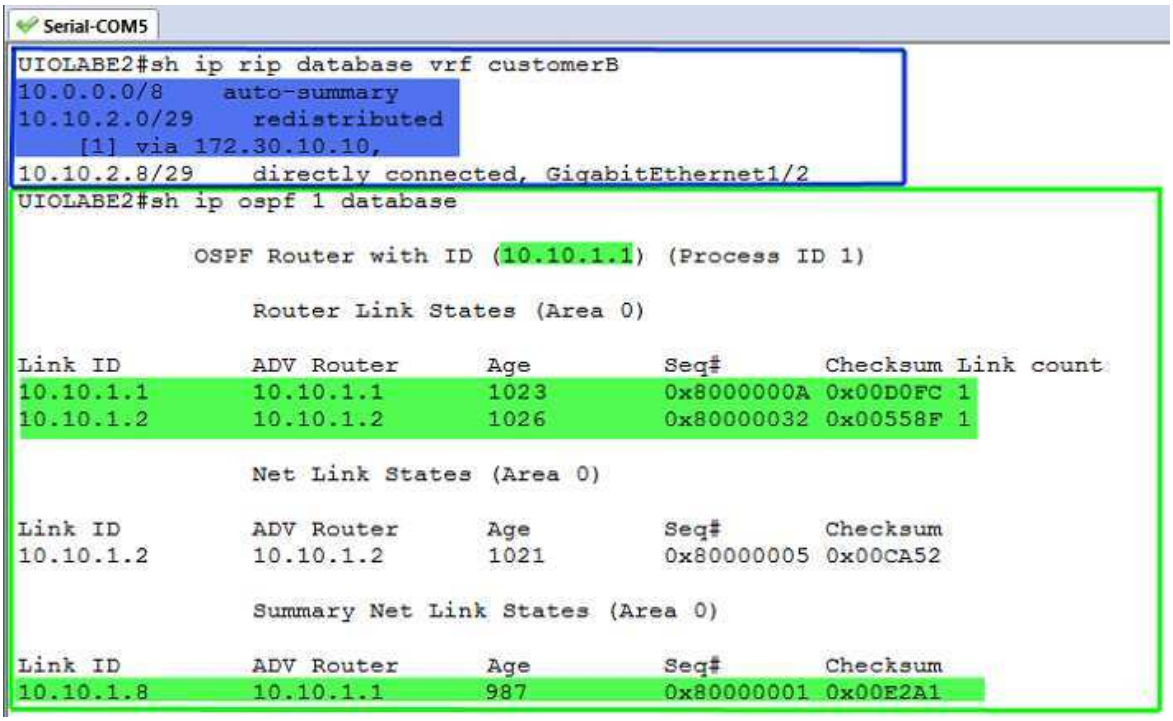


Figura 4.61: Verificación del enrutamiento entre PE- CE

Para el cliente de la VRF “customerA” el protocolo de enrutamiento en ejecución es OSPF, para verificar las entradas de la base de datos contenida en el proceso OSPF 1, se aplica el comando ***show ip ospf 1 database*** donde se observan dos redes (recuadro verde figura 4.61), la primera red es la que se encuentra conectada directamente al router local “UIOLABE02”, que posee el identificador de proceso OSPF 1 “10.10.1.1”, identificando esta red en la sección “*Router Link States*”, donde aparecen las dos direcciones IP del enlace local, la segunda red es la red remota, la cual se visualiza en la sección “*Summary Net Link States*” cuya red aprendida es “10.10.1.8”.

Para obtener una tabla más detallada de las etiquetas utilizadas para una VRF en particular se puede usar el comando **“show ip bgp vpnv4 all tags”**, un ejemplo de su salida se muestra en la figura 4.62, en la que se observa que la etiqueta 16 identifica los paquetes asociados a la instancia VRF “customerA” (resaltado

anaranjado) y la etiqueta 17 a los paquetes de la instancia VRF “customerB” (resaltado amarillo).

```
UIOLABE01#show ip bgp vpnv4 all tags
   Network          Next Hop      In tag/Out tag
Route Distinguisher: 1:100
   10.10.1.0/29     172.30.10.40    notag/16
Route Distinguisher: 1:200
   10.10.2.8/29     172.30.10.40    notag/17
Route Distinguisher: 1:500 (customerA)
   10.10.1.0/29     172.30.10.40    notag/16
   10.10.1.8/29     0.0.0.0         IPv4 VRF Aggr:16/nolabel(customerA)
Route Distinguisher: 1:600 (customerB)
   10.10.2.0/29     0.0.0.0         IPv4 VRF Aggr:17/nolabel(customerB)
   10.10.2.8/29     172.30.10.40    notag/17
```

Figura 4.62: Salida del comando “show ip bgp vpnv4 all tags”

Una vez comprobados algunos de los parámetros de configuración de las instancias VRF, se procedió a realizar las pruebas de conectividad, con la ayuda de los comandos **ping** y **traceroute** además de algunas capturas de paquetes con la ayuda de wireshark.

```
UIOLABE01#ping  10.10.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.2, timeout is 2 seconds:
.....
UIOLABE01#ping vrf customerA 10.10.1.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
UIOLABE01#ping vrf customerA 10.10.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
UIOLABE01#ping vrf customerA 10.10.1.5

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.5, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
UIOLABE01#ping vrf customerA 10.10.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
UIOLABE01#ping  10.10.1.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.1.10, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

Figura 4.63: Prueba de conectividad ping “vrf customerA”

El comando ping se usa para verificar el funcionamiento de una VRF, comprobando la conectividad entre los sitios de la VPN. Cuando se comprueba la conectividad desde un router de frontera PE es necesario especificar la instancia VRF que se desea verificar utilizando la sentencia ***ping vrf [vrf-name] [ip_address].***

En la figura 4.63 se tiene el ejemplo de conectividad para la VRF “customerA”, en donde para realizar las pruebas de conectividad, se necesita ejecutar los comandos dentro de la instancia VRF en prueba, ya que esta es la que conoce las tablas de enrutamiento necesarias para llegar a la red especificada.

En el caso resaltado en amarillo se observa que para llegar a uno de los sitios del cliente “customerA” con IP “10.10.1.10” se ejecutó el comando ***ping vrf customerA 10.10.1.10***, ya que si el comando se lo ejecuta fuera de la instancia VRF este buscará las rutas en la tabla de enrutamiento general donde estas no existen y por lo tanto no podrían llegar a su destino. En la figura 4.63 en la parte resaltada de celeste se muestra que al aplicar el comando ***ping 10.10.1.10*** este no tiene éxito, como es el caso resaltado en amarillo. En la figura 4.64 se muestran las pruebas de conectividad para la instancia VRF “customerB”.

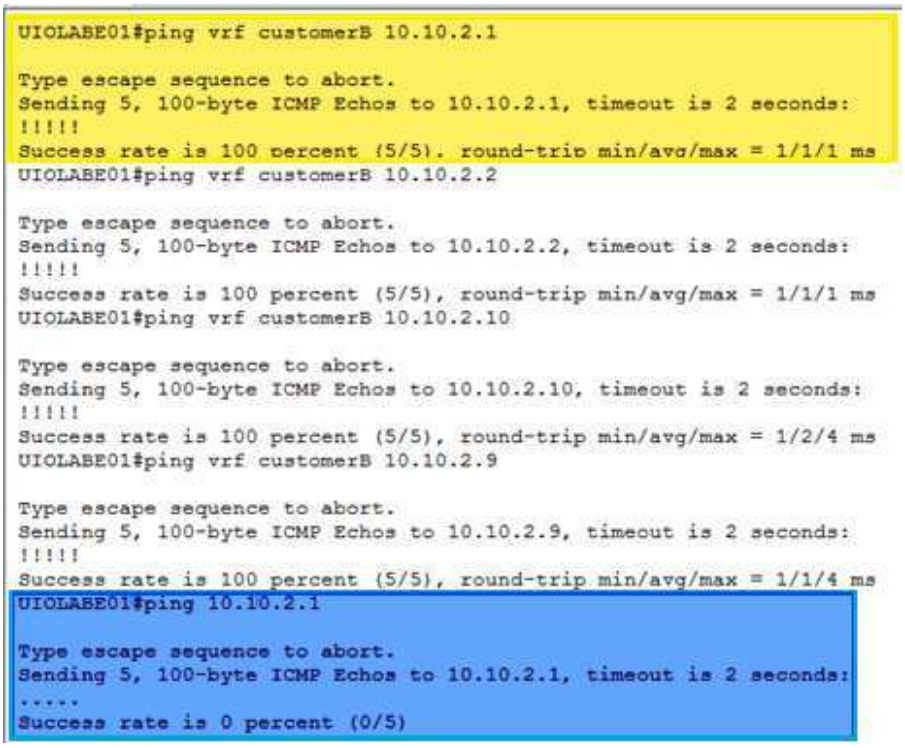


Figura 4.64: Prueba de conectividad ping “vrf customerB”

Otra prueba de conectividad es la de realizar un traceroute, de igual manera este comando debe ser ejecutado dentro de la instancia VRF en prueba, usando el comando ***traceroute vrf [vrf-name] [ip_address]***, en la figura 4.65 se muestra la ejecución del comando para cada una de las instancias VRF configuradas.

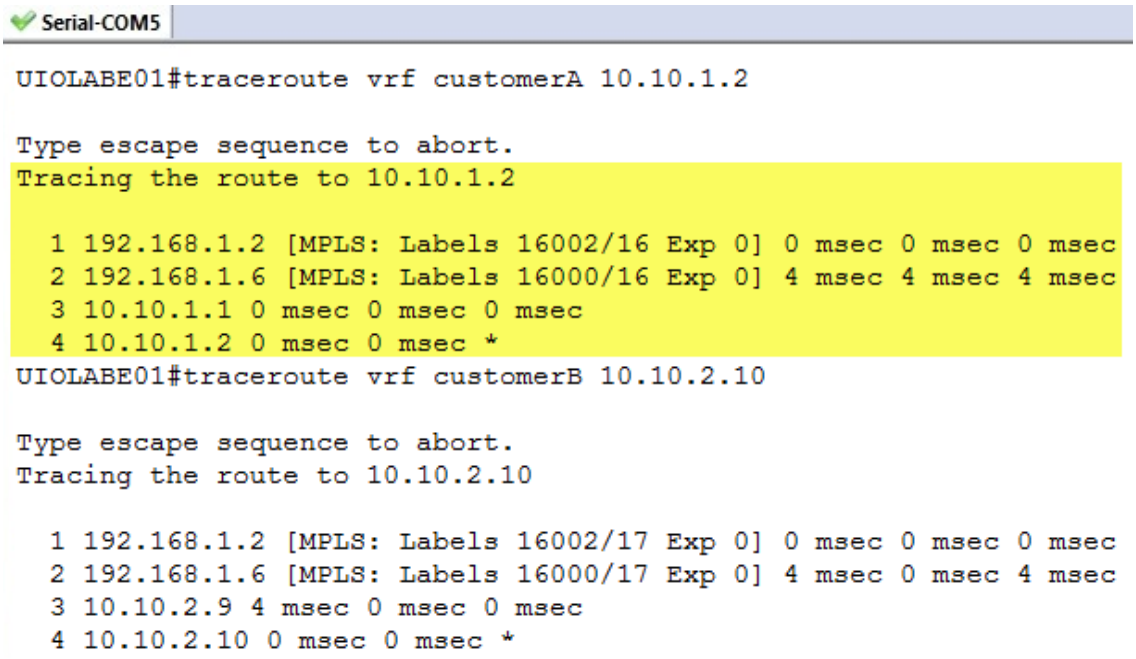


Figura 4.65: Prueba de conectividad traceroute

En la figura 4.65 se observa cada uno de los saltos que van tomando los paquetes hacia su destino y como se van manejando las etiquetas en MPLS. Por ejemplo en la sección resaltada de amarillo se muestra que los paquetes que van dirigidos hacia la IP “10.10.1.2” de la vrf *customerA* a la salida del router “UIOLABE01” se la etiqueta doblemente, la etiqueta más interna, para este caso la etiqueta 16 identifica la VRF y la más externa el camino LSP que tomará salto a salto, es por ello que en el primer salto esta etiqueta tiene el valor “16002”, al llegar al siguiente router este la intercambia por la etiqueta “16000”.

En la figura 4.66 se muestran las pruebas de conectividad desde el cliente, y debido a que ellos no tienen la necesidad de manejar MPLS para alcanzar sus redes remotas, el backbone MPLS se comporta de forma transparente para los clientes; ellos solo deben ejecutar las pruebas en un ambiente puramente IP, ejecutando tanto los comandos ping y traceroute sin ninguna instancia VRF.

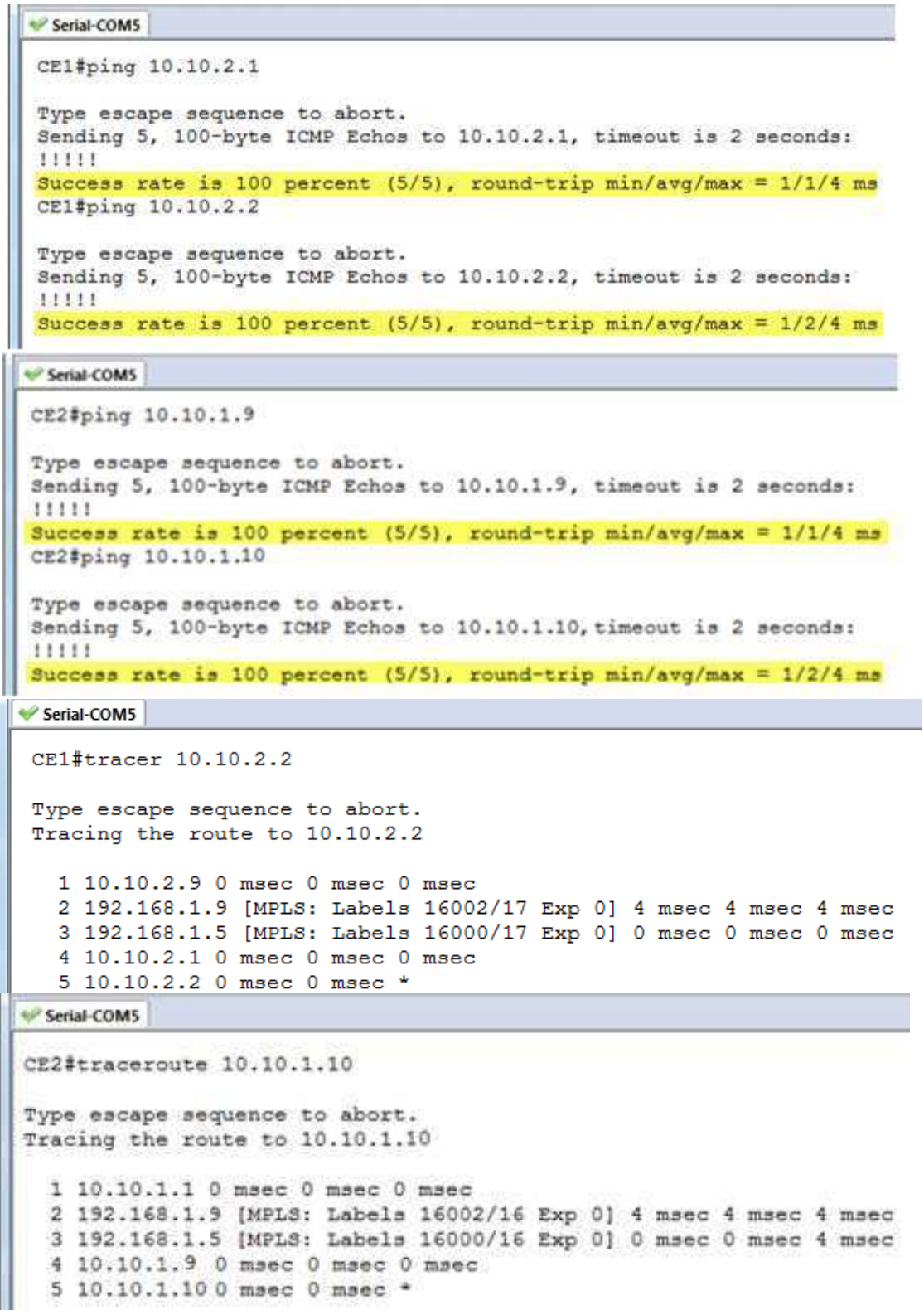
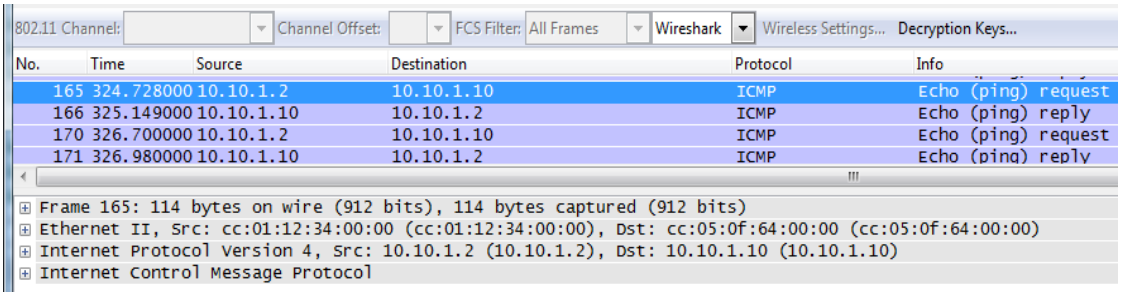
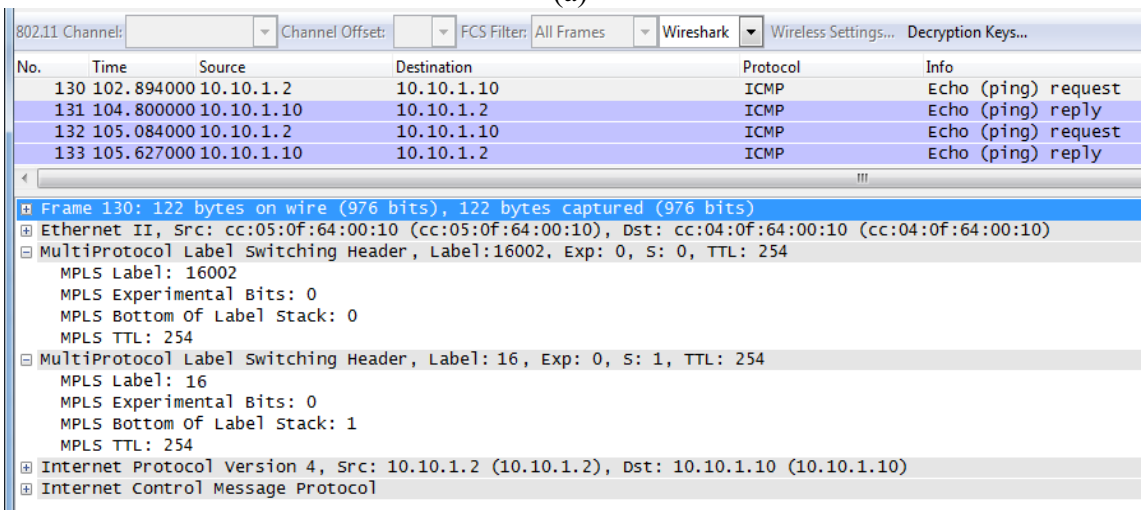


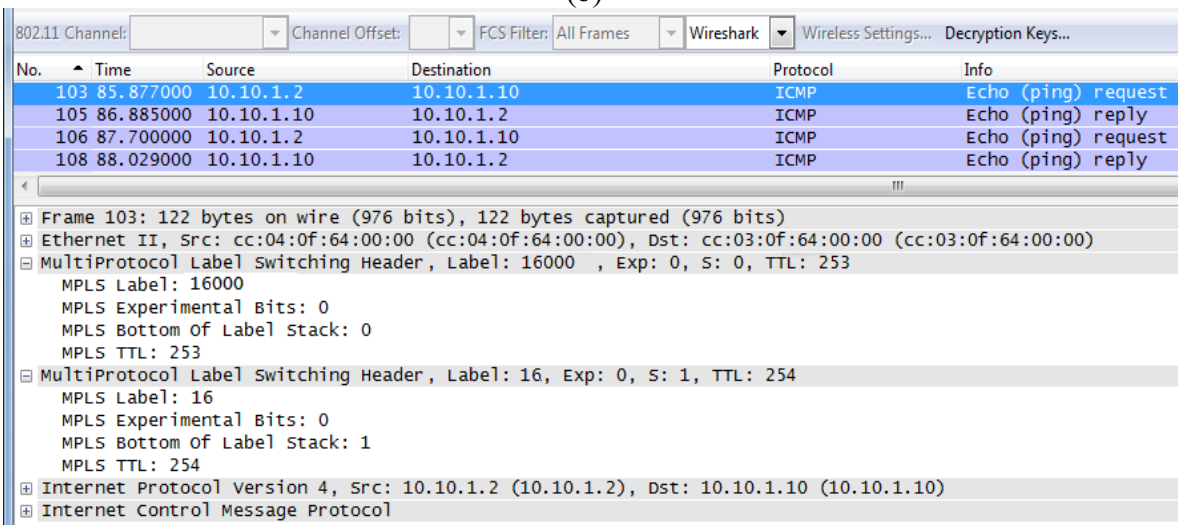
Figura 4.66: Pruebas de conectividad desde los equipos del cliente



(a)



(b)



(c)

Figura 4.67: Capturas Wireshark.

En la figura 4.67 se presentan algunos paquetes dirigidos desde el router del cliente CE4 (10.10.1.2) hacia su sitio remoto (10.10.1.10), capturados en algunos routers de la topología. La primera figura 4.67(a) muestra una captura de los paquetes a la salida del router del cliente “CE4”; donde se observa que estos no son etiquetados, y van como un paquete IP puro.

Para el caso de la figura 4.67(b) la captura está realizada a la salida del router PE2 “UIOLABE02” hacia el router P “UIOLABP02”, en donde los paquetes son etiquetados doblemente y tratados mediante MPLS. La etiqueta 16 identifica que el paquete viene de la vrf *customerA*, en cambio que la etiqueta 16002 identifica el camino LSP hacia el router P. En la figura 4.67(c) el paquete es capturado en el enlace entre routers P en donde solo se intercambian las etiquetas más externas la 16002 por la etiqueta 16000 manteniendo la etiqueta interna 16 para identificar la VRF.

4.5 PRUEBAS Y RESULTADOS DE QoS [7] [8] [13] [14] [24]

Para realizar las pruebas de QoS se parte de la topología básica en la que se realiza la habilitación de MPLS, en esta topología se tiene configurado y funcionando IS-IS, LDP y habilitado MPLS en las interfaces, por lo que en esta sección no se detallan las pruebas del funcionamiento básico.

4.5.1 LIMITACIÓN DEL TRÁFICO

A continuación se muestran las pruebas de *traffic policing*, en las que se limita el tráfico que ingresa por una determinada interfaz.

Esta prueba se realizó antes de clasificar el tráfico y asignarlo a una clase específica en base al valor de precedencia IP de cada paquete, por esta razón se usa la *class-default,* clase a la que pertenece todo el tráfico entrante. La limitación del tráfico se realiza para todo el volumen de tráfico que ingresa por la interfaz. Las configuraciones necesarias se muestran a continuación:

```
policy-map 10Mbps
  class class-default
    police cir 10000000
     conform-action transmit
     exceed-action drop
     violate-action drop
interface interface GigabitEthernet1/1
service-police input 10Mbps
```

La configuración mostrada es un ejemplo de todas las *traffic policing* configuradas en PE1, se las asocia como política de entrada en las interfaces por las que

ingresa el tráfico a la red, se configura únicamente el CIR (en bps), que es el valor máximo que puede alcanzar el tráfico (para la política 10Mbps), que será trasmitido por la red, no se asigna un valor para el tráfico en exceso por lo que se lo descarta, se lo configura de esta manera, porque dentro de la red de CNT se lo implementa de esta forma.

La figura 4.68 se realizó gracias a las herramientas de análisis que ofrece el generador de tráfico IXIA, donde el eje "Y" representa el flujo de tráfico en Mbps y en el eje "X" el tiempo.

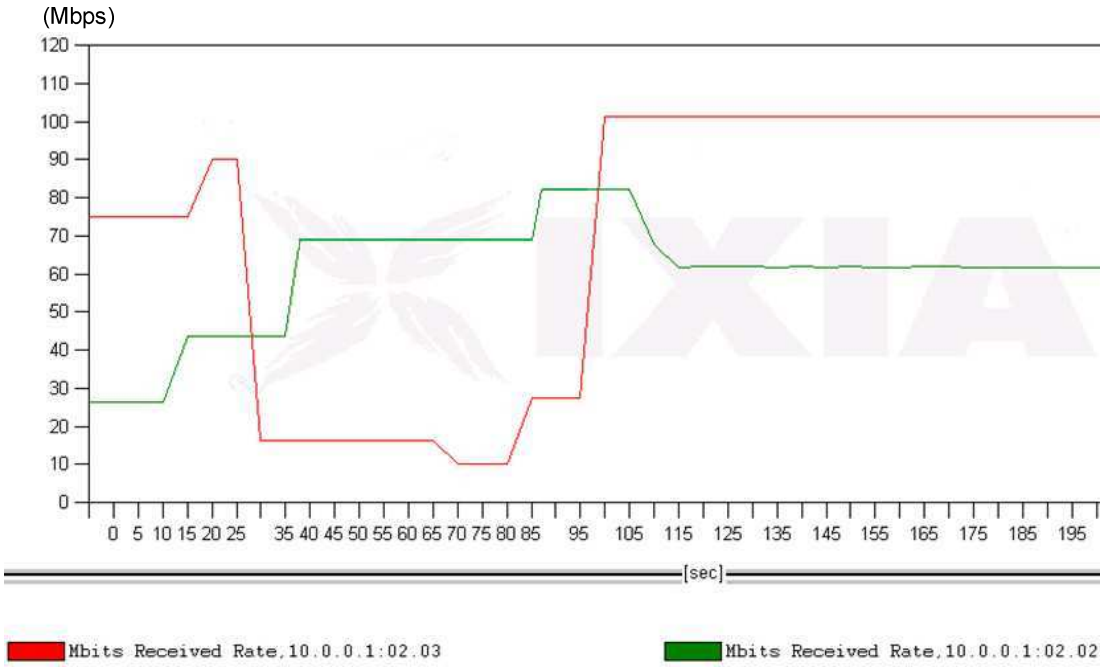


Figura 4.68: Tráfico recibido en IXIA2.

En la figura 4.68 se observa el gráfico del flujo de tráfico recibido en IXIA 2, en verde se observa el tráfico del cliente 1 que llega a la interfaz gi2/2 del generador, esta proviene de la interfaz Gi2/2 de IXIA1. En la interfaz por la que ingresa el tráfico en PE1 (Gi1/1) se asocia una política inicial de 25Mbps aplicada hasta los 10 segundos, en este punto se cambia por una de 45 Mbps, a los 35 s esta se cambia por una de 70 Mbps, a los 85 s se la cambia por una de 80 y a los 110 s por una de 60Mbps, en el gráfico se puede observar que los limites aplicados al tráfico coinciden con lo configurado por lo que se comprueba su adecuado funcionamiento, permitiendo a un proveedor de servicios limitar el tráfico máximo de su cliente, de esta manera se asegura que cumpla con el perfil contratado.

Para el flujo en rojo se tiene algo similar, este es el tráfico recibido por la interfaz Gi2/3 del generador, que proviene de la interfaz Gi2/1 de IXIA1, la política inicial configurada en Gi1/2 de PE1 es de 75Mbps, a los 20s se cambia por una de 90Mbps, a los 25 por una de 15Mbps, a los 65 por una de 10 Mbps, a los 85 una de 20Mpbs y a los 95 por una de 100 Mbps, con esto se observa que una política aplicada en diferentes interfaces tendrá el mismo efecto, pues la política de 20Mbps se aplicó en las dos interfaces y se obtuvo el mismo resultado. Los tiempos de los cambios de las políticas no son exactos sino que se tomaron como base de lo que se observa en el gráfico.

4.5.2 MARCADO DE TRÁFICO

Lo siguiente que se probó es el marcado del tráfico que se realiza en los nodos de borde (Cisco 6500), para realizar esto se debe manejar precedencia IP en los nodos PEs, ya que los paquetes generados por las tres interfaces del IXIA tienen marcado el campo ToS. Las configuraciones para crear las clases en los nodos PE son:

```
!
! Creación de la clase Datos coincide con los paquetes que tengan
! el campo de precedencia IP o el EXP de MPLS en 3
!
class-map match-any Datos
  match ip precedence 3
  match mpls experimental topmost 3
!
! Creación de la clase DatosNoCriticos coincide con los paquetes
! que tengan el campo de precedencia IP o el EXP de MPLS en 1
!
class-map match-any DatosNoCriticos
  match mpls experimental topmost 1
  match ip precedence 1
!
! Creación de la clase DatosCriticos coincide con los paquetes que
! tengan el campo de precedencia IP o el EXP de MPLS en 5
!
class-map match-any DatosCriticos
  match mpls experimental topmost 5
  match ip precedence 5
!
```

Las configuraciones anteriores crean tres clases de servicio, para cada una se tiene dos criterios de coincidencia, cualquier paquete que cumpla uno de los dos

criterios se considera parte de esa clase. Se crean dos criterios debido a que en los nodos de frontera se manejan dos tipos de paquetes, los que llegan con etiquetamiento MPLS (proveniente de los nodos Ps), y llevan la información de QoS en el campo EXP de la etiqueta MPLS; y los paquetes IP (provenientes de los clientes) sin etiquetas, que llevan la información de QoS en el campo ToS, usado por “precedencia IP”.

Con las configuraciones mostradas el tráfico proveniente de los generadores, pertenece a una clase, los paquetes únicamente tendrán marcado el campo ToS, por lo que es necesario trasladar este valor al campo EXP, para que los routers del backbone MPLS puedan dar la QoS requerida. El campo ToS de precedencia IP y el EXP de MPLS es de 3 bits (8 posibles valores), como los dos campos tienen la misma longitud se puede marcar al campo EXP con el mismo valor del ToS. A continuación se muestra la manera de realizar el marcado del campo EXP con el valor del campo ToS.

```
!
! Creación de la política que marca el campo EXP en los paquetes
! MPLS al salir de la interfaz Gi1/25
!
policy-map SalidaNodosP
  class DatosNoCriticos
   set mpls experimental imposition 1
  class Datos
   set mpls experimental imposition 3
  class DatosCriticos
   set mpls experimental imposition 5
!
! Asociación de la política a la interfaz correspondiente
!
interface interface GigabitEthernet1/25
service-police output SalidaNodosP
```

Las configuraciones mostradas permiten crear una política que realiza el marcado del campo EXP en cada flujo de tráfico antes de enviarlo al nodo P, se la asocia como una política de salida en la interfaz Gi1/25 de UIOLABE01, para comprobar que la clasificación y marcado se realiza de manera correcta se usa el comando ***show policy-map interface gi1/25***.

En la figura 4.69 se observa que se realizó la clasificación y marcado del tráfico, se observan las tres clases de tráfico creadas y la clase por defecto, para cada

una de las clases se tienen el nombre de la clase, los dos criterios de coincidencia: uno con la precedencia IP y el otro con el campo EXP; la acción que en caso es el marcado del campo EXP y estadísticas de los paquetes que son parte de esa clase.

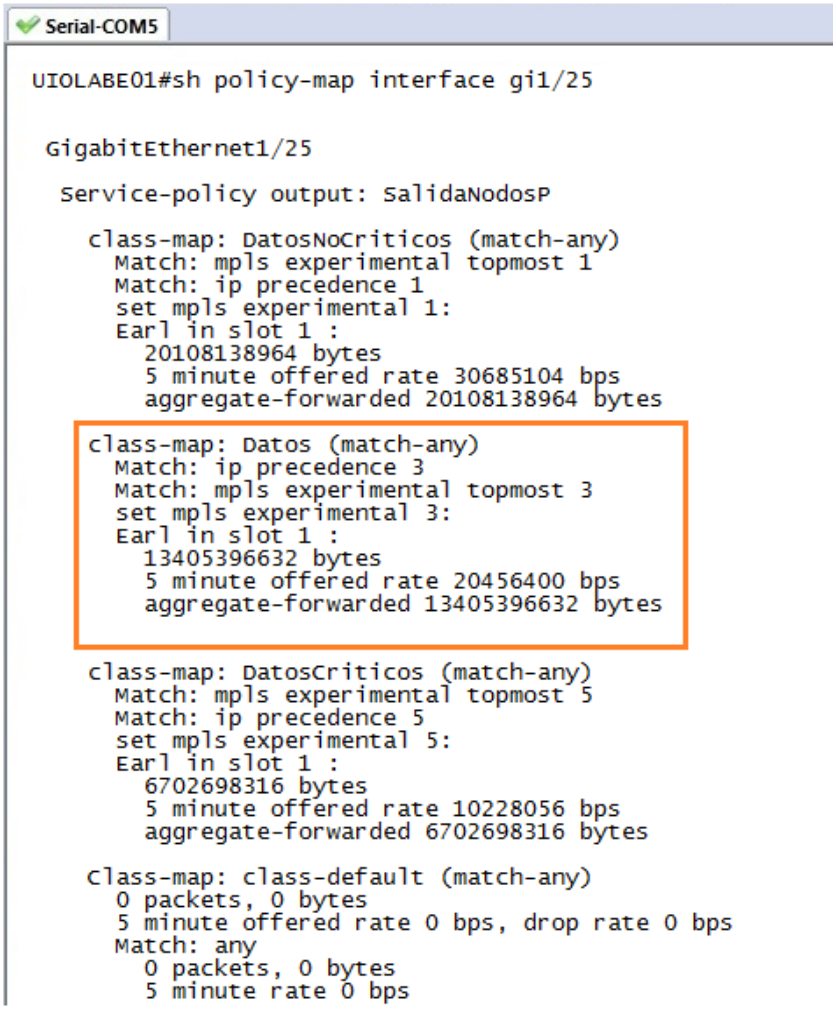


Figura 4.69: Estadísticas de tráfico de la interfaz Gi1/25 de UIOLABE01.

Por ejemplo para la clase datos los criterios de coincidencia que se observan son: el valor del campo EXP o ToS del paquete debe ser 3, la política coloca el valor del campo EXP a 3, se tienen 13405396632 bytes que coinciden y un tasa promedio en los últimos 5 minutos de 20456400 bps.

Para comprobar que el tráfico está siendo marcado y clasificado en su totalidad se dejaron pasar más de 5 minutos, y se compararon los valores que se muestran en las estadísticas con los que se establecieron en cada interfaz Esto se observa en la tabla 4.1.

Flujos de IXIA 1			Estadísticas en UIOLABE01	
Interfaz	**Ancho de banda (porcentaje de 1Gbps)**	**Valor marcado en el campo ToS**	**Clase de tráfico**	**Tasa promedio en los últimos 5 minutos**
Gi2/2	30%	1	DatosNoCriticos	30.68 Mbps
Gi2/3	20%	3	Datos	20.45 Mbps
Gi2/4	10%	5	DatosCriticos	10.22 Mbps

Tabla 4.1- Comparación de los valores configurados y las estadísticas obtenidas.

Comparando los valores obtenidos en las estadísticas con los configurados en los generadores se observa que son similares; por lo que se concluye que todos los flujos enviados por los generadores se están clasificando, son parte de una clase y están siendo marcados de manera adecuada. Los valores no son iguales debido a que en los generadores IXIA, el tráfico a crear se configura como un porcentaje del ancho de banda de la interfaz, por lo que los anchos de banda configurados no son exactos.

Dentro de los nodos P de la topología, la clasificación del tráfico se la realizará basándose en el campo EXP, por lo que las configuraciones para crear las clases de servicio y el criterio de coincidencia para los paquetes que son parte de una clase son:

```
!
! Creación de la clase Datos que coincide con los paquetes con EXP
! con un valor de 3
!
class-map match-any Datos
  match mpls experimental topmost 3
!
! Creación de la clase DatosNoCriticos que coincide con los
! paquetes con EXP con un valor de 1
class-map match-any DatosNoCriticos
  match mpls experimental topmost 1
!
! Creación de la clase DatosCriticos que coincide con los
! paquetes con EXP con un valor de 5
!
class-map match-any DatosCriticos
  match mpls experimental topmost 5
!
```

Con estas configuraciones los nodos P no manejan precedencia IP, realizan QoS basándose en el valor del campo EXP de las etiquetas MPLS. Para comprobar que el marcado en los nodos PE se realizó de manera adecuada y que los nodos P clasifican el tráfico se creó la siguiente política:

```
policy-map PoliticaSalida
  class Datos
  class DatosNoCriticos
  class DatosCriticos
!
interface interface GigabitEthernet2/2
service-police output PoliticaSalida
```

Esta política no realiza ninguna acción, únicamente se utiliza para observar las estadísticas de la interfaz Gi2/2 que se conecta con el otro nodo P, el resultado del comando show se muestra a continuación:

En la figura 4.70 se puede observar las estadísticas que se ofrecen para la política “PoliticaSalida”; para cada clase se observa el numero de paquetes, el número de bytes y la tasa promedio para los últimos 5 minutos, se observa que está realizando la clasificación de los paquetes y asignándolos a una clase con lo que se comprueba que se está llevando a cabo el marcado en los nodos Ps.

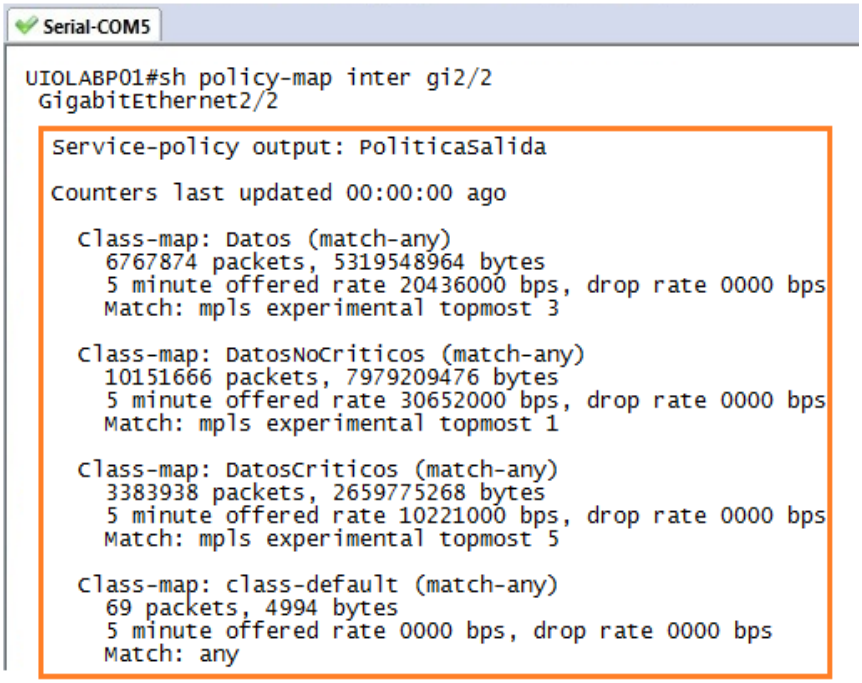


Figura 4.70: Estadísticas de la interfaz Gi2/2 de UIOLABP01.

Al comparar las estadísticas con las obtenidas en la figura 4.69 se observa que los valores obtenidos son similares, por lo que se comprueba que se está realizando una clasificación adecuada para todo el flujo en los nodos Ps. La comparación se observa en la tabla 4.2.

Estadísticas en UIOLABE01		Estadísticas en UIOLABP01	
Clase de tráfico	**Tasa promedio en los últimos 5 minutos**	**Clase de tráfico**	**Tasa promedio en los últimos 5 minutos**
DatosNoCriticos	30.68 Mbps	DatosNoCriticos	30.65 Mbps
Datos	20.45 Mbps	Datos	20.43 Mbps
DatosCriticos	10.22 Mbps	DatosCriticos	10.22 Mbps

Tabla 4.2- Comparación de las estadísticas obtenidas en UIOLABE01 con las obtenidas en UIOLABP01.

4.5.3 MANEJO DE CONGESTIÓN Y *TRAFFIC SHAPING*

Previo a mostrar el manejo de congestión y el *traffic shaping* es necesario observar cómo se comportan los equipos frente a un evento de congestión sin ninguna configuración de QoS.

En las interfaces Gi2/3 y Gi2/4 se configura un flujo de 780Mbps y 980Mpbs respectivamente, estos flujos saturarán el enlace entre el equipo PE y P ya que es un enlace de 1 Gbps que no lograra trasmitir el 1.76 Gbps generado por IXIA, el gráfico de tráfico obtenido en el generador de tráfico se observa en la figura 4.71.

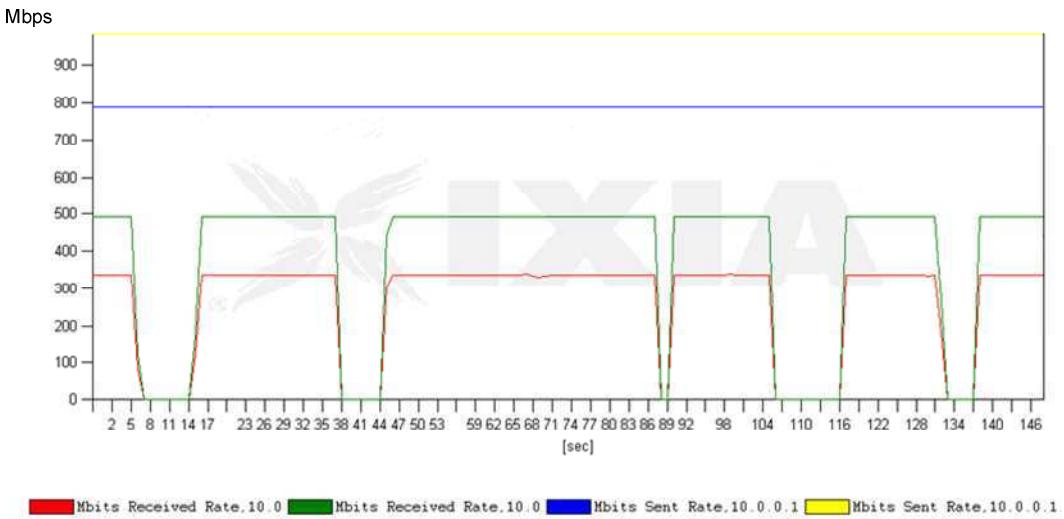


Figura 4.71: Gráfico del tráfico en eventos de congestión.

En la figura 4.71 se observa en azul y amarrillo el tráfico enviado a la red, en verde y rojo se muestra el tráfico que se recibe en las interfaces del generador. Se observa que mucho del tráfico enviado se pierde; pues los flujos de tráfico recibidos son menores a los enviados, la pérdida de paquetes se da por la limitada capacidad de trasmisión de las interfaces físicas.

También se observa que existen momentos en los que no se recibe ningún tráfico en las interfaces, esto se debe a que se pierde el reenvío MPLS cuando las sesiones LDP expiran. La congestión causa que los mensajes de mantenimiento de sesión se pierdan, haciendo que los temporizadores LDP expiren, finalizando la sesión. Este es el comportamiento de los diferentes enlaces en momentos de estrés en ausencia de QoS.

La intermitencia de las sesiones LDP se observan en la figura 4.72, aquí se mira que la sesión LDP de UIOLABE02 con UIOLABP02 se reinicia cada cierto intervalo, por lo que no se mantiene un reenvío constante de paquetes en la red.

Figura 4.72: Intermitencias en las sesiones LDP.

El comportamiento descrito muestra que para manejar el concepto de sobresuscripción[2], es necesario asegurar un ancho de banda mínimo para el mantenimiento de las sesiones, evitando que se pierda conectividad y reenvío de paquetes.

En las pruebas no se muestra como reservar un ancho de banda mínimo para el mantenimiento de las sesiones; sin embargo como en CNT la sobresuscripción se utiliza para los clientes HOME, se presentará una opción alternativa, en la que para controlar que no se saturen la capacidad de trasmisión disponible en los

[2] Concepto utilizado por los proveedores de servicio en el que se vende más capacidad de la disponible, con la finalidad de obtener un mejor uso de los recursos. Esto se realiza por que no todos los clientes acceden de manera concurrente a un servicio.

enlaces, se colocará un política que controle el máximo ancho de banda que una clase puede utilizar (se usa la sentencia *shape*). Los paquetes que pertenecen a la clase DatosNoCriticos emularán el tráfico del los clientes HOME.

Con esto se puede vender más capacidad de trasmisión de la disponible y no se afectará a los demás servicios de la red, en caso de que se tenga un gran número de clientes conectados de manera concurrente el tráfico generado por estos no superará el máximo ancho de banda configurado, por lo que no se creará congestión en los enlaces de la red, conservando el envío de los paquetes de mantenimiento de sesión. La política de salida aplicada en todas las interfaces de UIOLABP02 que permite realizar esto es:

```
policy-map PoliticaSalida
 !
 ! Asignación del 20% del ancho de banda a la clase Datos
 !
 class Datos
  bandwidth percent 20
!
! Asignación del 30% del ancho de banda a la clase DatosCriticos
!
 class DatosCriticos
  bandwidth percent 30
!
! Asignación del 10% del ancho de banda a la clase DatosCriticos,
! un máximo del 15 % y un máximo en la cola de 20000 paquetes
!
 class DatosNoCriticos
  bandwidth percent 10
  shape average percent 15
  queue-limit 20000 packets
 !
!
 class class-default
 !
 end-policy-map
interface interface GigabitEthernet0/0/1/1
service-police output PoliticaSalida
```

Las configuraciones anteriores crean una política que asigna recursos a los paquetes que son parte de una clase de tráfico. Para la clase DatosNoCrtiticos asigna un ancho de banda mínimo garantizado del 10%, una cola máxima de 20000 paquetes y una tasa pico máxima de envío del 15%, este será el límite del tráfico de que pueden utilizar los clientes HOME, para la clase Datos se asigna un

mínimo ancho de banda del 20% y para la clase DatosCriticos un mínimo ancho de banda del 30%. Se la asocia como política de salida en la interfaz Gi0/0/1/1.

Luego de haber realizado los cambios que permiten generar un evento de congestión en UIOLABP02 descritos en el capítulo 3, se procedió a realizar la clasificación de los paquetes en base a la precedencia IP, aumentando las siguientes configuraciones en UIOLABPE02:

```
class-map match-any Datos
  match ip precedence 3
  match mpls experimental topmost 3
class-map match-any DatosNoCriticos
  match mpls experimental topmost 1
  match ip precedence 1
class-map match-any DatosCriticos
  match mpls experimental topmost 5
  match ip precedence 5
!
```

Para probar el funcionamiento del traffic shaping, utilizada en la clase DatosNoCriticos, se generó un tráfico de 70Mbps sobre la interfaz Gi2/1, 40Mbps en la interfaz Gi2/2 y 60Mbps en la interfaz G2/3 del IXIA 2.

Figura 4.73: Tráfico de en IXIA 1

En la figura 4.73 se observa tres flujos de tráfico, en un inicio ninguno de estos excede los límites máximos, por lo que se trasmiten sin problema, en el instante de tiempo 67 segundos se incrementa el tráfico de Gi2/3 (Clase DatosNoCriticos)

a 310 Mbps por lo que el tráfico recibido se incrementa, en un inicio se observa un pico antes de la estabilización del flujo en 150Mbps, este valor corresponde con el 15% de ancho de banda configurado, con esto se comprueba que el comando *shape* limita el tráfico máximo para un interfaz, pudiendo utilizarse para controlar el tráfico de los clientes cuando se utiliza la sobresuscripción.

El pico corresponde al comportamiento del algoritmo token bucket, partiendo de que en cada intervalo de tiempo se generan bc tokens y en casos de congestión se pueden utilizar hasta bc+be tokens. En el intervalo anterior a generar los 310Mbps no se consumen todos los tokens generados por lo que se tiene bc+be tokens disponibles, al generarse el evento de congestión se envía una ráfaga de tráfico que utiliza todos los tokens almacenados, por lo que se observa un pico que excede el 15% configurado, una vez se consumen los tokens en exceso se generarán tokens a una tasa bc constante por lo que se estabiliza el flujo de tráfico y se enviará a una tasa de 150 Mbps.

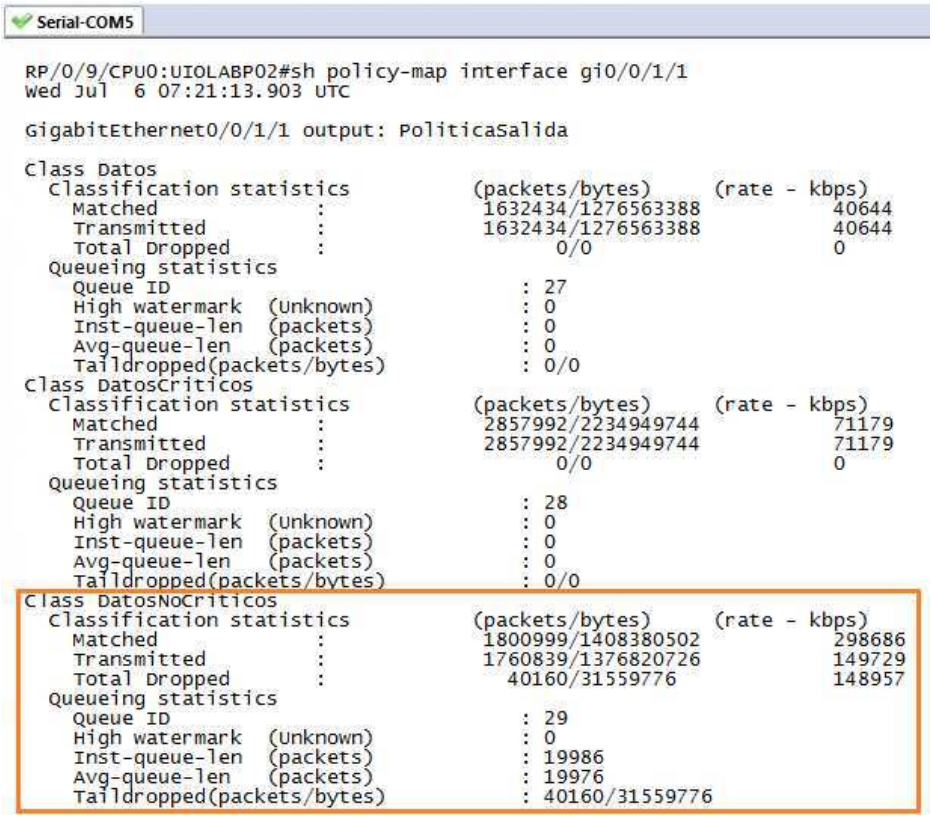


Figura 4.74: Estadísticas de la política Politicassalida.

El la figura 4.74 se observa las estadísticas del tráfico en la interfaz Gi0/0/1/1 es diferente de las presentadas anteriormente, porque el resultado obtenido es para el IOS XR, se observa las estadísticas para las tres clases.

A continuación se detalla únicamente para la clase DatosNocriticos, en la que se generó un exceso de tráfico, en la primera sección se observa las estadísticas de la clasificación, se muestran los paquetes que cumplen con los criterios de coincidencia, los paquetes trasmitidos y los paquetes descartados, las estadísticas se muestran en número de paquetes, bytes y Kbps.

A continuación se tiene un segundo grupo con las estadísticas de encolamiento, de estas las que tiene relevancia son el tamaño instantáneo de la cola que es de 19986 paquetes, el tamaño promedio de la cola que es 19976 paquetes y los paquetes descartados por *tail drop* en número de paquetes y bytes. Se observa que el tamaño de la cola no superan los 20000 paquetes comprobándose que lo configurado como límite máximo del tamaño de la cola se cumple.

La última prueba realizada para QoS está diseñada para probar el funcionamiento del comando *bandwith*, se usó el mismo escenario de la prueba anterior, en este caso se probará el mínimo ancho de banda garantizado para la clase DatosCriticos, para probar se colocaron las siguientes condiciones iniciales: en el IXIA 2 en la interfaz gi2/2 se generaron 430 Mbps marcados con precedencia 1, en la interfaz gi2/3 410Mbps con precedencia 3 y en Gi2/4 que genera el flujo de tráfico para la clase DatosCriticos no se envía ningún flujo de tráfico al inicio, cuando inicie el flujo se marcará con precedencia IP de 5.

En el lado de IXIA 1 no se realiza ningún cambio, pues solo recibirá los flujos y realizará el gráfico del tráfico que ingresa por las interfaces, las condiciones iniciales descritas se muestra en la figura 4.75 desde el segundo 235 al 307.

Con estas condiciones iniciales se obtiene un flujo total de 840 Mbps que estarían haciendo uso del 84% del ancho de banda de la interfaz sin saturar los enlaces.

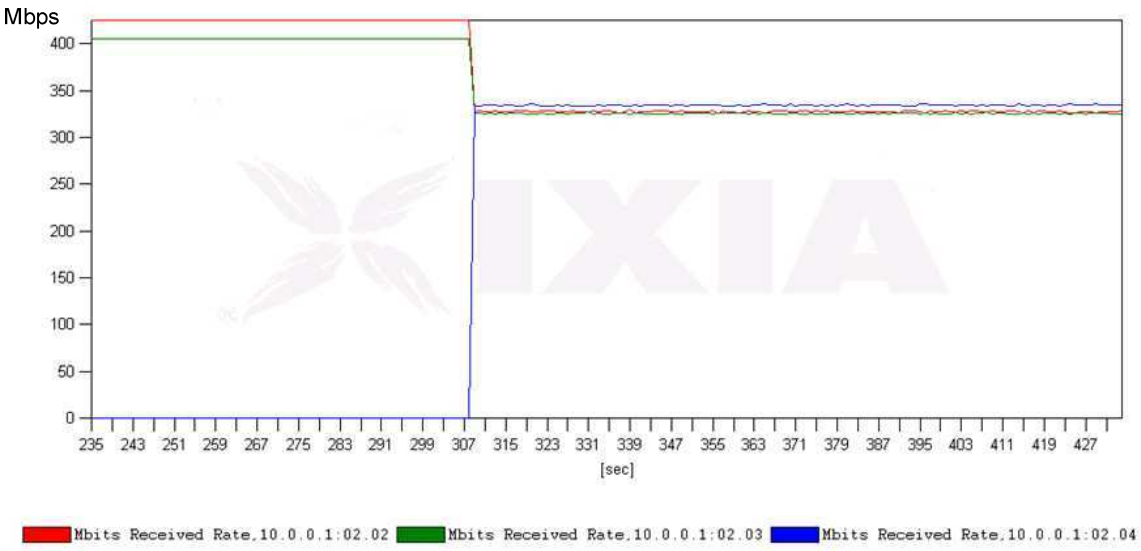


Figura 4.75: Tráfico en IXIA 1.

En el segundo 307 se genera un flujo de 350 Mbps por la interfaz Gi2/4 de IXIA 2, donde este tráfico generado será parte de la clase DatosCriticos, que tiene garantizado un ancho de banda mínimo del 30%, en la gráfica se observa que apenas se genera el flujo de tráfico automáticamente se reciben más de 300Mbps (flujo de color azul), con esto se comprueba que en un evento de congestión se garantiza al menos este mínimo ancho de banda del 30% para la clase DatosCriticos, se observa que asigna más capacidad de transmisión por que el ancho de banda que no se debe asegurar se reparte para todas las clases configuradas.

4.6 VERIFICACIÓN DE LA OPERACIÓN DE MPLS TRAFFIC ENGINNERING [32] [37] [39]

Una de las primeras pruebas que se plantea, es mostrar la creación de túneles entre dos routers de edge “UILABPE1 y UIOLABPE2”, el primero de los túneles a ser creado, tendrá como característica que el camino LSP que seguirá el túnel de ingeniería de tráfico (TE) se creará de forma dinámica, en cambio que para el otro túnel TE el camino LSP se establecerá de forma explícita, a continuación se presentan las configuraciones de la creación de dichos túneles en el router de edge UIOLABE1.

```
mpls traffic-eng tunnels
```

```
!
interface Loopback100
 ip address 172.30.10.10 255.255.255.255
!
interface Tunnel1
 ip unnumbered Loopback100
 tunnel destination 172.30.10.50
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 5 5
 tunnel mpls traffic-eng bandwidth  25
 tunnel mpls traffic-eng path-option 1 explicit name LSP1
!
interface Tunnel3
 ip unnumbered Loopback100
 tunnel destination 172.30.10.50
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 6 6
 tunnel mpls traffic-eng bandwidth  69
 tunnel mpls traffic-eng path-option 1 dynamic
!
ip explicit-path name LSP1 enable
 next-address 192.168.1.2
 next-address 192.168.1.14
 next-address 172.30.10.50
```

En la configuración mostrada el *Tunnel1* seguirá un camino LSP explícito, con prioridad 5 y ancho de banda 25 kbps, el *Tunnel3* seguirá un camino LSP dinámico, con prioridad 6 y ancho de banda 69 kbps. Para los dos túneles la IP asociada a los túneles es la dirección de la loopback100, para que estos túneles puedan activarse se requiere que se habilite el soporte TE de manera global, y sobre las interfaces que pueden ser posibles candidatas para formar parte de una ruta LSP de TE, en estas interfaces también se deben configurar los parámetros de reserva de ancho de banda de RSVP, para el caso de la prueba se reservó un ancho de banda de 512 kbps en cada una de las interfaces como se muestra a continuación:

```
interface GigabitEthernetX/XX
 ip address 192.168.1.5 255.255.255.252
 ip router isis
 speed nonegotiate
 mpls traffic-eng tunnels
 mpls label protocol ldp
 mpls ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 512 512
```

A continuación se presentan las pruebas y resultados obtenidos al configurar los túneles de Ingeniería de Tráfico.

El comando ***show mpls traffic-eng tunnels brief*** permite verificar el estado de los túneles, mostrando si el túnel TE se encuentra activo o no. También entrega información del camino LSP, mostrando las interfaces que lo conforman y que interfaz es de *upstream* y *downstream* del túnel, muestra si el proceso LSP Tunnel, reenvío de tráfico y FRR (Fast ReRoute) se encuentran activos.

En la figura 4.76 se muestra la salida del comando ***show mpls traffic-eng tunnels brief*** al ejecutarlo en el router "UIOLABE1" donde fueron creados dos túneles TE uno explícito "*Tunnel1*" y otro dinámico "*Tunnel3*", con los parámetros antes descritos, cuyo destino es el router PE "UIOLABE2" de router ID 172.30.10.50, de ahí que se observa en la figura 4.76 que el proceso LSP Tunnel y el reenvío de tráfico se encuentran activos, no así FRR que será habilitado más adelante para probar la otra característica de TE.

Se muestra en la figura 4.76 que tanto el túnel 1 y 3 son identificados con el hostname del router origen del túnel y el número de interfaz túnel, "UIOLABPE1_t1 y UIOLABPE1_t3", el destino del túnel es la dirección de la loopback compartida del router UIOLABPE2 "172.30.10.50". Como el comando esta ejecutado en el origen del túnel este solo tiene interfaces de *downstream,* la Gi1/26 y Gi1/25 para el túnel 1 y 3 respectivamente, además muestra el estado de los túneles y el estado del protocolo, los cuales se encuentran activos, lo que quiere decir que los parámetros de reserva de ancho de banda permiten establecer los túneles.

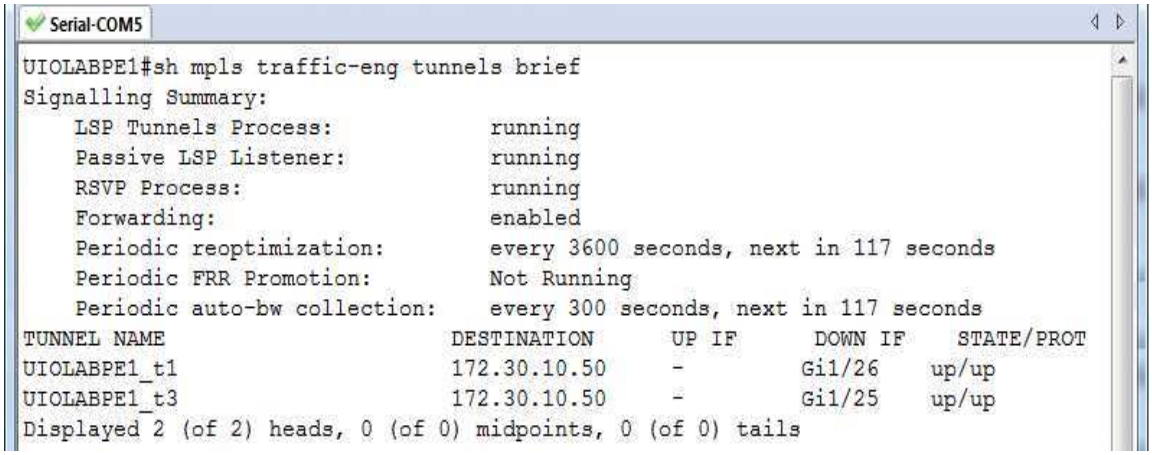


Figura 4.76: Salida del comando "show mpls traffic-eng tunnels brief".

A continuación se variarán las demandas de ancho de banda (AB) en los túneles de TE, con el objetivo de demostrar que si la cantidad de AB reservado en las interfaces, no es la suficiente para soportar la demanda de AB requerido para un túnel, este no podrá habilitarse.

Si una interfaz es utilizada por varios túneles TE, la suma de los requerimientos de AB de los mismos, no podrán superar la reserva de AB configurada en dicha interfaz, caso contrario el último túnel que requiera de la interfaz no podrá habilitarse. En el caso de querer habilitar el túnel se debe reconfigurar la reserva de AB en las interfaces ó disminuir la cantidad de AB requerido por el túnel, capaz de que la reserva de AB en las interfaces, puedan llevar los flujos cumpliendo los requisitos de AB de cada uno de los túneles que utilizan la interfaz.

Para la realización de esta prueba se cambió el requerimiento de AB del túnel 3 de 69 Kbps (tunnel mpls traffic-eng bandwidth 69) a un AB de 600 Kbps (tunnel mpls traffic-eng bandwidth 600). Debido a que la reserva de ancho de banda en las interfaces es de tan solo 512 Kbps éste no podrá ser habilitado, al aplicar de nuevo el comando "**show mpls traffic-eng tunnels brief**" en la salida se diferencia que el túnel 3 no puedo habilitarse, esto se observa en la figura 4.77.

```
UIOLABPE1#sh mpls traffic-eng tunnels brief
Signalling Summary:
    LSP Tunnels Process:            running
    Passive LSP Listener:           running
    RSVP Process:                   running
    Forwarding:                     enabled
    Periodic reoptimization:        every 3600 seconds, next in 117 seconds
    Periodic FRR Promotion:         Not Running
    Periodic auto-bw collection:    every 300 seconds, next in 117 seconds
TUNNEL NAME                 DESTINATION     UP IF      DOWN IF    STATE/PROT
UIOLABPE1_t1                172.30.10.50    -          Gi1/26     up/up
UIOLABPE1_t3                172.30.10.50    -          unknown    up/down
Displayed 2 (of 2) heads, 0 (of 0) midpoints, 0 (of 0) tails
```

Figura 4.77: AB requerido por un túnel TE vs AB reservado en las interfaces.

El comando ***show mpls traffic-eng tunnels destination [ip-address]*** muestra la información del estado de los túneles TE configurados hacia un destino, además muestra los parámetros asociados con los túneles, un ejemplo de la ejecución del comando se presenta en la figura 4.78, el resultado se presenta únicamente para el túnel 1.

```
UIOLABPE1#show mpls traffic-eng tunnels destination 172.30.10.50

Name: UIOLABPE1_t1                          (Tunnel1) Destination: 172.30.10.50
  Status:
    Admin: up          Oper: up     Path: valid       Signalling: connected
    path option 1, type explicit LSP1 (Basis for Setup, path weight 20)

  Config Parameters:
    Bandwidth: 25     kbps (Global)  Priority: 0  0   Affinity: 0x0/0xFFFF
    Metric Type: TE (default)
    AutoRoute: disabled LockDown: disabled Loadshare: 25  bw-based
    auto-bw: disabled
  Active Path Option Parameters:
    State: explicit path option 1 is active
    BandwidthOverride: disabled  LockDown: disabled  Verbatim: disabled


  InLabel  :  -
  OutLabel : GigabitEthernet1/25, 19
  RSVP Signalling Info:
       Src 172.30.10.10, Dst 172.30.10.50, Tun_Id 1, Tun_Instance 115
    RSVP Path Info:
      My Address: 192.168.1.1
      Explicit Route: 192.168.1.2 192.168.1.14 172.30.10.50
      Record   Route:   NONE
      Tspec: ave rate=25 kbits, burst=10 bytes, peak rate=25 kbits
    RSVP Resv Info:
      Record   Route:  172.30.10.30(19) 172.30.10.50(0)
      Fspec: ave rate=25 kbits, burst=1000 bytes, peak rate=25 kbits
  History:
    Tunnel:
      Time since created: 2 hours, 55 minutes
      Time since path change: 2 hours, 19 minutes
      Number of LSP IDs (Tun_Instances) used: 115
    Current LSP:
      Uptime: 27 minutes, 48 seconds
      Selection: reoptimization
    Prior LSP:
      ID: path option 1 [113]
      Removal Trigger: re-route path verification failed
```

Figura 4.78: Ejemplo “show mpls traffic-eng tunnels destination ip-address”

En la figura 4.78 se puede observar que para el túnel 1 creado en el router UIOLABPE01, este se encuentra administrativamente y operacionalmente activo; su dirección de destino es la “172.30.10.50”; el tipo de LSP que usa es explícito y se denomina “LSP1”; muestra los parámetros de configuración del túnel (AB, AutoRoute, PathOption); la información de cómo se maneja el etiquetamiento MPLS para el túnel, en este caso se identifica a los paquetes del túnel 1 con un valor de etiqueta 19; informa la ruta LSP explicita que sigue el túnel 1 “192.168.1.2 , 192.168.1.14 , 172.30.10.50”; además muestra un historial del túnel en el que entre otros parámetros se muestra el tiempo de actividad del mismo.

En los túneles TE se utilizó la sentencia “tunnel mpls traffic-eng autoroute announce”, que permite al IGP tomar en cuenta al túnel en los cálculos SPF (Shortest Path First), habilitando el envío de tráfico sobre el túnel. En la figura 4.79 se presentarán las tablas de enrutamiento formadas por el IGP, donde se observa que los Túneles TE 1 y 3 se encuentran como entradas de dicha tabla.

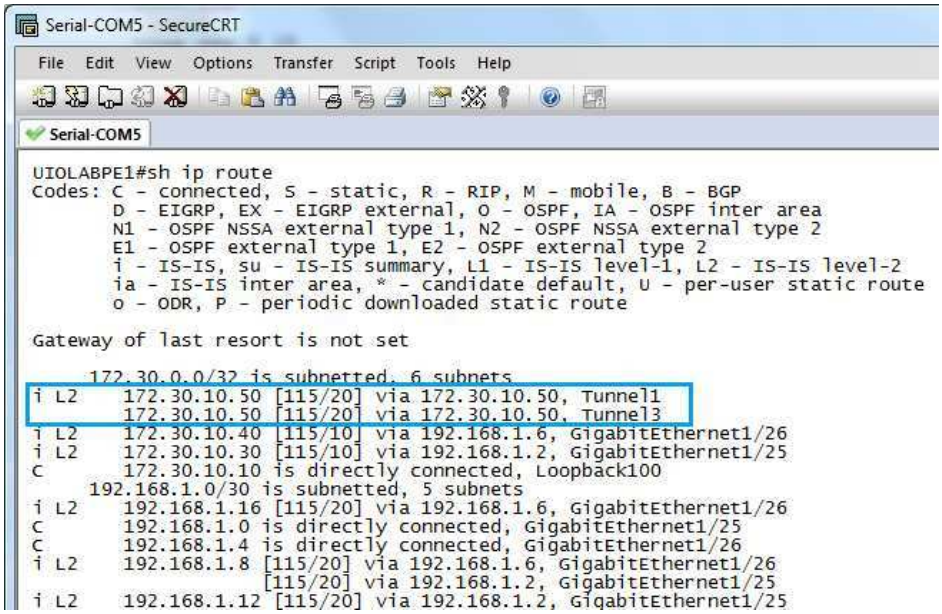


Figura 4.79: Túneles TE y calculo SPF del IGP

En la tabla de enrutamiento de "UIOLABPE1" mostrada en la figura 4.79 los Tuneles TE 1 y 3 se encuentran como el mejor camino para llegar al router "UIOLABPE2" de IP 172.30.10.50, ya que estas son las rutas de menor costo para llegar a dicho router, el IGP ve al túnel TE como una conexión punto a punto. En la figura 4.80 se observa que todo el tráfico dirigido hacia la red 172.30.10.50 se balancea por los dos túneles TE.

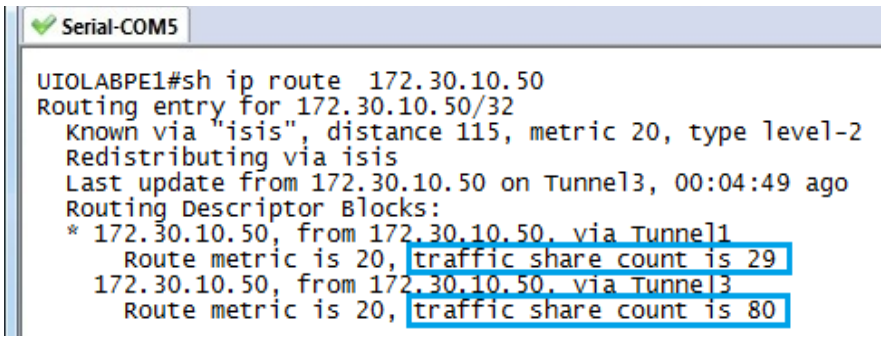


Figura 4.80: Balanceo de carga asimétrico por túneles TE

En la figura 4.80 se observa un balanceo asimétrico, esto se debe a que el ancho de banda reservado para los tuneles TE 1 y 3 es diferente. Para tener un balanceo simétrico por los dos túneles, se procede a configurar un AB igual tanto en el túnel 1 y 3 (69 kbps), si se revisa el balanceo de carga al destino 172.30.10.50 luego de haber cambiado los AB, se observa que el balanceo de carga se realiza de forma simétrica, esto se muestra en la figura 4.81.

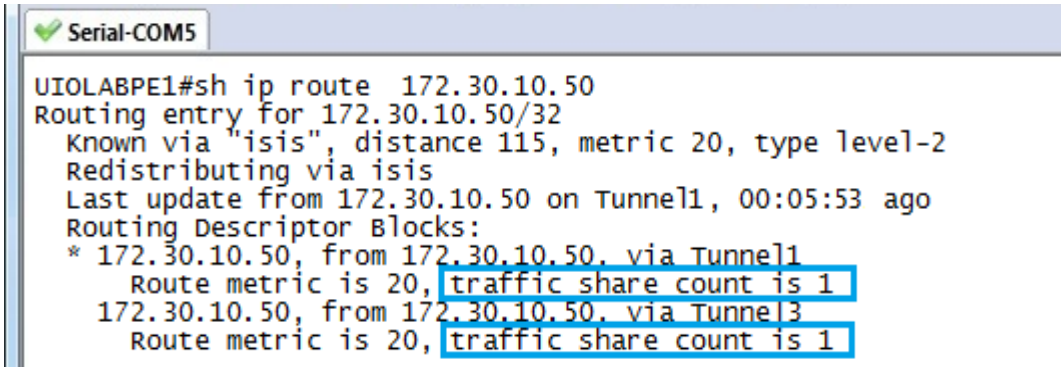


Figura 4.81: Balanceo de carga con costo igual por túneles TE

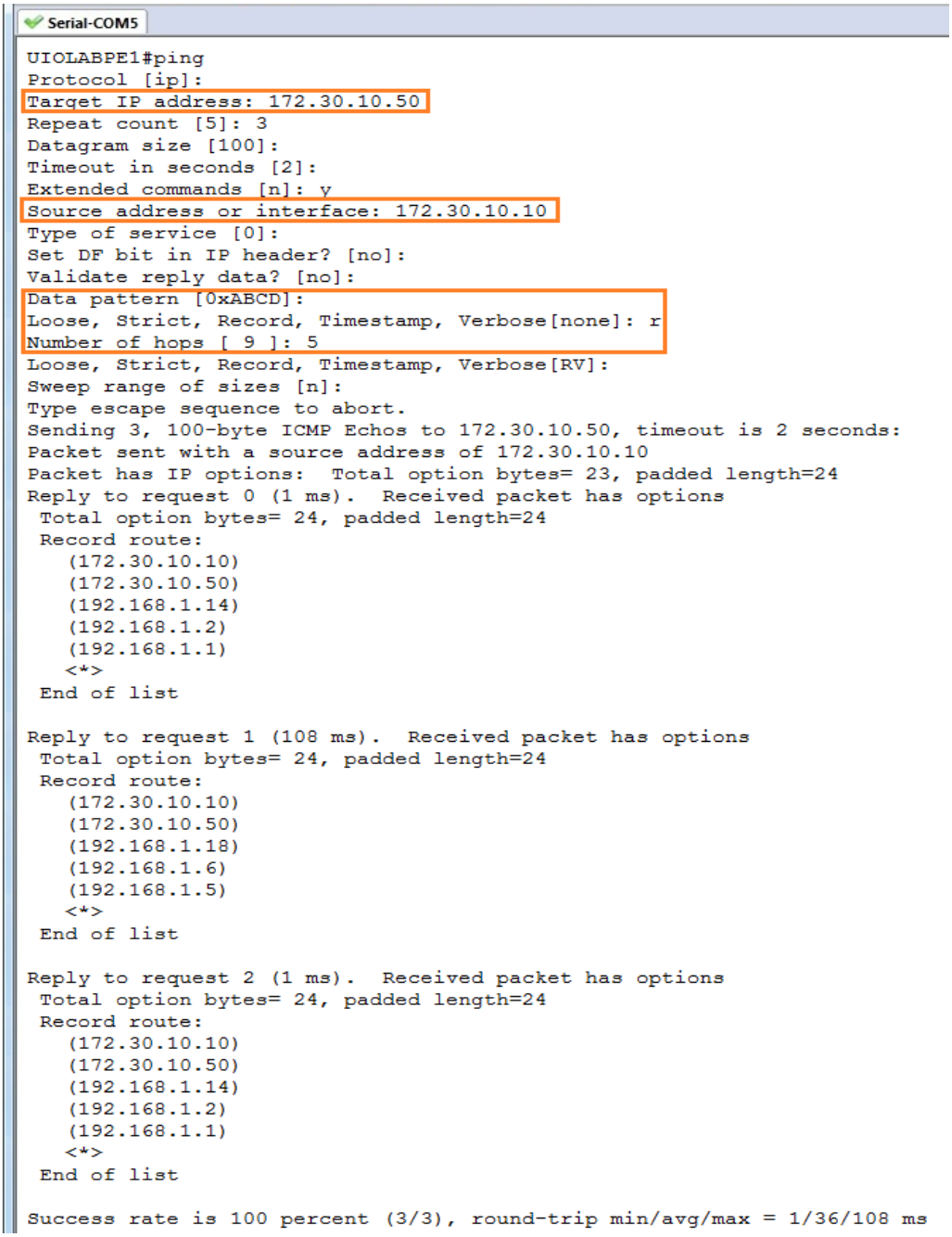


Figura 4.82: Ping extendido (Comprobación Tunel TE)

Otra de las pruebas que se realizó para comprobar el funcionamiento de los túneles TE fue realizar un ping extendido, el ejemplo se muestra en la figura 4.82, en esta se observa la ejecución de un ping extendido hacia el destino del túnel (172.30.10.50), se utiliza como dirección de origen la IP del router UIOLABPE1 (172.30.10.10), se establece que grabe el patrón que siguen los datos (saltos), el número de saltos máximo a grabar es 5.

En la figura 4.82 se observa el resultado del ping extendido. Los mensajes icmp de solicitud alcanzan su destino en un salto de la 172.30.10.10 a la 172.30.10.50, en cambio los mensajes ICMP de respuesta pueden tomar las rutas establecidas por el IGP, una ruta sigue los saltos 192.168.1.14, 192.168.1.2 , 192.168.1.1 y otra ruta sigue los saltos 192.168.1.18 , 192.168.1.6 , 192.168.1.5 (dos saltos para cada una), demostrando de esta manera que los Túneles TE simulan una conexión punto a punto unidireccional, enviando tráfico en un solo sentido.

Como siguiente fase en el análisis de MPLS TE, se procederá a probar la otra funcionalidad de Ingeniería de Tráfico con MPLS, la cual permite proteger los enlaces ante problemas de funcionamiento, y tener la capacidad de restauración de un túnel principal con un túnel de respaldo previamente configurado en el punto de fallo.

Para esta prueba se protegerá el túnel TE 1 en el router UIOLABP01, en caso de que falle el enlace entre éste y UILABPE2, para lo cual se realizó la configuración adicional del comando “tunnel mpls traffic-eng fast-reroute” dentro de la configuración de la interfaz Tunnel1 en el router UIOLABPE1. Además se debe configurar el túnel de *backup* en el router UIOLABP2. La configuración se muestra a continuación:

```
! Creación del túnel TE de backup (destino 172.30.10.50, tipo lsp
! explícito ”backup”)
interface Tunnel10
 ip unnumbered Loopback100
 tunnel destination 172.30.10.50
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng autoroute announce
 tunnel mpls traffic-eng priority 5 5
 tunnel mpls traffic-eng path-option 1 explicit name backup
!
```

```
! Interfaz a la que se desea proteger, indicándole que el túnel
! de respaldo es el Tunnel10
interface GigabitEthernet2/2
 ip address 192.168.1.13 255.255.255.252
 ip router isis
 speed nonegotiate
 mpls traffic-eng tunnels
 mpls traffic-eng backup-path Tunnel10
 mpls label protocol ldp
 mpls ip
 isis circuit-type level-2-only
 isis network point-to-point
 ip rsvp bandwidth 5000 5000
!
! Creación del LSP explicito asociado al túnel.
!
ip explicit-path name backup enable
 next-address 192.168.1.10
 next-address 192.168.1.18
 next-address 172.30.10.50
```

En esta configuración se observa que el túnel de respaldo creado es el Tunnel10, el cual sigue un LSP explícito denominado "*backup*" mostrado en la configuración. Una configuración adicional es la de configurar el comando "mpls traffic-eng backup-path Tunnel10" dentro de la interfaz perteneciente al enlace a proteger, este comando realiza la conmutación al túnel de respaldo en caso de que el enlace falle.

Para las siguientes pruebas las reservas de AB en las Interfaces serán de 5000 kbps, el requerimiento para el túnel 1 se cambió a 1000 kbps y el del túnel 3 se mantuvo en los 69 kbps.

A continuación se muestran los comandos de comprobación de FRR que permiten verificar que la protección de enlaces funciona.

El comando ***show mpls traffic-eng fast-reroute database*** muestra la base de datos de Fast Reroute, en la que se indica el estado de los túneles de TE y de los túneles de backup. En el caso de no estar en uso un túnel TE de backup este se encontrará en estado "*ready",* cambiando al estado "*active"* si se encuentra en uso, este comando solo mostrará resultados en el lugar donde se tenga configurado túneles de respaldo. En la figura 4.83 se observa el resultado del comando ejecutado en el router UIOLABP2.

```
UIOLABP2#show mpls traffic-eng fast-reroute database
Headend frr information:
Protected tunnel               In-label Out intf/label   FRR intf/label   Status

LSP midpoint frr information:
LSP identifier                 In-label Out intf/label   FRR intf/label   Status
172.30.10.10 1 [115]           19       Gi2/2:implicit-n Tu10:implicit-nu ready
UIOLABP2#
```

(a)

```
UIOLABP2#sh mpls traffic-eng fast-reroute database
Headend frr information:
Protected tunnel               In-label Out intf/label   FRR intf/label   Status

LSP midpoint frr information:
LSP identifier                 In-label Out intf/label   FRR intf/label   Status
172.30.10.10 1 [129]           25       Gi2/2:implicit-n Tu10:implicit-nu active
```

(b)

Figura 4.83: Comprobación de la protección de Enlaces con TE

En la figura 4.83 se muestra el resultado de la ejecución del comando “show mpls traffic-eng fast-reroute database”, en dos momentos diferentes, en el primer instante mostrado en la figura 4.83(a) el túnel de respaldo Tunnel10 se encuentra en estado *ready* es decir que se encuentra listo para actuar en el caso de que falle el enlace de la interfaz Gi2/2, en el segundo momento mostrado en la figura 4.83(b) el túnel de respaldo se encuentra en el estado *active* debido a que entro en funcionamiento para restaurar al túnel TE 1 por un error en el enlace de la interfaz Gi2/2, esto se logró al desconectar la interfaz Gi2/2 para simular una caída de enlace, además esto se probó mientras se realizaba un ping de varias repeticiones sobre el túnel Tunnel1 mostrado en la figura 4.84, comprobando que la restauración era inmediata sin pérdida de paquetes.

```
UIOLABPE1#ping 172.30.10.50 repeat 1000

Type escape sequence to abort.
Sending 10000, 100-byte ICMP Echos to 10.10.1.13, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 1/2/64 ms
```

Figura 4.84: Prueba de PING para comprobar FRR

Como una prueba adicional se requirió buscar la alternativa al comando “tunnel mpls traffic-eng autoroute announce”, debido a que con este comando todos los prefijos o redes, que se originan en el router de destino del túnel TE, son anunciados vía al túnel, lo cual no es óptimo porque solo ciertas redes de mayor importancia, o que transporten información crítica deben ser llevadas por el túnel.

En la prueba se quiere utilizar los túneles TE para transportar la información de ciertas instancias VRF, creadas en los routers PE, lo cual no sucedía con “tunnel mpls traffic-eng autoroute announce”; ya que el tráfico de toda VRF creada entre estos routers se enviaba por el túnel creado entre los mismos. Como una opción se pensó en crear rutas estáticas de la forma: “**ip route vrf** vrf_name x.x.x.x 255.255.255.255 TunnelX” lo cual no tuvo éxito, ya que entre los sitios extremos se perdía conectividad.

Para solucionar el problema de envío de tráfico sobre el túnel se buscó otra alternativa, cuya búsqueda llevó al uso de un atributo de BGP dentro de la configuración de una instancia VRF, el cual es “bgp next-hop Loopback XXX”, permitiendo que se force a utilizar como siguiente salto en las actualizaciones de MP-BGP la loopback XXX, y no la loopback configurada en BGP para las actualizaciones, es decir que para el caso de las VRFs la dirección de siguiente salto para las actualizaciones MP-BGP será una loopback distinta a la loopback compartida (loopback100) usada en la configuración global de BGP.

A continuación se muestra un ejemplo de la configuración realizada con este nuevo atributo:

```
! Creación de una VRF en la que se forzó que utilice como next
! hop a la dirección de la loopback20.
ip vrf customerA
 rd 1:100
 route-target export 1:100
 route-target import 1:100
 bgp next-hop Loopback20
!
interface Loopback20
 ip address 172.30.20.10 255.255.255.255
!
! Creación de una ruta estática que permite alcanzar la dirección
! de la loopback20 vía el túnel de TE “Tunnel1”.
!
```

```
ip route 172.30.20.50 255.255.255.255 Tunnel1
```

En esta configuración se muestran las variaciones con respecto a la ya explicada forma de configuración de las VRF, se observa que para la vrf customerA del ejemplo, la dirección utilizada para las actualizaciones MP-BGP es la de la loopback20 y no la de la loopback100.

Como no se debe publicar las redes de la loopback 20 por ISIS, se debe configurar una ruta estática, que permita enviar los paquetes dirigidos a esta red mediante el túnel. Para realizar la prueba se utilizó el túnel Tunnel1 creado en UIOLABPE1, con destino a UIOLABPE2 y se creó un túnel Tunnel2 en UIOLABPE2 con destino a UIOLABPE1, las configuraciones para UIOLABPE2 son:

```
! Crea una interfaz túnel TE de backup
!
interface Tunnel2
 ip unnumbered Loopback100
 mpls ip
 tunnel destination 172.30.10.10
 tunnel mode mpls traffic-eng
 tunnel mpls traffic-eng priority 0 0
 tunnel mpls traffic-eng bandwidth  50000
 tunnel mpls traffic-eng path-option 1 explicit name LSP2
 tunnel mpls traffic-eng fast-reroute
 ip rsvp bandwidth 50000
!
! Se crea un LSP explícito para asociarlo al túnel de backup
ip explicit-path name LSP2 enable
 next-address 192.168.1.13
 next-address 192.168.1.1
 next-address 172.30.10.10
!
! Crea la VRF customerA asociada el túnel TE
ip vrf customerA
 rd 1:100
 route-target export 1:100
 route-target import 1:100
 bgp next-hop Loopback20
!
interface Loopback20
 ip address 172.30.20.50 255.255.255.255
!
ip route 172.30.20.10 255.255.255.255 Tunnel2
```

El resto de configuraciones, como el protocolo entre el PE y CE, la asociación de una VRF a una interfaz, y la redistribución de las rutas por MP-BGP siguen siendo

las mismas que las mostradas en las pruebas de VPN capa 3. Además se crea una VRF “data” de la forma común sin asociarla a un bgp-next hop diferente sino que esta trabajará con la loopback compartida. Para verificar dichas configuraciones a continuación se presentan algunas pruebas:

Serial-COM5

```
UIOLABPE1#sh ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.30.0.0/32 is subnetted, 6 subnets
i L2    172.30.10.50 [115/20] via 192.168.1.6, GigabitEthernet1/26
                     [115/20] via 192.168.1.2, GigabitEthernet1/25
i L2    172.30.10.40 [115/10] via 192.168.1.6, GigabitEthernet1/26
i L2    172.30.10.30 [115/10] via 192.168.1.2, GigabitEthernet1/25
C       172.30.10.10 is directly connected, Loopback100
C       172.30.20.10 is directly connected, Loopback20
S       172.30.20.50 is directly connected, Tunnel1
     192.168.1.0/30 is subnetted, 5 subnets
i L2    192.168.1.16 [115/20] via 192.168.1.6, GigabitEthernet1/26
C       192.168.1.0 is directly connected, GigabitEthernet1/25
C       192.168.1.4 is directly connected, GigabitEthernet1/26
i L2    192.168.1.8 [115/20] via 192.168.1.6, GigabitEthernet1/26
                    [115/20] via 192.168.1.2, GigabitEthernet1/25
i L2    192.168.1.12 [115/20] via 192.168.1.2, GigabitEthernet1/25
UIOLABPE1#sh ip route vrf customerA

Routing Table: customerA
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 4 subnets
C       10.10.1.8 is directly connected, Loopback10
B       10.10.1.12 [200/0] via 172.30.20.50, 00:33:19
C       10.10.1.0 is directly connected, GigabitEthernet1/1
B       10.10.1.4 [200/0] via 172.30.20.50, 00:33:19

UIOLABPE1#
UIOLABPE1#sh ip route vrf data

Routing Table: data
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/30 is subnetted, 3 subnets
B       10.10.2.8 [200/0] via 172.30.10.50, 00:31:47
C       10.10.2.0 is directly connected, Loopback30
B       10.10.2.4 [200/0] via 172.30.10.50, 00:31:47
UIOLABPE1#
```

Figura 4.85: Tablas de Enrutamiento (VRF sobre túnel TE)

La primera de las pruebas es verificar la creación de las VRFs, como se mostró en las pruebas de VPN capa 3, dichas pruebas no se mostrarán en este tema, la prueba que se muestra en la figura 4.85 es la revisión de las tablas de enrutamiento, se muestra la tabla global y la tabla específica de cada una de las VRFs, con el fin de demostrar que los paquetes de “customerA” siguen el camino del túnel y los de “data” un camino establecido por el IGP.

Como se señala en la figura 4.85 en la tabla de enrutamiento de la vrf customerA las rutas aprendidas desde el sitio remoto se aprenden vía 172.30.20.50, que es la dirección de la loopback20 configurada en el router PE remoto, si esta IP se revisa en la tabla de enrutamiento global se puede observar que esta tiene una entrada estática vía el túnel Tunnel1, es decir que el tráfico de “customerA” generado en el router UIOLABPE1 y dirigido hacia el sitio remoto ubicado en el router UIOLABPE2 será enviado mediante el túnel Tunnel1.

En cambio si se revisa la tabla de enrutamiento de la vrf “data”, las rutas aprendidas desde el sitio remoto se aprenden vía 172.30.10.50, que es la dirección de la loopback100 (loopback compartida por el proceso bgp para sus actualizaciones) configurada en el router PE remoto, si esta IP se revisa en la tabla de enrutamiento general se puede observar que esta tiene dos rutas aprendidas por el IGP ISIS, demostrando que el tráfico de esta VRF se envía por las rutas aprendidas por ISIS y no sobre un túnel TE.

En la figura 4.86 se presentan las pruebas de conectividad para cada una de las VRFs con el uso de los comandos ping y traceroute.

En la figura 4.86 se puede observar que tanto las redes de la VRF customerA como las redes de la VRF data poseen conectividad, pero para el caso de las redes de la VRF customerA estas solo tienen un salto, ya que utilizan los túneles de TE, dando la apariencia de una red punto a punto, lo que se observa al hacer un traceroute a una de su redes remotas, como se muestra en el recuadro azul.

En cambio que para las redes de la VRF data se tiene varios saltos y dos opciones de ruta establecidas por el IGP ISIS, como lo indicaba la tabla de enrutamiento, esto se observa en el recuadro anaranjado.

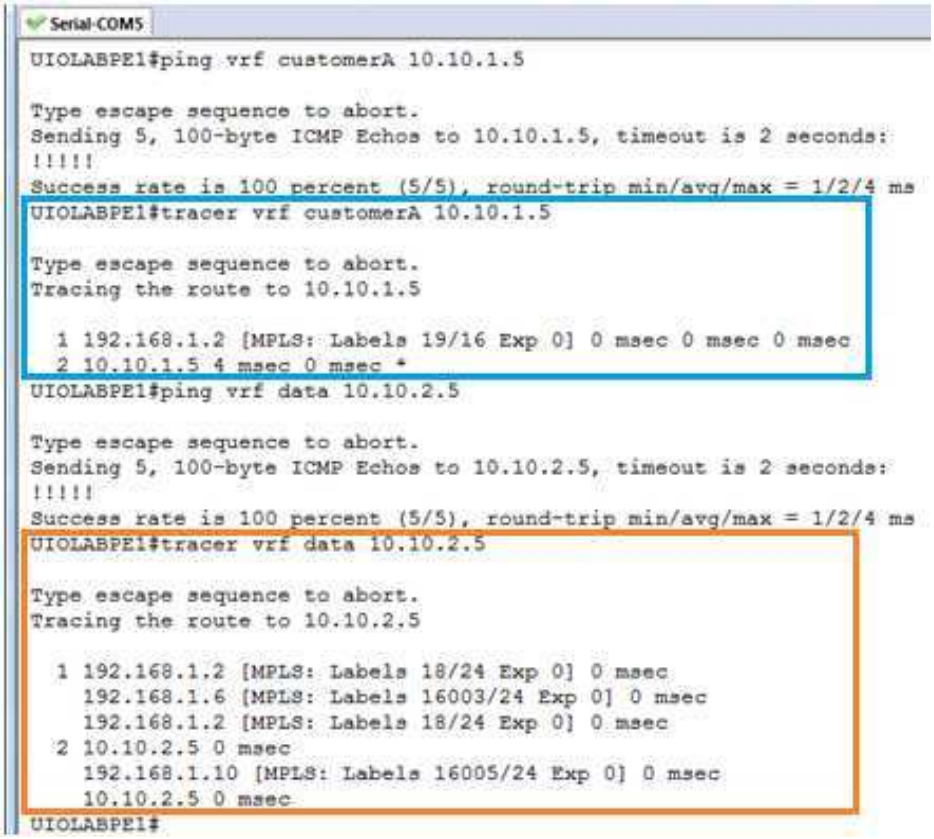


Figura 4.86: Pruebas de conectividad VRFs

4.7 VERIFICACIÓN DE LA OPERACIÓN DE MULTICAST SOBRE MPLS. [37] [40]

Esta prueba se encuentra basada en la topología de habilitación de un *backbone* MPLS, para sobre este montar el funcionamiento de multicast. A continuación se presentan unos ejemplos de la configuración de multicast aplicados en el backbone tanto para los routers con sistema IOS como para los routers con sistema IOS XR.

```
!IOS “UIOLABE01”
!Habilitacion de enrutamiento
!multicast
ip multicast-routing
ip multicast multipath
!
interface Loopback100
 ip address 172.30.10.10
255.255.255.255
!Habilita pim en modo sparse
!sobre las interfaces que manejan
!trafico multicast
 ip pim sparse-mode
!
interface GigabitEthernet1/1
 ip address 192.168.100.2
```

```
!IOS XR “UIOLABP01”
!Habilitacion de enrutamiento
!multicast
multicast-routing
 address-family ipv4
  interface Loopback100
   enable
  !
  interface GigabitEthernet0/0/1/0
   enable
  !
  interface GigabitEthernet0/0/1/1
   enable
!
!Habilita pim en modo sparse
!sobre las interfaces que manejan
```

```
255.255.255.252
 ip pim sparse-mode
!
!
interface GigabitEthernet1/25
 ip address 192.168.1.1
255.255.255.252
 ip pim sparse-mode
 ip router isis
 speed nonegotiate
 mpls label protocol ldp
 mpls ip
 isis network point-to-point
!Configura el punto de
!distribución del arbol multicast
ip pim rp-address 172.30.10.10
```

```
!trafico multicast
router pim
 address-family ipv4
!Configura el punto de
!distribución del arbol multicast
rp-address 172.30.10.10
  log neighbor changes
  interface Loopback100
   enable
  !
  interface GigabitEthernet0/0/1/0
   enable
  !
  interface GigabitEthernet0/0/1/1
   enable
  !
```

A continuación se presentarán las pruebas y resultados obtenidos al configurar Multicast sobre la topología del backbone MPLS.

El comando ***show ip pim neighbor*** permite mostrar una lista de las adyacencias PIM activas que se tienen con otros vecinos PE o P routers.

```
UIOLABE01#show ip pim neighbor
PIM Neighbor Table
Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      P - Proxy Capable, S - State Refresh Capable, G - GenID Capable
Neighbor          Interface                Uptime/Expires    Ver   DR
Address                                                            Prio/Mode
192.168.1.2       GigabitEthernet1/25      00:23:11/00:01:23 v2    1 / DR G
```

Figura 4.87: Salida del comando “show ip pim neighbor”

En la figura 4.87 se muestra un ejemplo del resultado de la ejecución del comando “*show ip pim neighbor*” en el router UIOLABE01, se muestra que ha descubierto un vecino PIM por la interfaz GigabitEthernet1/25, la dirección IP del vecino PIM es 192.168.1.2; el tiempo que dicho vecino se encuentra en funcionamiento, es de 00:23:11; el tiempo antes de que el vecino agote el timer de espera (00:01:23) por un mensaje PIM Hello, que indique que el vecino sigue activo; la versión de PIM que utiliza el vecino.

En el caso de la prueba se encuentra manejando la versión 2 de PIM; la prioridad y modo de operación del router designado, para el ejemplo este tiene una prioridad de 1 la cual es establecida por defecto, se encuentra en modo router designado. Este comando se utiliza para verificar que todos los vecinos PIM se encuentren activos, utilizando el modo y versión correcta, la variante de este comando en un sistema IOS XR es “*show pim neighbor*”.

Otro de los comandos que nos permiten verificar que interfaces se encuentran configuradas con PIM, su modo de operación (*sparse* o *dense*), su versión, prioridad, el número de vecinos descubiertos y el router designado DR es el comando ***show ip pim interface***.

```
UIOLABE01#
UIOLABE01#show ip pim interface

Address          Interface                Ver/   Nbr    Query  DR     DR
                                          Mode   Count  Intvl  Prior
172.30.10.10     Loopback100              v2/S   0      30     1      172.30.10.10
192.168.100.2    GigabitEthernet1/1       v2/S   0      30     1      192.168.100.2
192.168.1.1      GigabitEthernet1/25      v2/S   1      30     1      192.168.1.2
UIOLABE01#
```

Figura 4.88: Salida del comando “show ip pim interface”

En la figura 4.88 se muestra el resultado de la ejecución de dicho comando, se observa que para el router UIOLABE01 se ha habilitado PIM en tres interfaces, “Loopback100, gi1/1 y gi1/25”, cuyas direcciones IP son 172.30.10.10, 192.168.100.2 y 192.168.1.1 respectivamente, se encuentran funcionando con la versión 2 de PIM y en modo *sparse* “V2/S”, se ha hallado un vecino PIM por la interfaz GI1/25 ya que en el campo “Nbr Count” se tiene un valor de 1 para esta interfaz; la prioridad del router designado es de 1 para todas las interfaces, por lo que para elegir la IP que identifica al DR se usa la dirección más alta configurada en el router.

El comando ***show ip pim rp*** muestra los puntos activos de encuentro/distribución de los árboles creados (RP), que se encuentran almacenados con sus entradas respectivas de enrutamiento multicast.

Serial-COM5

```
UIOLABE01#
UIOLABE01#show ip pim rp
Group: 239.255.255.250, RP: 172.30.10.10, next RP-reachable in 00:01:10
Group: 224.1.1.1, RP: 172.30.10.10, next RP-reachable in 00:00:26
Group: 224.0.1.40, RP: 172.30.10.10, next RP-reachable in 00:01:14
UIOLABE01#
```

Figura 4.89: Salida del comando “show ip pim rp”

En la figura 4.89 se observa que para todos los grupos multicast el punto de encuentro RP es el mismo 172.30.10.10 esto es correcto ya que éste se configuró de forma manual con el comando “ip pim rp-address 172.30.10.10” para todos los grupos multicast y no de forma dinámica.

El comando ***show ip mroute*** *[group-name | group-address]* ***[source]*** ***[summary]*** ***[count]*** ***[active*** *kbps]*, muestra la información de las tablas de enrutamiento multicast, según el parámetro adicional que se use con el comando, éste permitirá mostrar una información en específico. Por ejemplo con el parámetro "summary" se muestra un resumen de cada una de las entradas de la tabla de enrutamiento, o de una fuente multicast especificada; "count" muestra estadísticas de un grupo o fuente multicast, como el número de paquetes, paquetes por segundo, la tasa promedio de paquetes y bits por segundo; "active" muestra las tasas de envío de fuentes activas hacia grupos de difusión multicast.

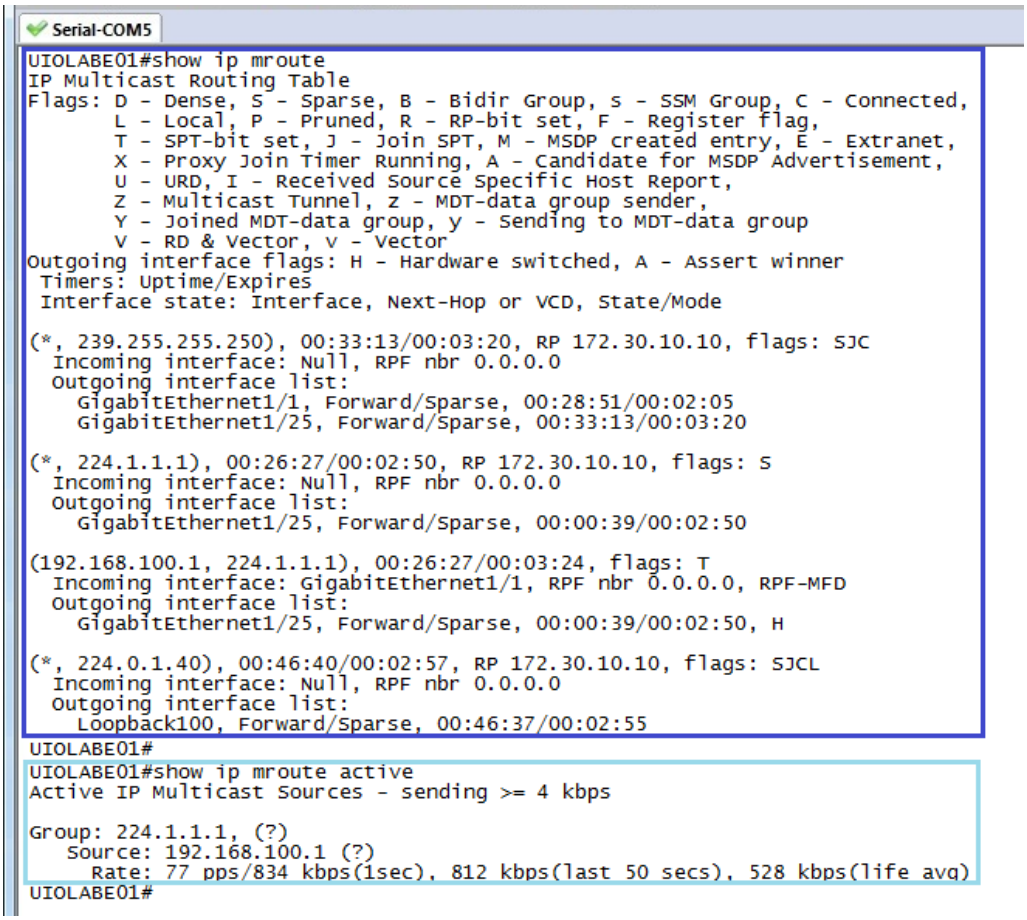


Figura 4.90: Salida del comando "show ip mroute [active]"

En la figura 4.90 en la primera sección se observa el resultado de la ejecución del comando "show ip mroute" ejecutado en el router UIOLABE01, se observan tres grupos multicast de la forma (*,G), donde el asterisco simboliza cualquier fuente y G el grupo multicast disponible, esto se debe a que la información de los grupos multicast es distribuida mediante el uso de un árbol compartido, llamado así

porque varias fuentes emisoras comparten el árbol de distribución, además se observa una entrada de la forma (S,G) donde S es la fuente, la entrada es (192.168.100.1 , 224.1.1.1), esto se debe a que cuando un receptor requiere la emisión de un grupo multicast, este determina una mejor ruta hacia la fuente, y envía un “join”, el cual se indica mediante el formato (S,G).

En la segunda sección señalada en la figura 4.90 se muestra la ejecución del comando “show ip mroute active” en el router UIOLABE01, muestra las emisiónes multicast activas. En el ejemplo se observa una transmisión activa para el grupo de difusión multicast 224.1.1.1, la fuente de difusión del grupo multicast es la dirección 192.168.100.1.

Las velocidades de transferencia son de 77paquetes por segundo, una tasa de transmisión en el último segundo de 834 kbps, y en los últimos 50 segundos a una velocidad de 812 kbps, para una velocidad de transmisión promedio de 528 kbps. Para los routers con un sistema IOS XR, los comandos “show ip mroute” son remplazados por los comandos “show mfib route” y “show mrib route”.

Para la difusión de un streaming vía multicast se hizo uso de la aplicación VLC (Video LAN Media Player), en la figura 4.91 se presentan las pantallas de configuración de VLC para emitir una transmisión de video dentro de un grupo multicast 224.1.1.1 en el puerto 1234.

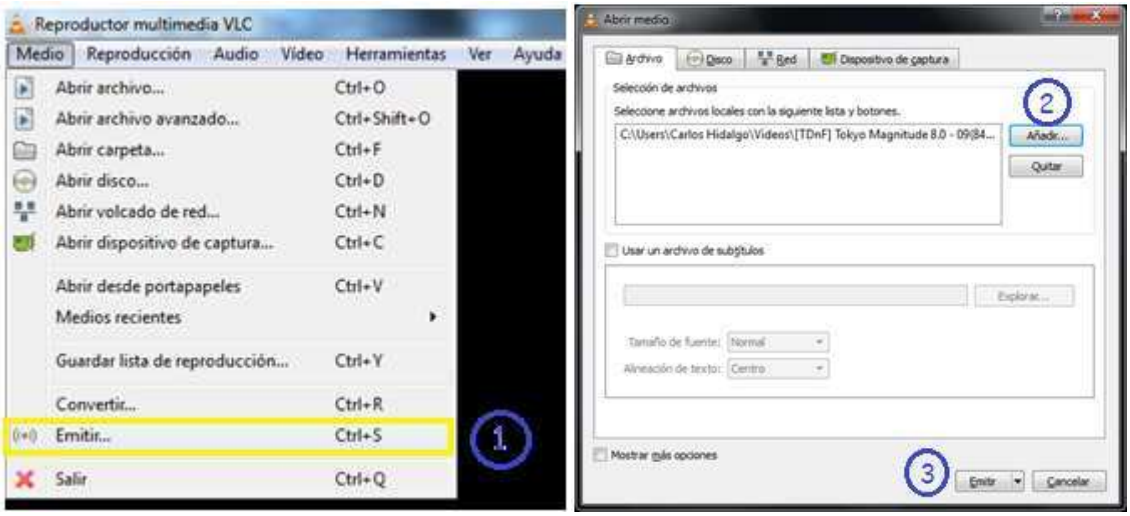


Figura 4.91: Configuración VLC server parte 1

Para poder empezar a configurar la transmisión, en el paso (1) se elige en el menú “Medio”, la opción emitir; que abre la pantalla mostrada en el paso (2) donde elegimos el archivo a transmitir; en el paso (3) se selecciona la opción emitir para pasar a configurar los parámetros de la transmisión, como la fuente a transmitir, el método de transmisión para los destinos, y parámetros opcionales como la configuración del tiempo de vida TTL para los paquetes multicast.

Figura 4.92: Configuración VLC server parte 2

En la pantalla del paso (4) mostrada en la figura 4.92 se comprueba el archivo a ser emitido desde la fuente en configuración, se elige siguiente y en la pantalla del paso (5) se elige el modo de transmisión de la fuente, para la prueba se elige la opción UDP (legacy) y se selecciona añadir.

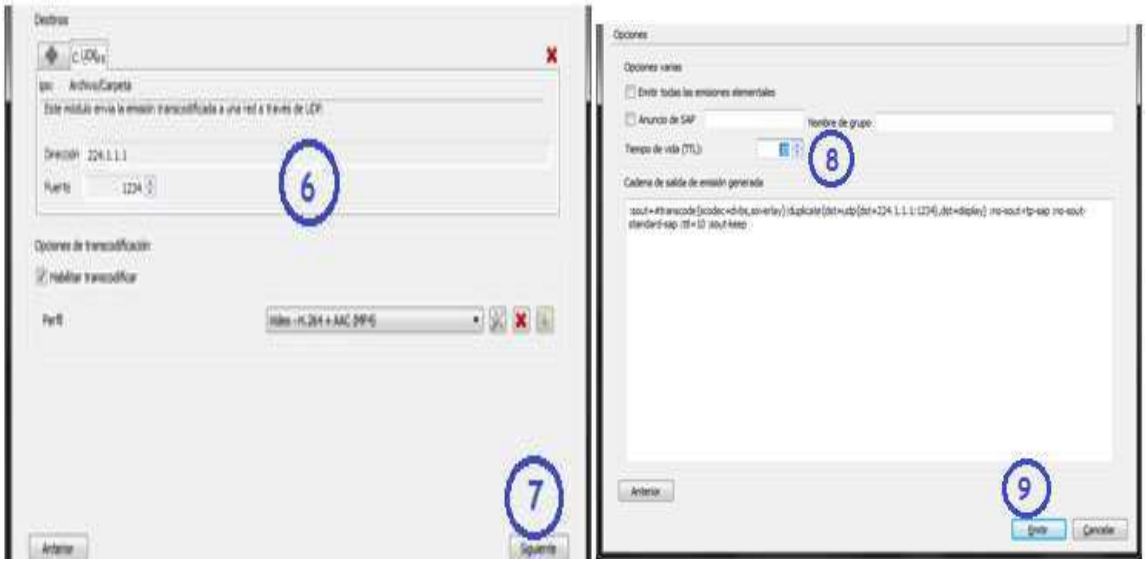


Figura 4.93: Configuración VLC server parte 3.

El siguiente paso (6) mostrado en la figura 4.93, se configura la IP del grupo multicast y el puerto de transmisión, los parámetros de configuración son “224.1.1.1:1234”, en el paso (7) se elige siguiente, para pasar a la pantalla de opciones, donde se manipula el valor TTL indicado en el paso (8), para que el paquete multicast pueda viajar sin problemas por el backbone MPLS. Este valor por defecto está establecido en 1 y no permitiría su transmisión por todo el backbone, ya que en su primer salto este seria descartado, en la prueba este valor fue establecido en 10, y como último paso (9) se selecciona emitir.

Para los receptores la configuración del VLC media player se muestra a continuación, donde el primer paso es seleccionar del menú Medio la opción “Abrir volcado de red” mostrado en la figura 4.94.

El siguiente paso (2) es configurar la URL de la fuente, la cual debe ser ingresada de la forma “udp://@224.1.1.1:1234”, para en el paso (3) seleccionar la opción reproducir.

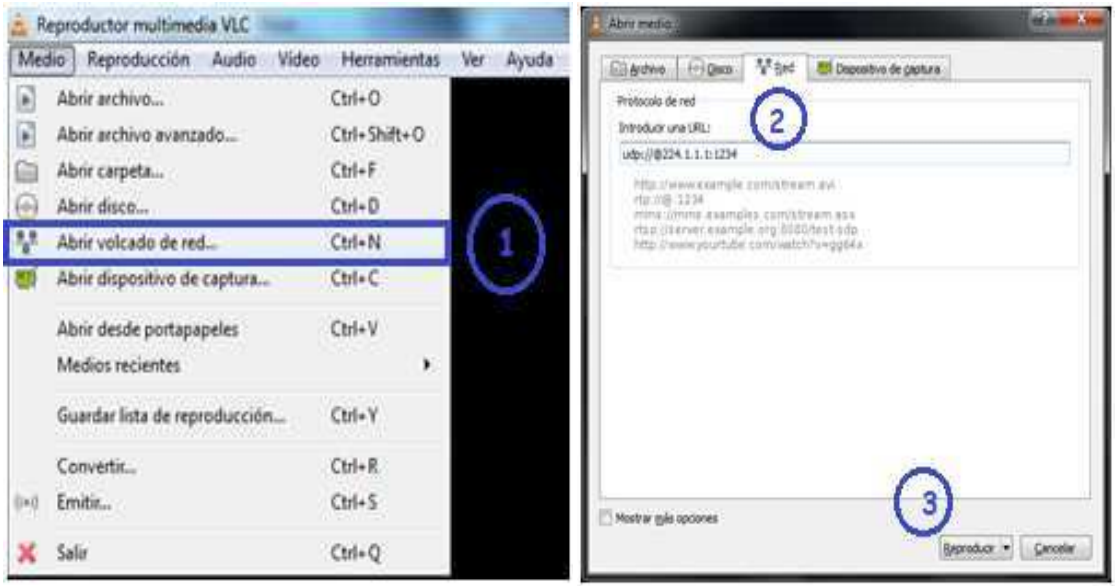


Figura 4.94: Configuración VLC cliente

A continuación en la figura 4.95 se presentan los resultados de la transmisión configurada:

Figura 4.95: Resultados

Como una prueba adicional se realizaron pruebas sobre el IPTV en desarrollo del backbone MPLS de CNT E.P, para lo cual se integro al backbone MPLS de CNT E.P, el equipo cisco 7609-S, algunas de las configuraciones no pueden ser mostradas debido a su grado de confidencialidad pero si se dará una idea de estas en la figura 4.97.

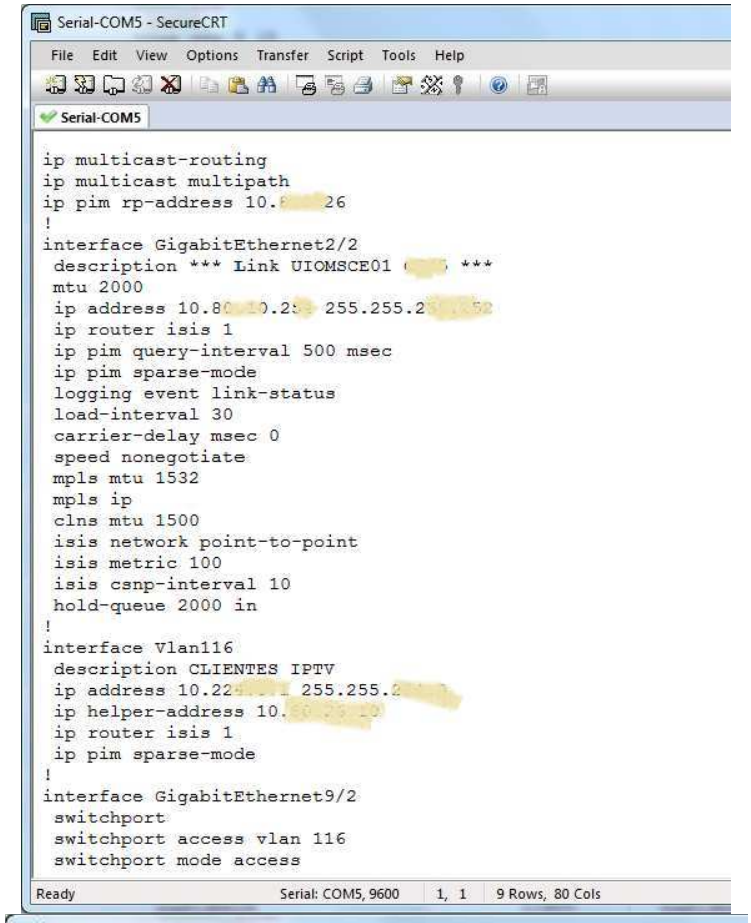


Figura 4.96: Configuraciones IPTV Cisco 7609

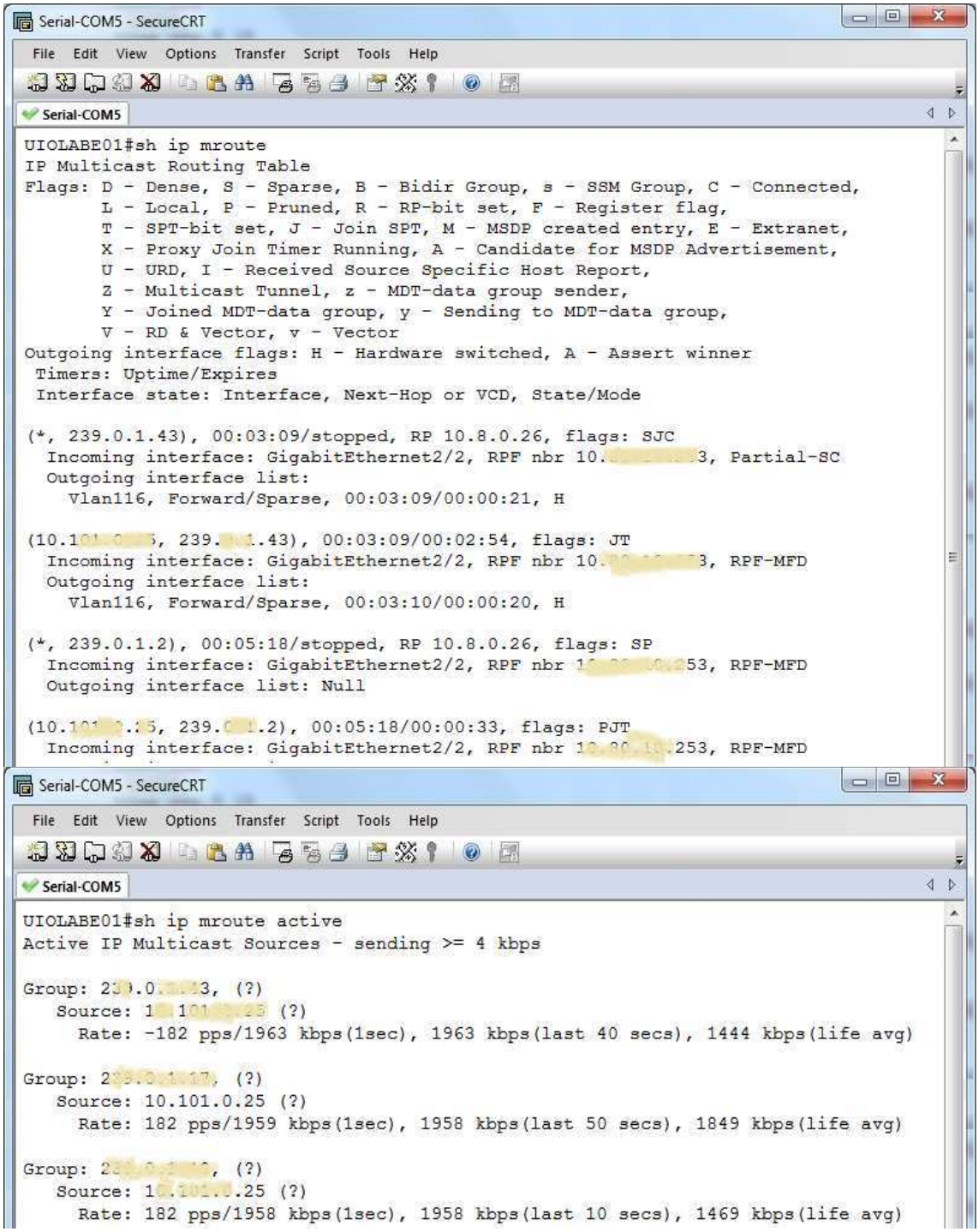


Figura 4.97: Pruebas de show ip mroute

En la figura 4.97 se muestra los resultados de la ejecución de comandos “show ip mroute” y “show ip mroute active” donde se encuentran grupos de difusión multicas en funcionamiento, y con transferencia de datos.

A continuación en la figura 4.98 se presentarán algunos de los resultados del funcionamiento de IPTV.

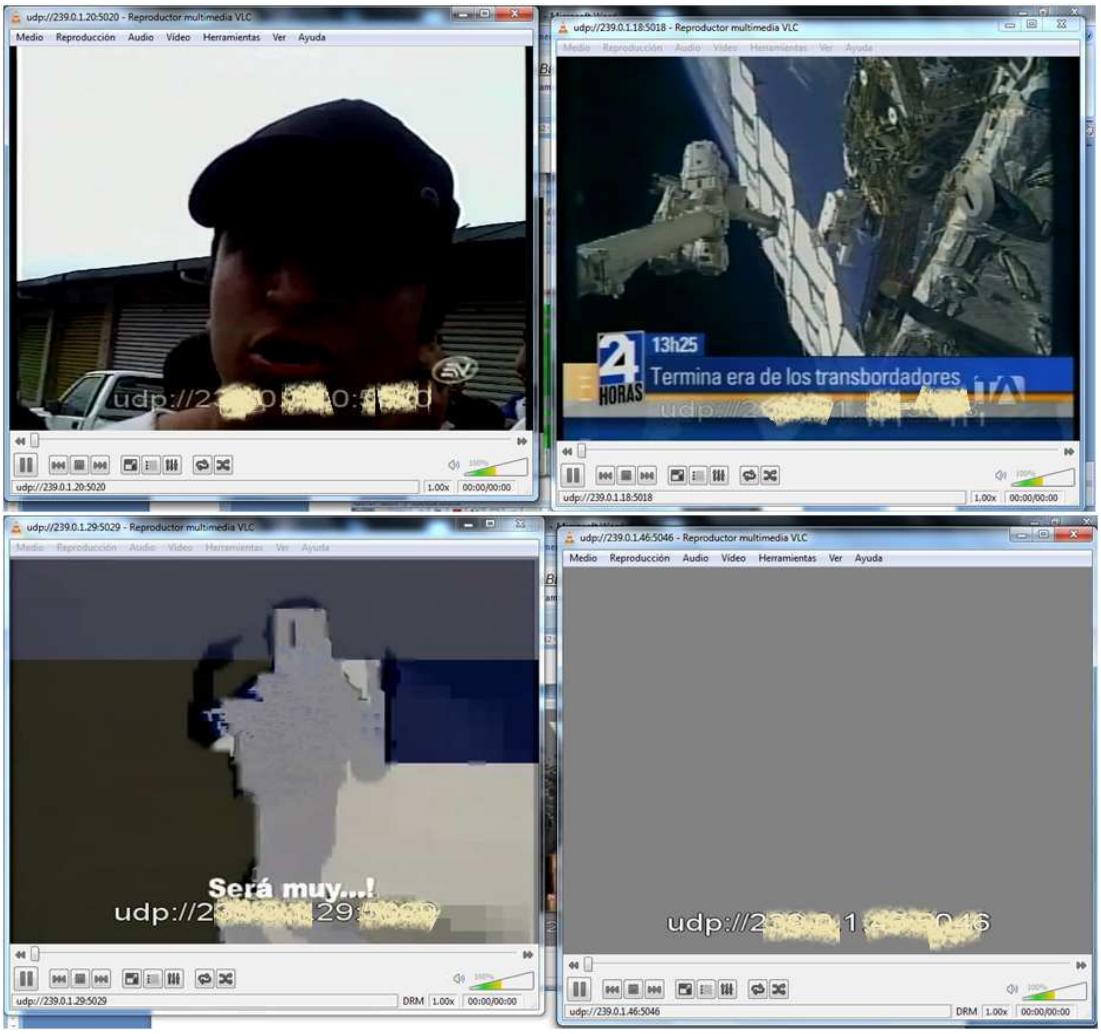


Figura 4.98: Pruebas de IPTV

En la figura 4.98 se muestran algunos de los canales de televisión implementados en el IPTV en desarrollo por CNT E.P, donde se observa que algunos de estos tienen una calidad óptima mientras que otros se encuentran muy distorsionados o demasiado pixeleadas por lo cual este producto sigue en desarrollo para corregir estas fallas.

4.8 PRUEBAS Y RESULTADOS DE *SERVICE INSTANCE* [15] [25]

Previo a la realización de las pruebas solicitadas por parte de CNT, es necesario realizar una comprobación inicial, que permita observar que el equipo 7600 del laboratorio se integro a la red MPLS nacional de la CNT E.P.

En la figura 4.99 se muestra el correcto establecimiento de la adyacencia ISIS con el equipo PE del nodo Mariscal (enmarcado en amarillo), necesaria para conocer las redes de CNT; se observa también el establecimiento de la sesión LDP (enmarcado en anaranjado), que habilita el intercambio etiquetas entre los routers, permitiendo que el equipo del laboratorio utilice MPLS.

Al observa el establecimiento de las sesiones se comprueba su integración a la red de CNT, para finalizar la comprobación se observo que en la tabla de enrutamiento se disponía de rutas, no se muestra la tabla de enrutamiento y en las direcciones IP de las sesiones se observa únicamente el último octeto, para proteger el direccionamiento IP de CNT que es confidencial.

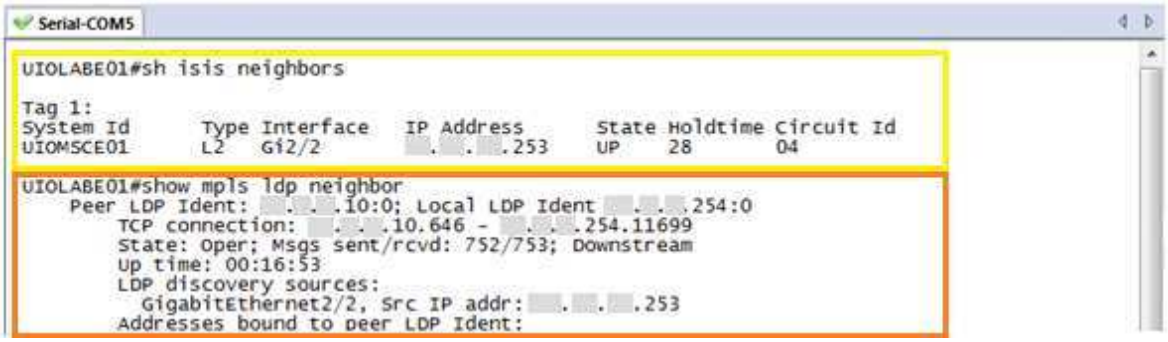


Figura 4.99: Establecimiento de sesiones IS-IS y LDP.

Después de comprobar el correcto funcionamiento de las configuraciones iniciales, lo siguiente es comprobar que el túnel de capa 2, creado entre el equipo del laboratorio y el equipo de Guayaquil, se encuentre funcionando. La comprobación del funcionamiento se muestra en la figura 4.100 donde se observa que el túnel con VC 2854 se encuentra en estado UP, esto indica que el túnel se estableció de manera adecuada y que se puede enviar los paquetes por la VPN.

Figura 4.100: Estado de la VPN.

A continuación se procedió a verificar el adecuado funcionamiento de las service instace creadas en UIOLABE01. Para realizar esto en las PC conectadas al switch UIOLABE02, se establecen sesiones PPPoE con el BRAS ubicado en Guayaquil, cada una de las PCs están ubicadas en VLANs diferentes, y la *service instance* configurada en UIOLABE01 será la encargada de realizar una agregación de capa 2. Permitiendo que los dos flujos sean parte de la interface VLAN 201, en esta interface VLAN se configura el túnel que permite comunicarse con el BRAS de Guayaquil. Las configuraciones que permiten realizar lo descrito son:

Configuración en el router UIOLABE01:

```
! Configuraciones que crean las service instance en Gi2/3,
! realizan la agregación del tráfico proveniente de UIOLABE02 de
! las VLAN 201 y 1436 en el bridge domain 201 de UIOLABE01
!
interface GigabitEthernet2/3
  mtu 2000
  no ip address
 service instance 201 ethernet
  encapsulation dot1q 201
  rewrite ingress tag pop 1 symmetric
  bridge-domain 201
 !
 service instance 1436 ethernet
  encapsulation dot1q 1436
  rewrite ingress tag pop 1 symmetric
  bridge-domain 201
 !
! A continuación la configuración de la interfaz VLAN 201 en la
! que se crea el túnel
!
interface Vlan201
 description PRUEBAS PPPOE LAB
 mtu 1900
 no ip address
 xconnect XX.XX.XX.100 2854 encapsulation mpls
!
```

Configuración en el router UIOLABE02:

```
! Configuración de la interfaz en la que se conecta la PC1 y se
! crea la sesión PPPoE1
!
interface GigabitEthernet1/3
 switchport
 switchport access vlan 201
```

```
 switchport mode access
! Configuración de la interfaz en la que se conecta la PC2 y se
! crea la sesión PPPoE2
!
interface GigabitEthernet1/4
 switchport
 switchport access vlan 1436
 switchport mode access
! Configuración de la interfaz en la que se conecta la interfaz
! del generador IXIA que simula al DSLAM1
!
interface GigabitEthernet1/5
 switchport
 switchport access vlan 1436
 switchport mode access
! Configuración de la interfaz en la que se conecta la interfaz
! del generador IXIA que simula al DSLAM2
!
interface GigabitEthernet1/6
 switchport
 switchport access vlan 201
 switchport mode access
!
! Configuración de la interfaz troncal por la que se envía el
! tráfico de las VLAN 201 y 1436 a UIOLABE02
!
interface GigabitEthernet1/25
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 201,1436
 switchport mode trunk
!
```

Configuración en el equipo de Guayaquil:

```
! Configuración de la interface VLAN en la que se crea el túnel
! para las pruebas.
!
interface Vlan2854
 description PRUEBAS PPPOE UIOLABE01
 mtu 1900
 no ip address
 xconnect XX.X.X.254 2854 encapsulation mpls
! Se añade la VLAN 2854 en el enlace que permite acceder al BRAS
! en guayaquil.
!
interface GigabitEthernet3/3
 description ### Link GYECNTB02 G1/0/2 hacia ACCESO ###
 switchport
 switchport trunk encapsulation dot1q
 switchport trunk allowed vlan 666,2410,2419-2424,2429,2551,2555,
2559,2563,257,12579,2583,2587,2591,2710,2720,2730,2731,2854
 switchport mode trunk
 speed nonegotiate
```

!

Para crear una conexión en Windows se hace lo siguiente en Internet Explorer, ir a Herramientas, en Opciones de Internet, escojo Conexiones y Configurar aquí se coloca el usuario y la contraseña y se realiza la conexión esto se observa en la figura 4.101.

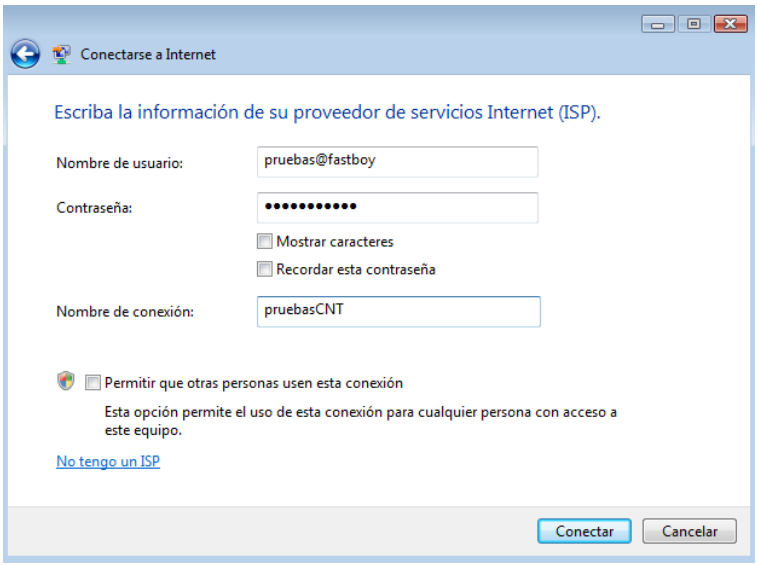


Figura 4.101: Creación de una sesión PPPoE

Una vez se establecieron las sesiones PPPoE como se observa en la figura 4.102 y se puedo navegar en internet desde las dos PCs se comprobó que las service instance funcionan de manera adecuada y que le túnel envía los paquetes a su destino.

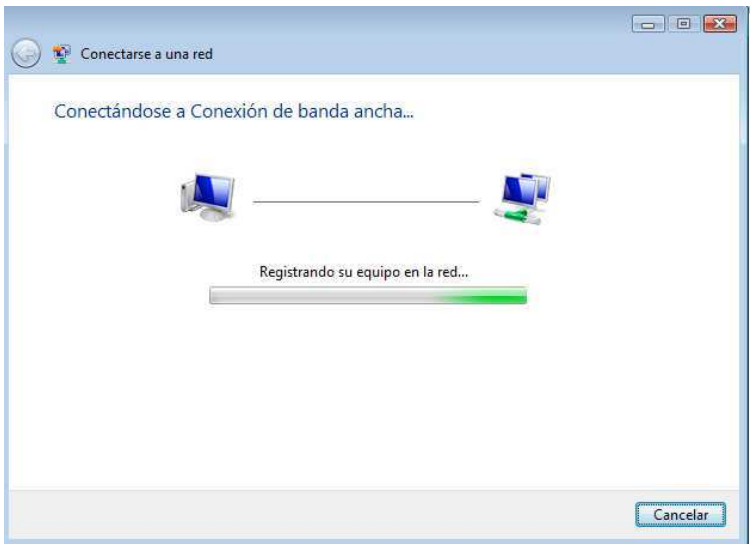


Figura 4.102: Establecimiento adecuado de la sesión PPPoE

El nombre de usuario y clave para acceder al BRAS fue proporcionado por CNT, estos permiten establecer las sesiones en cada PC, creándose una conexión de banda ancha PPPoE.

A continuación se procedió a realizar una MAC address flooding con el generador de tráfico, no se estableció un límite en el número máximo de direcciones, con lo cual se comprobó que se producía un ataque de denegación de servicios, pues las tablas MAC crecían sin control por lo que no se logró establecer la sesión PPPoE con el BRAS.

Una vez simulado el escenario más crítico se procedió a establecer un escenario más real, donde se disminuyo el número de MACs a generar en 1500 por cada interfaz del generador de tráfico, este es un número más adecuado de clientes que un DSLAM puede soportar, se procedió a limitar el tráfico máximo al 30 % de la capacidad total de 1Gbps de cada generador de tráfico ya que no se buscaba saturar el canal.

Una vez inundando con las direcciones MAC, se procedió a establecer de nuevo una sesión PPPoE, la cual se estableció de manera adecuada, comprobándose que la configuración de *service instance* es válida, y se puede aplicar en cualquier parte de la red, donde se desee realizar agregación de servicios, permitiendo de esta manera que CNT ofrezca una flexible conectividad de capa 2 para clientes corporativos como residenciales.

Una vez verificado el adecuado funcionamiento de las *service instance* en el laboratorio, se descarto que las nuevas configuraciones introducidas en el equipo 7600 de la localidad de Loja sean las que están generando el problema. En un inicio se pensó que las *service instance* no soportaban muchas direcciones MAC en la tabla y que esto causaba que los clientes no puedan establecer las sesiones PPPoE, al realizar estas pruebas se descarta un mal funcionamiento de estas configuraciones y se procede a revisar los otros elementos de la red (DSLAMs, Transmisión, BRAS), no se muestra la solución dada debido a que estos elementos son administrados por otras aéreas de la CNT a las que no se tuvo acceso.

4.9 TROUBLESHOOTING

4.9.1 TROUBLESHOOTING VPN CAPA 2 [6] [23]

En esta parte se pretende mostrar cómo realizar la corrección de errores para las VPN de capa 2, específicamente para las que permiten ofrecer conexiones punto a punto, cuyas pruebas y configuraciones fueron mostradas en una sección previa de este capítulo.

El primer paso para realizar el *troubleshooting* es tratar de descubrir la falla verificando el estado de la conexión virtual, usando el comando **show mpls l2transport vc** y sus variantes, esto se mostró en las pruebas de VPN capa 2, a continuación se resume las condiciones que deben cumplirse para que una conexión virtual se considere activa:

- Las interfaces en las en las que se configura el túnel deben estar activas.
- Que exista la etiqueta que se crea por el IGP.
- Que se tenga la etiqueta que identifica al circuito virtual.

Para que estas condiciones se cumplan se debe tener configurado de manera adecuada el IGP, el protocolo de distribución de etiquetas y habilitado MPLS en las interfaces, la manera de comprobar esto se fueron mostrando a lo largo del capítulo por lo que no se detallará sobre el tema.

Al usar la variante **show mpls l2transport vc detail,** si en la parte de MTU se tiene “remote unknow”, dos de las posibles causas que producen este mensaje son un desajuste en el MTU o que las interfaces remotas estén caídas. Se debe verificar que el MTU en los extremos sea el mismo.

En caso que lo anterior este correcto y el túnel continúe abajo se debe comprobar que se esté haciendo un adecuado intercambio de etiquetas, para esto se usa **show mpls forwarding-table**, si en el campo que corresponde a la etiqueta de salida se observa la palabra untagged, indica que no se están intercambiando las etiquetas. Algunas de las causa para que esto se produzca son que MPLS no está habilitado en la interfaz, o que CEF está deshabilitado.

Por lo que se debe comprobar la adecuada habilitación de MPLS en las interfaces, para realizar esto se usa el comando **show mpls interfaces** y para ver el funcionamiento de CEF el comando **show ip cef**.

Adicional a lo anteriormente mostrado también se disponen de comandos debug que permiten realizar operaciones de depurado para corregir errores de configuración, estos son:

- El **debug mpls l2transport signaling message** se usa para comprobar que el tipo de VC sea el adecuado, si se usa subinterfaces con encapsulamiento dod1Q debe ser VC type 4, si se usa directamente en las interfaces debe ser vc type 5.
- El **debug acircuit event** provee información de todos los circuitos conectados.
- El **debug mpls l2transport vc event** se usa para observar mensajes de eventos AToM de los circuitos virtuales.
- El **debug mpls l2transport packet data** permite mirar el flujo de paquetes a través de del túnel de capa 2.

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO 4

LIBROS

[1] **MARTEY**, Abe; **STURGESS**, Scott. "*IS-IS Network Design Solutions*". Cisco Press. Febrero 2002.

[2] **FARAZ**; ZAHEER; **LIU**; MARTEY. **"***Troubleshooting IP Routing Protocols*". Cisco Press. Mayo 2002.

[3] **DOYLE**, Jeff; **DEHAVEN**, Carroll. "*Routing TCP/IP, Volume II*". Cisco Press. Abril 2001.

[4] **HALABI**, Sam; **MCPHERSON**, Danny. "*Internet Rounting Architectures*". Segunda Edición. Cisco Press. Agosto 2000.

[5] **PARKHURST**, William; "*Cisco BGP-4 Command and Configuration Handbook*". Cisco Press. 2001.

[6] **LUO**; PIGNATARO; **BOKOTEY**; CHAN. "*Layer 2 VPN Architectures*". Cisco Press. Marzo 2005.

[7] **ALVAREZ**, Santiago. "*QoS for IP/MPLS Networks*". Cisco Press. Junio 2002.

[8] **SINCHE**, Soraya. "*Sistemas de Cableado Estructurado*". Apuntes de Clase. Semestre Septiembre 2008 – Febrero 2009

[9] **LOBO**, Lancy; **LAKSHMAN**, Umesh. "*MPLS Configuration on Cisco IOS Software*". Cisco Press. Octubre 2005.

[10] **ALWAYN**, Vivek. "*Advanced MPLS Design and Implementation*". Cisco Press. Septiembre 2001.

[11] **GUICHARD**, Jim; **PEPELNJAK**, Ivan. "*MPLS and VPN Architectures*", Cisco Press, Octubre 2000.

[12] **LEWIS**, Mark. "*Troubleshooting Virtual Private Networks*". Cisco Press. Mayo 2004

TESIS

[13] **NIETO**, Luisiana. "*Diseño y configuración de calidad de servicio en la tecnología MPLS para un proveedor de servicios de internet*". EPN. Mayo 2010.

PDF, RFC, PAPERS

[14] **ANÓNIMO**. "*Building Scalable Cisco Internetworks*". Student Guide. Cisco System. Version 3.0. Volume 1. 2006.

[15] ***ANÓNIMO***. "*Cisco IOS IP Routing Protocols Command Reference*". Cisco System. Noviembre 2008.

[16] **ANÓNIMO**. "*Cisco IOS XR Routing Configuration Guide*". Cisco System. 2007.

[17] **ANÓNIMO**. "*Building Scalable Cisco Internetworks*". Student Guide. Cisco System. Version 3.0. Volume 2. 2006.

[18] **ANÓNIMO**. "*Cisco IOS Quality of Service Solutions Configuration Guide*". Cisco System.

[19] **ANÓNIMO**. "*Configuring MPLS QoS". Cisco System*.

[20] **ANÓNIMO**. "*EVC Fundamentals". Cisco System*.

[21] **ANÓNIMO**. "*Configuring Ethernet Virtual Connections (EVCs)*". Cisco System.
URL: http://www.Cisco.com/en/US/docs/switches/metro/me3600x_3800x/software/release/12.2_52_ey/configuration/guide/swevc.pdf

[22] **ANÓNIMO**. "*Suplemento sobre cableado estructurado*".
URL: http://www.espoch.edu.ec/Descargas/noticias/dacee2_CCNA1_CS_Structured_Cabling_es.pdf

[23] **HASSAN**, Yusuf; **ASATI**, Rajiv. "*Troubleshooting Mpls Networks*". Cisco Systems. 2004.
URL: http://www.Cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6557/prod_presentation0900aecd80312051.pdf

[24] **ANÓNIMO**. "*Cisco IOS XR Troubleshooting Guide Troubleshooting MPLS Services*". Cisco Systems.
URL: http://www.Cisco.com/en/US/docs/routers/asr9000/software/asr9k_r4.0/ troubleshooting/guide/tr40mpl.pdf

INTERNET

[25] **ANÓNIMO**. "*Implementing IS-IS on Cisco IOS XR Software*"
URL: http://www.Cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.0/routing/configuration/guide/rc3isis.html

[26] **ANÓNIMO**. "*IP Routing Protocol-Independent Commands : redistribute (IP) Through traffic-share min*"

URL: http://www.Cisco.com/en/US/docs/ios/12_2/ iproute/command/ reference/1rfindp2.html

[27] **ANÓNIMO**. ” *IP Routing Protocols Commands: K through M*”
URL: http://www.Cisco.com/en/US/docs/ios/12_3t/ip_route/command/ reference/ip2_k1gt.html

[28] **ANÓNIMO** ”*How to block one or more networks from BGP peer*”
URL: http://www.cisco.com/en/US/tech/tk365/technologies_tech_ note09186a00801310cb.shtml

[29] **ANÓNIMO**. “*Implementing BGP on Cisco IOS XR Software*”.
URL: http://www.Cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/routing/ configuration/guide/rc37bgp.html#wp1197962

[30] **ANÓNIMO** “*Routing Policy Commands on Cisco IOS XR Software*“.
URL: http://www.Cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/routing/ command/reference/rr37plcy.html#wp1135677.

[31] **ANÓNIMO** “*Any Transport over MPLS*”.
URL: http://www.Cisco.com/en/US/docs/ios/12_0s/feature/guide/ fsatom28.html.

[32] **ANÓNIMO** “*MPLS DiffServ Tunneling Modes*”.
URL: http://www.Cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ ftdtmode.html#wp1154997.

[33] **ANÓNIMO** “*Configuring Layer 1 and Layer 2 Features*”.
URL: http://www.Cisco.com/en/US/docs/routers/7600/install_config/ ES40_config_guide/es40_chap4.html#wp1627009

[34] **ANÓNIMO** “*Configuring the Cisco 7600 Series Ethernet Services 20G Line Card*”
URL: http://www.Cisco.com/en/US/docs/routers/7600/install_config/ ES20_config_guide/baldcfg.html#wp1507850

[35] **ANÓNIMO** “Gabinete net-access”
URL: http://www.gruposaytel.com.mx/detalles.php?id=6

[36] **ANÓNIMO** “*Accesorio bajada de cables escalerilla*”
URL: http://www.enavar.com/images/productos/dev100gs.jpg

[37] **ANÓNIMO** “Organizador de cables”
URL: http://images2.cableorganizer.com/panduit/fiber-runner-system/ FRIV45_inside-corner_cables-s.jpg

[38] **ANÓNIMO**. “*How to Troubleshoot the MPLS VPN*”. Cisco Systems.
URL: http://www.Cisco.com/en/US/tech/tk436/tk428/ technologies_tech_note09186a0080093fcd.shtml#routeinfo

[39] **ANÓNIMO**. "*Cisco IOS XR MPLS Configuration Guide, Release 3.7*". Cisco Systems.
URL: http://www.Cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.7/mpls/configuration/guide/gc37book.html

[40] **MILIVOJEVIC**, Marko. "*Multicast MPLS VPNs*". Blog IPExpert.
URL: http://blog.ipexpert.com/2010/06/07/multicast-mpls-vpns/

[41] **ANÓNIMO**. "*Multicast Quick-Start Configuration Guide*". Cisco System.
URL: http://www.Cisco.com/en/US/tech/tk828/technologies_tech_note09186a0080094821.shtml

[42] **ANÓNIMO**, "*Cisco IOS Switching Services Command Reference, Release 12.2*". Cisco Systems.
URL: http://www.Cisco.com/en/US/docs/ios/12_2/switch/command/reference/fswtch_r.html

[43] **ANÓNIMO**. "*Multicast-VPN -- IP Multicast Support for MPLS VPNs*". Cisco Systems.
URL: http://www.Cisco.com/en/US/docs/ios/12_2s/feature/guide/fs_mvpn.html#wp1048025

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

En este capítulo se describe un conjunto de conclusiones y recomendaciones derivadas de la realización del proyecto propuesto

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La creación de esquemas de prueba haciendo uso de los equipos de laboratorio que dispone CNT E.P. permite realizar diferentes ensayos de servicios y configuraciones, en la búsqueda de reducir las fallas, optimizar los recursos de red y disminuir las pérdidas económicas generadas por la falta de servicios de la red.

- Para utilizar MPLS para el transporte de información, se debe tomar en cuenta que es un protocolo que necesita de otros para su adecuado funcionamiento. Para habilitar MPLS es necesario previamente configurar un protocolo enrutamiento interior y uno de distribución de etiquetas, también se debe tener presente que en los enrutadores Cisco es un prerrequisito básico la habilitación de la conmutación CEF.

- Los nodos LSRs únicamente realizan la conmutación de paquetes etiquetados, esto permite que MPLS ofrezca una alta velocidad de conmutación en el núcleo de la red, reduciendo el retardo en la entrega de los paquetes, asegurando el adecuado funcionamiento de aplicaciones sensibles como la VoIP, video conferencia e IPTV.

- La interfaz de loopback es importante para que se puedan establecer los diferentes servicios de MPLS, a través de esta dirección se realiza el establecimiento y mantenimiento de sesiones LDP e ISIS, que permiten el envío de un flujo continuo de información.

- Se observa que todos los routers cisco tienen por defecto habilitado el comportamiento PHP, esto permite ahorrar una búsqueda en la tabla de enrutamiento de los nodos LERs, lo que permitirá ahorrar el uso de CPU, que en estos dispositivos es importante, ya que al manejar conmutación MPLS e IP utilizan mayores capacidades de procesamiento.

- Los filtros de rutas BGP son flexibles y permiten restringir el acceso a cualquier red, de esta manera se puede establecer dos políticas de manera general, una en la que se permiten todas las redes y solo se deniegan especificas, no es el más optimo, o una política en la que se deniega todo y solo se permite ciertas rutas, este esquemas es más seguro pero su implementación se dificulta.

- La utilización de múltiples enlaces entre sistemas autónomos permite implementar redundancia, y si además realiza balanceo de carga con BGP se optimizará el uso de los recursos.

- Con las VPNs de capa 2 MPLS tiene un nuevo esquema para ofrecer interconexiones punto a punto de dos localidades de un cliente, en este nuevo enfoque se facilita la configuración en el lado del cliente ya que el cliente ve a la conexión como una conexión Ethernet local, permitiéndole establecer adyacencias de cualquier protocolo de enrutamiento.

- Las VPNs capa 2 permiten mantener compatibilidad hacia atrás, pues permiten mantener el uso de esquemas como el HUB and SPOKE de frame relay, ofreciendo a los proveedores de servicio una opción en la que la migración se puede realizar en etapas.

- La prueba de VPNs capa 3 que se desarrolló permitió observar que su utilización permite a un Proveedor de Servicios mantener una separación de tráfico a nivel de capa 3, usando de distintas tablas de enrutamiento para sus clientes VPN, de esta manera se controla que no crezcan indiscriminadamente una sola tabla de enrutamiento, optimizando los tiempos de procesamiento en la búsqueda de prefijos de red para el envió de paquetes en un router.

- Dentro de la prueba de VRFs se logró comprobar que este tipo de infraestructura VPN permite mantener un espacio de direccionamiento “compartido-independiente”, es decir que tanto el Proveedor de Servicios como cada uno de los Clientes VPN L3 son capaces de utilizar todo el rango de direcciones IPv4 de forma independiente, de modo que cada cliente puede usar el mismo direccionamiento utilizado en otra VPN o que esté usando el mismo ISP, sin interferir con los mismos, asegurando de esta forma que el tráfico de datos de cada VRF se mantenga por separado.

- De forma general se consiguió establecer que los beneficios que permite una topología VPN L3 “VRF”, a un Proveedor de servicios es tener escalabilidad, seguridad, la implementación de complejas topologías VPN con el manejo de las políticas de importación y exportación de rutas “route-target”.

- El marcado de los campos de QoS en un paquete permite que durante su transporte por la red se le pueda clasificar para asociarlo a una clase de tráfico, y de esta manera garantizar el comportamiento adecuado para estos flujos.

- Al usar los diferentes algoritmos de manejo de congestión, se observa que existe una alternativa para ofrecer sobresuscripción sobre una red de transporte de un proveedor de servicios, en esta se limita la cantidad máxima de ancho de banda que un tipo de tráfico puede usar en una interfaz de un router, evitando que genere congestión y perdidas en la transmisión de otros flujos de mayor importancia.

- El uso de *traffic policing* permite que un proveedor de servicios controle que el cliente cumpla con los acuerdos SLAs establecidos, en estos se controla en tráfico que cumple con el perfil y se le da un tratamiento adecuado en la red, adicionalmente se puede definir un tráfico en exceso al que se le dará un tratamiento con menor prioridad y que se lo puede descartar en caso de congestión.

- Se comprobó que los anchos de banda mínimos garantizados se cumplen en un evento de congestión con lo que se puede garantizar una adecuada asignación de recursos para los flujos de tráfico.

- El desarrollo de la prueba de MPLS con Ingeniería de Tráfico, permitió observar que existen dos formas de manipulación del tráfico con Túneles TE, de forma explícita o dinámica, siendo la explícita la forma más optima y flexible de manipulación, donde el administrador de red define un camino LSP en particular para cada túnel, sin depender del IGP. Esta característica se ve más necesaria cuando se trata de túneles de backup para la protección de enlaces, ya que al establecer de forma explícita el túnel de respaldo, la conmutación hacia éste es más rápida, que esperar hasta que IGP recalcule una ruta para el túnel de backup, disminuyendo de esta forma la perdida de datos mientras se da la conmutación.

- En Ingeniería de Tráfico se encontró que el comando “tunnel mpls traffic-eng autoroute announce”, permite al IGP tomar al túnel en los cálculos SPF (Shortest Path First) para el envio de tráfico, pero se observó que este comando anuncia todos los prefijos o redes, que se originan en el router de destino del túnel TE vía al túnel, lo cual no es óptimo en un Proveedor de Servicios porque solo ciertas redes de mayor importancia, o que transporten información crítica deben ser llevadas por un túnel TE.

- Para el caso de CNT E.P. se estableció que para el envío de tráfico de una VRF sobre un túnel de Ingeniería de Tráfico, se haga uso de un atributo de BGP “bgp next-hop Loopback XXX” dentro de la configuración de una instancia VRF, permitiendo de esta manera que se force a utilizar como siguiente salto en las actualizaciones de MP-BGP, una loopback diferente a la loopback configurada en BGP (loopbak compartida) para las actualizaciones, dicha loopback se encuentra asociada a un túnel TE.

- En el caso de establecer un tráfico *multicast* en una red de Proveedor de Servicios, mediante la simulación se determinó que el uso de un árbol de distribución compartido, establecido con PIM *Sparse Mode* es la forma más

óptima de realizar dicha configuración, debido a que como se trata de una red de gran utilización, no se debe inundar la red con tráfico innecesario que podría causar congestión y problemas para el resto de servicios que se ofrecen en la red, y PIM-SM permite el tráfico únicamente a los segmentos de red que se interesan en recibir el tráfico y han realizado un pedido explícito de los datos.

- Se verificó que a pesar de tener un alto número de direcciones MAC en las tablas de una *service instance* esto no afectaba el correcto establecimiento de las sesiones PPPoE que permiten la salida a internet de los clientes HOME de CNT, descartando que el problema sea una mala configuración o mal funcionamiento de las nuevas prestaciones de las tarjetas 7600-ES+20G3CXL de Cisco.

5.2 RECOMENDACIONES

- Los caminos LSP de MPLS se establecen a partir de las mejores rutas que seleccionan un protocolo IGP en este caso ISIS, por lo que es importante realizar una configuración de las métricas en las diferentes interfaz de acuerdo a su velocidad de transmisión, de esta manera se asegura que la selección del LSP sea óptima.

- Se recomienda que para realizar el balanceo de carga se realice un análisis del volumen de tráfico generado por las diferentes redes, de esta manera se realizará un mejor uso de los enlaces disponibles, esto debido a que no todas las redes generan un flujo de tráfico igual, existen direcciones IP especificas que generan una mayor cantidad de tráfico.

- Se recomienda que al crear mapas de rutas, listas de prefijos y *routing policy,* antes de utilizarlos en la red de backbone de CNT E.P: primero se los pruebe en el laboratorio, de esta manera se asegura que se obtenga el resultado es esperado y se podrá corregir su comportamiento en caso de que presente fallas, evitando que cause problemas en los clientes de la red del proveedor de servicios.

- Se recomienda que un Proveedor de Servicios como CNT E.P con infraestructura MPLS, utilice las VPN MPLS L3 “VRF” para manejar de forma separada el tráfico de sus servicios como Internet, voip, iptv, entre otros y de esta forma tener tablas de enrutamiento por separado para cada uno de ellos, facilitando su gestión y optimizando su funcionamiento. Además se recomienda que aunque no es necesario que el nombre asignado a una VRF, sea el mismo en todos los routers PEs que participan de la VPN, esto se convierta en una política de administración para facilitar la gestión y revisión de problemas de una VPN L3.

- Para la CNT E.P. se recomienda que se establezcan túneles de ingeniería de tráfico entre todos los equipos del backbone MPLS, permitiendo de esta forma que aunque físicamente se tenga una topología *partial mesh,* lógicamente se pueda establecer una topología full mesh y de esta forma manipular y manejar los flujos importantes de tráfico entre todos los equipos, reduciendo los tiempos de latencia, optimizando los recursos de la red.

- Se recomienda que en el caso de usar un túnel de Ingeniería de Tráfico para el envío de paquetes de VPNs Capa 3, los túneles TE utilizados sean los establecidos entre los PEs routers, puesto que si se lo asigna a un túnel que termina en un P router antes del PE router, este descartará el paquete debido a que al arribar al router P lo hace con una única etiqueta, que identifica la VPN, el router P no tiene conocimiento del etiquetamiento VPN.

TERMINOLOGÍA

ETSI European Telecommunications Standards Institute

SDH Jerarquía Digital Sincrónica es el estándar internacional de comunicaciones aceptado por la UIT para redes de transmisión de alta capacidad sobre redes ópticas y eléctricas que pueden transportar señales digitales. Tecnologías como ATM, IP/MPLS o ADSL se apoyan en SDH para alcanzar la ansiada banda ancha.

NG-SDH Next Generation SDH es la evolución y mejora de Redes SDH, permite un mayor potencial y eficiencia de servicios de banda ancha, transportando de manera eficiente los datos sin la necesidad de remplazar la base de la infraestructura SDH, únicamente cambiando los nodos edge.

DWDM Dense Wavelength Division Multiplexing es una técnica de transmisión de señales a través de fibra óptica usando la banda C (1550 nm), reúne múltiples señales y las envía al mismo tiempo a lo largo de una fibra, con transmisiones que tienen lugar en diferentes longitudes de onda.

ROADM Reconfigurable Optical Add-Drop Multiplexer es un dispositivo que tiene la capacidad de controlar la dirección y el enfoque de la emisión de luz infrarroja y visible dentro de un rango de diferentes longitudes de onda, se utiliza a menudo con cualquier sistema que hace uso de multiplexación por división de longitud de onda o WDM.

OLA Optical Line Amplifier Amplifica la señal DWDM conjunta en el dominio óptico (sin ningún tipo de regeneración eléctrica de cada uno de los canales individuales) para su transporte a largas distancias.

PCMCIA *Personal Computer Memory Card International Association* interfaces para conectar perifericos.

VoQ Virtual Output Queuing es una estrategia de encolamiento en la que cada puerto de entrada organiza el buffer en varias colas lógicas, una por cada puerto de salida.

ASIC Application specific integrated circuit, son circuitos especializados diseñados para realizar una función en particular.

I-Flex Cisco Interface Flexibility: Arquitectura modular que usa ranuras para colocar tarjetas que permiten extender las capacidades del router.

BFD Bidirectional Forwarding Detection es un protocolo de red que se utiliza para detectar fallas entre dos motores de transmisión conectadas por un enlace. Proporciona baja sobrecarga de detección de fallas, incluso en medios físicos que no son compatibles con la detección de fallos de cualquier tipo, tales como Ethernet, circuitos virtuales, túneles y caminos MPLS Label Switched.