ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS, PROPUESTA, SIMULACIÓN DE UNA METODOLOGÍA PARA LA MIGRACIÓN DE LA RED MPLS ZONA PICHINCHA DE LA CNT EP DE IPV4 A IPV6 Y DE LA APLICACIÓN DE CALIDAD DE SERVICIO (QOS), Y COMPROBACIÒN EN UN PROTOTIPO DE LABORATORIO

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

ALBUJA GRANDA RAMIRO SANTIAGO
santo364@yahoo.com
GUTIÉRREZ LÓPEZ LUIS RICARDO
luis_r_gl@hotmail.com

DIRECTOR: ING. XAVIER ALEXANDER CALDERÓN HINOJOSA MSc.
xavier.calderon@epn.edu.ec
CO-DIRECTOR: ING. JAIME JOSÉ GALLARDO ZAVALA
jaime@huawei.com

Quito, Marzo 2014

DECLARACIÓN

Nosotros, Ramiro Santiago Albuja Granda y Luis Ricardo Gutiérrez López, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado 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.

_____	_____
Ramiro Santiago Albuja Granda	Luis Ricardo Gutiérrez López

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por Ramiro Santiago Albuja Granda y Luis Ricardo Gutiérrez López, bajo nuestra supervisión.

_____

Ing. Xavier Alexander Calderón Hinojosa MSc.
DIRECTOR DEL PROYECTO

_____

Ing. Jaime José Gallardo Zavala
CO-DIRECTOR DEL PROYECTO

AGRADECIMIENTOS

Antes que nada quiero agradecer a Dios por regalarme el don de la vida; por guiarme siempre en cada decisión y camino que tomo y por las bendiciones que me ha brindado.

A mi hermosa familia por creer siempre en mí y por brindarme su apoyo incondicional en todo momento; especialmente en esta etapa fundamental de mi vida.

A la CNT EP por permitirme aportar con un granito de arena en tan prestigiosa empresa, así como al personal de IP/MPLS quienes nunca me cerraron las puertas y estuvieron siempre dispuestos ante cualquier duda.

A mi amigo Luis Gutiérrez por su valioso aporte en este proyecto así como su dedicación y paciencia para realizar el mismo.

Santiago Albuja

AGRADECIMIENTOS

Ante todo quiero agradecer a Dios por haberme dado la salud y la vida para poder culminar este proyecto; y por haberme ayudado cada instante de mi vida.

A mi familia; mi querida madre María del Carmen y mi padre Luis; quienes con su infinita paciencia y amor supieron guiar mis pasos y enseñarme a ser un hombre de bien, que me supieron brindar todo el apoyo necesario en todos los aspectos de mi vida y gracias a eso pude culminar esta gran etapa de mi vida. A mis hermanos Diana y Daniel quienes me brindaron todo su apoyo desde que comencé mi carrera hasta el día de hoy, gracias por estar a mi lado siempre.

Al Ing. Jaime Gallardo, un gran amigo y mentor que me ayudó a poder desarrollar y culminar este proyecto.

A mi amigo Santiago Albuja por su ayuda y constancia en este proyecto y en toda nuestra carrera.

Luis Gutiérrez

DEDICATORIA

El presente proyecto lo quiero dedicar a las cuatro mujeres que más amo en el mundo: a mi linda esposa Katty, que ha sido un baluarte y un apoyo constante en mi vida y a lo largo de este trabajo ya que sin ella a mi lado no lo hubiera logrado, a mis dos hijitas, Ana Paula & Isabella, quienes son la razón de mi vida y el incentivo diario para salir adelante; y a mi mamita Chio quien ha velado por mi desde siempre y que con su esfuerzo y ejemplo diario me ha enseñado mucho en mi vida.

Para mi padre y mis hermanos con todo el cariño y amor del mundo, toda mi dedicación y esfuerzo.

Santiago Albuja

DEDICATORIA

A mi madre que gracias a ella he podido ser un hombre de bien y ha sido mi principal soporte durante toda mi vida, y me ha guiado a lo largo de la vida.

A mi padre que ha sido el más grande ejemplo que he tenido, mi inspiración y la persona que me ha guiado a lo largo de mi carrera.

En especial a mi querido hermano Daniel, que ha estado a mi lado toda la vida.

A mi Hermana y su familia que han sido un gran apoyo.

Luis Gutiérrez

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

CAPÍTULO 1

CAPITULO 2

CAPÍTULO 5

ÍNDICE DE TABLAS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

CAPÍTULO 5

RESUMEN

El presente proyecto tiene como objetivo el desarrollar una metodología para la migración de clientes IPV6 en la red MPLS de la CNT EP para la zona de Pichincha, minimizando el impacto por el cambio de direcciones, dimensionamiento de equipos y de red; y mediante la simulación y la comprobación en un prototipo en el laboratorio, comprobar su funcionamiento en cuanto a conectividad y calidad de servicio (QoS).

En el primer capítulo se presenta una descripción detallada del funcionamiento de la tecnología MPLS con respecto a su definición; elementos de la red, asignación, distribución y reenvío de etiquetas, así como las aplicaciones que nos brinda este protocolo. Se detallará también la comparación estructural del datagrama IPV4 con IPV6 y el análisis a profundidad del protocolo IPV6 como: el formato de cabecera, cabeceras de extensión y direccionamiento.

El capítulo dos muestra un análisis detallado de la situación actual de la red MPLS del CNT zona Pichincha, así como de su operación, equipos que operan, direccionamiento y Calidad de Servicio (QoS). Adicionalmente se presenta un análisis de las direcciones IPV4 disponibles en el Ecuador.

El tercer capítulo contiene un análisis de los diferentes métodos de migración de IPV4 a IPV6 como son dual-stack y tunneling; además se presenta la propuesta para la migración con un mínimo impacto en la red y que no requiera mucha inversión.

En el capítulo cuatro se realiza el análisis en cuanto a software y hardware de los equipos que actualmente se encuentran en funcionamiento en la red MPLS de CNT; se presenta además, luego de su respectivo estudio, los requerimientos para poder realizar la migración así como la descripción de costos para la misma.

El capítulo cinco presenta un estudio de los principales simuladores del mercado para poder elegir el que mejor se ajuste a los requerimientos del proyecto. Se muestran los resultados de la simulación de la red MPLS en su estado actual en cuanto a configuraciones y pruebas en el laboratorio con el objeto de comprobar su correcto funcionamiento; igualmente la simulación de la red MPLS soportando el protocolo IPV6 y el análisis de QoS.

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

PRESENTACIÓN

Frente al crecimiento constante de las redes de interconexión e Internet, y ante la demanda de los clientes por obtener varios servicios funcionando en común; las empresas de telecomunicaciones se ven en la necesidad obligada de satisfacer las necesidades del usuario al poder ofrecer servicios de calidad por un precio razonable. Actualmente la tecnología MPLS permite transmitir varios servicios por un mismo medio, garantizando la individualidad de los mismos; y es así como la Corporación Nacional de Telecomunicaciones en la actualidad cuenta con un backbone MPLS el cual ha ido creciendo hasta el punto de contar con equipos que soporten este protocolo en todo el país.

Al ser MPLS un protocolo con la capacidad de integrar voz, datos y video en una plataforma en común, su utilización y demanda ha ido creciendo exponencialmente, al punto que las direcciones IPV4 en el Ecuador se están agotando día tras día. Es preciso contar con una metodología de migración a IPV6 en la cual no se vea afectado el funcionamiento de la red; adicionalmente de contar con un laboratorio en el cual se puedan realizar pruebas y configuraciones como si las mismas se estuvieran efectuando en un ambiente real.

Tomando en cuenta lo anteriormente expuesto; el presente proyecto tiene como finalidad crear un prototipo de laboratorio en el cual se pueda simular la red MPLS de CNT para la provincia de Pichincha, por la cantidad de equipos que presenta y considerando que al realizar una simulación, el limitante es el procesamiento y memoria del equipo al cual se configure el mismo.

Este proyecto tiene como enfoque el poder implementar un laboratorio mediante software para poder simular la red MPLS y así poder desarrollar diferentes configuraciones y casos de prueba críticos con el objetivo de no realizar las mismas en una red operativa y prevenir problemas en el momento de la migración.

CAPÍTULO 1

CONCEPTOS BÁSICOS Y ESTUDIO DE LA TECNOLOGÍA MPLS E IPV6

1.1 MPLS (MULTIPROTOCOL LABEL SWITCHING – CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO)

1.1.1 HISTORIA [12]

El internet basado en la tecnología IP (*Internet Protocol*) apareció en los años 90. La tecnología IP tenía un pobre desarrollo en el reenvío de paquetes ya que era inevitable la dependencia de software en la búsqueda de rutas a través de grandes algoritmos de búsqueda.

Con el desarrollo de las tecnologías de red, la tecnología ATM surgió. Usa celdas de tamaño constante y mantiene una tabla de celdas que es mucho más pequeña que una tabla de rutas. Sin embargo, comparada con la tecnología IP de ese entonces, ATM hacía un mejor reenvío de paquetes. Esta tecnología no se hizo tan popular debido a que usa protocolos complejos y que tiene un gran costo de despliegue.

La tecnología IP tradicional es simple y tiene un bajo costo de despliegue. La gente quería realizar una combinación técnica que junte las ventajas de IP y ATM. Y aquí es donde nació MPLS.

1.1.2 INTRODUCCIÓN [12]

MPLS trabaja entre la capa de enlace y la capa de red en la arquitectura TCP/IP[1].

[1] Conjunto de protocolos de red en los que se basa Internet y que permiten la transmisión de datos entre redes de computadoras.

Es una red WAN (*Wide Area Network*) que basa su funcionamiento en el enrutamiento de etiquetas. Siempre busca la comunicación extremo a extremo. El propósito de MPLS es estandarizar el transporte de datos, permitiendo que varias tecnologías viajen a través de un mismo paquete; para esto necesitamos integrarlo en la capa de red, además MPLS añade capacidades de ingeniería de tráfico al ruteo IP (plano de control).

MPLS no está limitada a algún protocolo en específico de la capa de enlace y acepta cualquier medio de transferencia de paquetes de capa 2. El origen de MPLS es el Protocolo de Internet versión 4 (IPV4); el núcleo de MPLS puede ser extendido a múltiples protocolos de red, como lo dice su nombre, “Multiprotocolo”.

La tecnología MPLS trata de una tecnología de túnel que en lugar de un servicio o una aplicación. Soporta múltiples protocolos y servicios. Además asegura la transmisión de datos.

1.1.3 MPLS MODO TRAMA [1]

El término MPLS Modo Trama (Frame Mode MPLS) denota el uso de MPLS con encapsulamiento Ethernet u otra interfaz con encapsulamiento basado en tramas. No incluye interfaz con encapsulación ATM ya que ésta utiliza MPLS modo celda. ATM MPLS tiene un único tipo de requerimientos debido a su longitud de celda fija. En la figura 1.1, se puede observar las tramas para las 3 situaciones antes nombradas.

1.1.4 ESTRUCTURA DE LA RED MPLS [1] [3] [4] [7]

El elemento fundamental en una red MPLS es el LSR (Label Switching Router – Router de Conmutación de Etiquetas). Muchos LSR en una red forman un dominio MPLS. Los LSRs que se encuentran en el límite del dominio MPLS y se conectan a otras redes son los LER (Label Edge Router – Router de borde de etiquetas). Los LSR dentro de un dominio MPLS son los LSR núcleo. Si un LSR

se conecta a uno o más nodos contiguos que no son nodos MPLS, estos son los LER. En la figura 1.2 se puede visualizar la estructura MPLS.

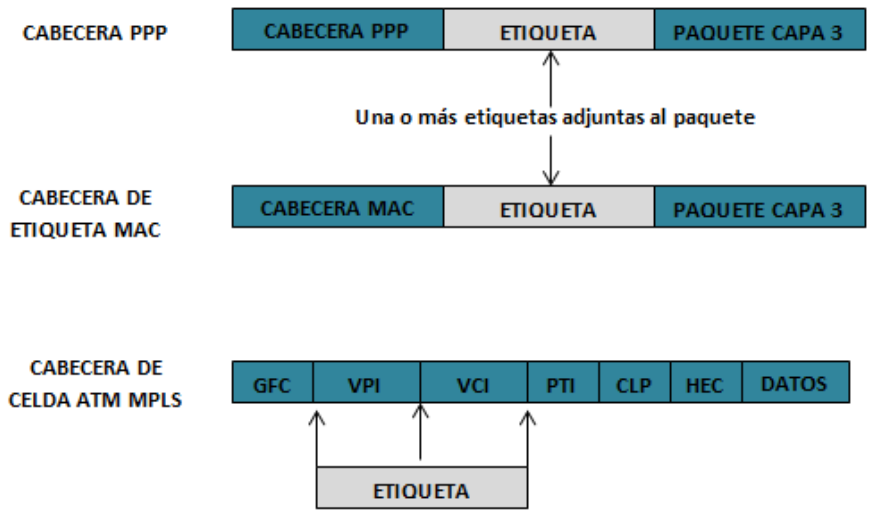


Figura 1.1: MPLS modo trama [1]

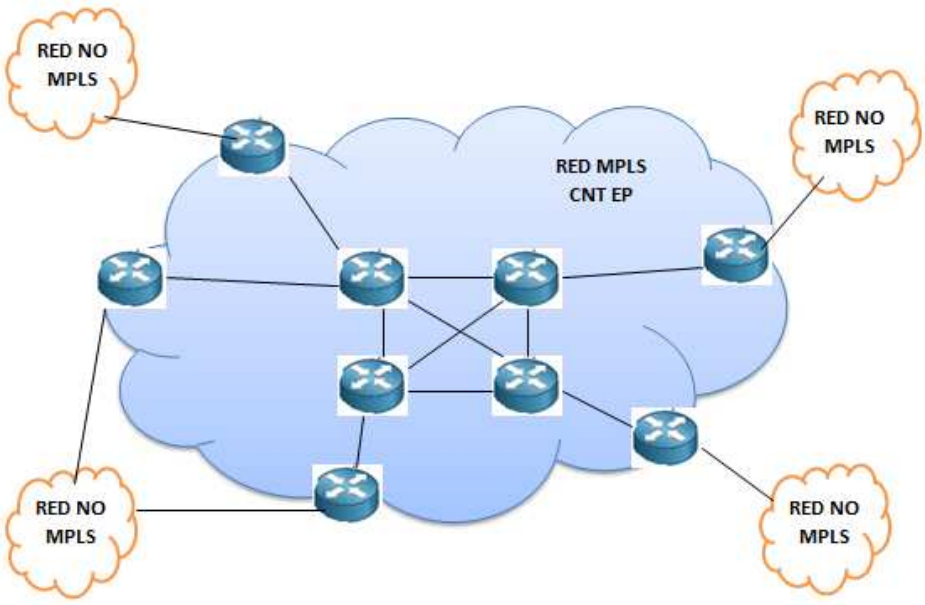


Figura 1.2: Estructura MPLS

La transferencia de paquetes en el dominio MPLS se basa en etiquetas. Cuando un paquete IP entra en una red MPLS, el LER (Label Edge Router) analiza este paquete IP y luego le añade la respectiva etiqueta al mismo. Todos los nodos dentro de la red MPLS reenvían paquetes de acuerdo a las etiquetas, y cuando

los paquetes IP dejan la red MPLS, las etiquetas son borradas en el LER que se encuentra a la salida.

El camino que los paquetes IP hacen a través de la red MPLS es el LSP (Label Switched Path). Un LSP es un camino unidireccional en el mismo sentido que el flujo de datos. El nodo por donde ingresan los datos es el de entrada, y por el que salen es el de salida. El camino que hay entre estos dos nodos es llamado LSP. Cabe resaltar que un LSP puede tener una o varias rutas de tránsito pero un solo ingreso y una sola salida. La figura 1.3 muestra el funcionamiento del LSP en una red MPLS.

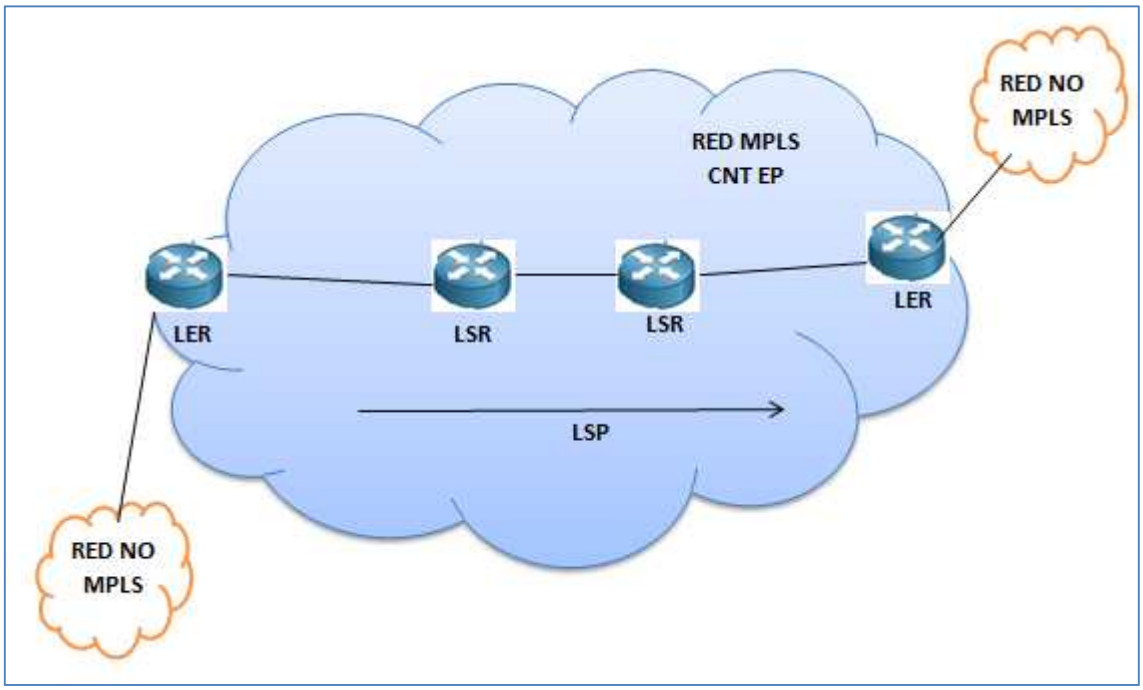


Figura 1.3: LSP en una red MPLS

1.1.4.1 FEC (Forwarding Equivalence Class – Clase de Equivalencia de Reenvío)

Se puede definir al FEC como una representación de una agrupación de paquetes compartiendo características similares tales como: dirección IP, origen, destino y tipo de tráfico. Estos tendrán el mismo tratamiento durante su viaje en la red ya que circulan por un mismo trayecto LSP hasta llegar a su destino correspondiente.

Para asegurar la escalabilidad[2], los flujos de datos deben ser manejados en grupos y no individualmente. MPLS asegura la escalabilidad soportando la agregación mediante el uso de FEC. En los LER se realiza la agregación, estos son los responsables de clasificar los paquetes y asociarlos a un FEC en particular; de esta clasificación se obtiene el valor de la etiqueta que tendrá cada paquete.

1.1.4.2 Etiqueta MPLS

Una etiqueta es un identificador corto de longitud constante que solo tiene significado dentro del dominio MPLS. La etiqueta MPLS se coloca delante del PDU (Protocol Data Unit) de red y detrás de la cabecera de nivel de enlace. MPLS reduce significativamente el procesamiento mediante el uso de etiquetas. Ya que la etiqueta es asignada a un respectivo FEC, los routers MPLS no tienen que analizar a todo el paquete, solo basta analizar la etiqueta para así poder realizar la conmutación.

Las etiquetas usualmente corresponden a redes de destino, similar a un enrutamiento capa 3; igualmente pueden corresponder a:

- Destino de VPN capa 3.
- Circuito virtual de capa 2.
- Interfaz de egreso.
- QoS.

La Figura 1.4 indica los campos que constan en la etiqueta.

Figura 1.4: Estructura de la cabecera de un paquete MPLS (etiqueta) [7]

[2] Capacidad de mejorar recursos para ofrecer una mejora (idealmente) lineal en la capacidad de servicio.

Una etiqueta contiene los siguientes campos:

- **Etiqueta (20 bits):** es un valor con significado local, que permite al router decidir su próximo salto; los valores del 0 al 15 son reservados.
- **EXP (3 bits):** indica la clase de servicio o precedencia IP.
- **S (1 bit):** campo de Stack que indica un grupo o stack de etiquetas.
- **TTL (8 bits):** tiempo de vida; tiene la misma funcionalidad que en un paquete IP.

1.1.4.3 Pila de Etiquetas

Es un conjunto ordenado de etiquetas. Un paquete MPLS puede llevar muchas etiquetas al mismo tiempo. La etiqueta a lado de la cabecera de capa 2 es llamada la etiqueta “top”. La que está junto a la cabecera de capa 3 es la etiqueta del fondo (bottom label). Las etiquetas pueden ser anidadas ilimitadamente. La figura 1.5 muestra los campos contenidos en la pila de etiquetas.

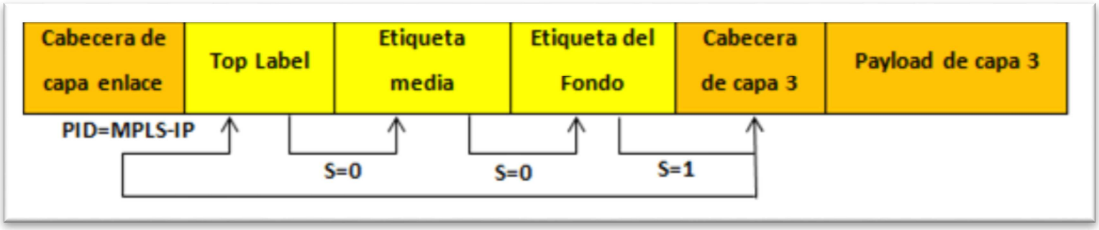


Figura 1.5: *Label Stack* (Pila de etiquetas) [1]

La pila de etiquetas organiza las etiquetas de acuerdo a la regla LIFO[3](Last In, First Out – Último en ingresar, primero en salir).En la mayoría de los casos solo una etiqueta es asignada a un paquete. Existen algunas instancias en donde más de una etiqueta es utilizada:

- **VPN`s MPLS:** BGP (Border Gateway Protocol) multiprotocolo (MP -BGP) es utilizado para propagar una segunda etiqueta que identifica la VPN

[3] Guarda analogía con una pila de platos, en la que los platos van poniéndose uno sobre el otro, y si se quiere sacar uno, se saca primero el último que se puso.

adicional a la etiqueta que es propagada por LDP[4] para identificar el camino.

- **Ingeniería de Tráfico MPLS (MPLS TE):** utiliza RSVP[5] (resource reservation protocol – protocolo de reserva de recursos) para establecer túneles LSP. RSVP propaga etiquetas que son utilizadas para identificar el túnel LSP. Esta etiqueta se encuentra adicionada a la etiqueta que es propagada por LDP (Label Distribution Protocol) para identificar la etiqueta LSP subyacente.

Una etiqueta no contiene ninguna información acerca del protocolo capa 3 que está siendo llevado en un paquete; esta falta de información significa que la identidad del protocolo de la capa de red debe ser deducible del valor de la etiqueta. Para protocolos de capa 2 que tienen campos TYPE y PID (Payload Identifier), nuevos valores indican que MPLS se encuentra habilitado en el protocolo capa 3.

1.1.4.3.1 Operaciones de Etiquetas

Las operaciones realizadas por las etiquetas son descritas a continuación:

- **Push**: Cuando el paquete IP ingresa al dominio MPLS, se añade una nueva etiqueta al paquete.
- **Swap**: Cuando el paquete es transferido dentro del dominio MPLS, el nodo que recibe el paquete intercambia la etiqueta al tope de la pila de etiquetas.
- **Pop**: Al final la etiqueta es retirada de la pila, en el caso de que haya, así se decrementa el número de etiquetas existentes.

1.1.4.3.2 Distribución de etiquetas

Los paquetes con el mismo destino pertenecen a un mismo FEC. Los LSR graban esta relación en la etiqueta y en el FEC, el LSR envía un mensaje y anuncia a los

[4] Protocolo de Distribución de etiquetas.
[5] Protocolo diseñado para reservar recursos de una red bajo la arquitectura de servicios integrados (IntServ).

LSR de arriba acerca de la relación FEC, etiqueta. Este proceso es llamado la distribución de etiquetas.

1.1.4.3.3 Protocolos de Distribución de Etiquetas

Los protocolos de distribución de etiquetas son protocolos de control de MPLS, llamados, protocolos de señalización. Son usados para clasificar FECs, distribuir etiquetas, crear y mantener LSP´s. MPLS utiliza múltiples protocolos de distribución de etiquetas como el LDP, el RSVP-TE y el MG-BGP.

1.1.4.4 LSR (Label Switching Router – Router de Conmutación de Etiquetas)

Son los encargados de conmutar y enrutar, de acuerdo a las etiquetas de cada paquete. El LSR no necesita revisar todo el paquete IP solo basta con revisar la etiqueta y así enrutar en base al valor de la misma. Físicamente pueden ser routers IP o switches ATM.

Para poder realizar las tareas, los nodos LSR utilizan dos protocolos que le ayudan a intercambiar la información que se requiera entre routers, estos protocolos son:

- Protocolos de enrutamiento interior.
- Protocolos de señalización.

El LSR cuando recibe un paquete remueve la etiqueta con la que llego, consulta la tabla de etiquetas, le asigna una nueva y lo envía al siguiente LSR.

1.1.4.5 LER (Label Edge Router – Router de Borde de Etiqueta)

Los LER son equipos ubicados en los extremos de una red y se encargan de encapsular y des encapsular el tráfico IP añadiendo las respectivas etiquetas. Primero se agrupa el tráfico común y los routers se encargan de conmutar a nivel de capa 2 de acuerdo a la etiqueta. Después el LER reenvía el paquete MPLS

basándose en la etiqueta. Cuando un paquete deja el dominio MPLS, la etiqueta es retirada. Los paquetes son convertidos en paquetes IP y son reenviados continuamente.

1.1.4.6 LSP (Label Switch Path – Camino de Conmutación de Etiquetas)

El camino que un FEC pasa a través de una red MPLS es llamado LSP. Un LSP funciona de la misma manera que un circuito virtual ATM y Frame Relay. El LSP es unidireccional desde el ingreso hasta la salida.

El LER de ingreso establece que paquetes se asocian a un determinado LSP en base al FEC del cual pertenece y entonces se procederá a colocar una etiqueta en el paquete la cual está asociada a un LSP, así ésta servirá para la conmutación dentro del núcleo de MPLS donde se ignorará la cabecera de capa de red del paquete.

1.1.4.7 Upstream y Downstream

El significado de upstream y downstream es muy importante para poder comprender de mejor manera la operación de distribución de etiquetas y para el reenvío de paquetes MPLS. Ambos conceptos son definidos con referencia al FEC de la red destino. La dirección de flujo planificado para los datos se denomina downstream, mientras que la dirección en la cual se transmite la información de protocolos de enrutamiento o distribución de etiquetas sigue un flujo en sentido contrario a los datos o en otras palabras upstream.

1.1.4.7.1 Unsolicited Downstream (Downstream no solicitado)

Este mecanismo es usado en la distribución de tramas. Cada router genera en sí mismo las etiquetas y los distribuye a los nodos adyacentes. No hay un procedimiento de control que regule como se propaguen las etiquetas. La figura 1.6 muestra un ejemplo de downstream no solicitado.

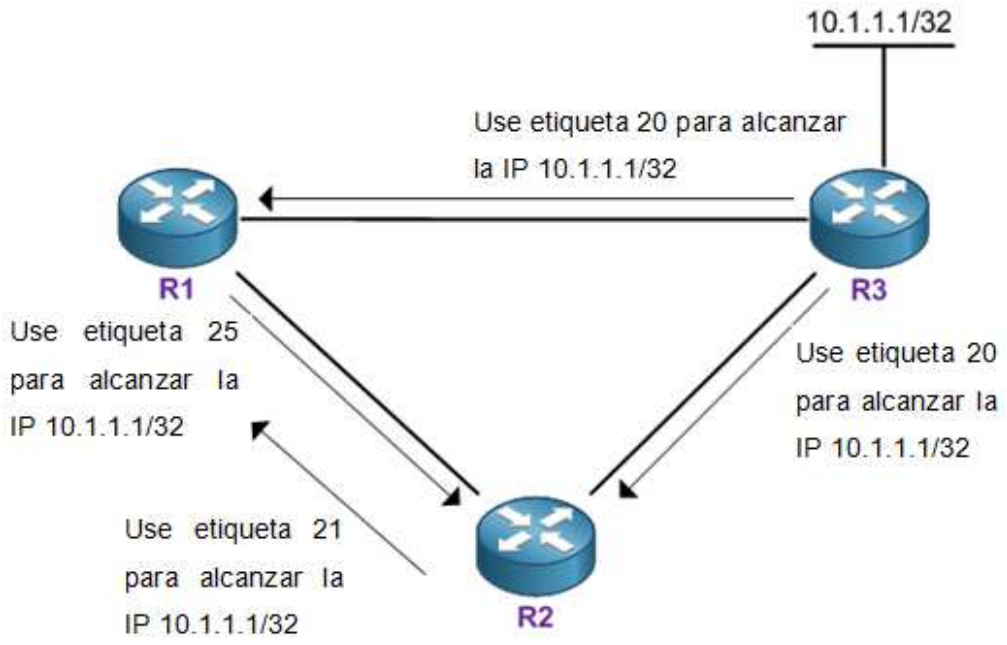


Figura 1.6: *Downstream* no solicitado

1.1.4.7.2 Downstream on demand (Downstream bajo demanda)

Este mecanismo es usado en la distribución de celdas. Cada router ATM, para cada destino existente en la tabla de enrutamiento, tiene que solicitar una etiqueta. En estos casos la propagación es hop-by-hop[6]. Estas dos técnicas de distribución de etiquetas se pueden utilizar dentro de la misma red MPLS pero no entre routers adyacentes. En la figura 1.7 se muestra el funcionamiento del downstream bajo demanda.

1.1.5 ARQUITECTURA MPLS [5]

La arquitectura MPLS está formada básicamente de dos componentes:

- El plano de datos.
- El plano de control.

[6] Método común de encaminamiento en redes en las que hay nodos intermedios entre la fuente y el destino

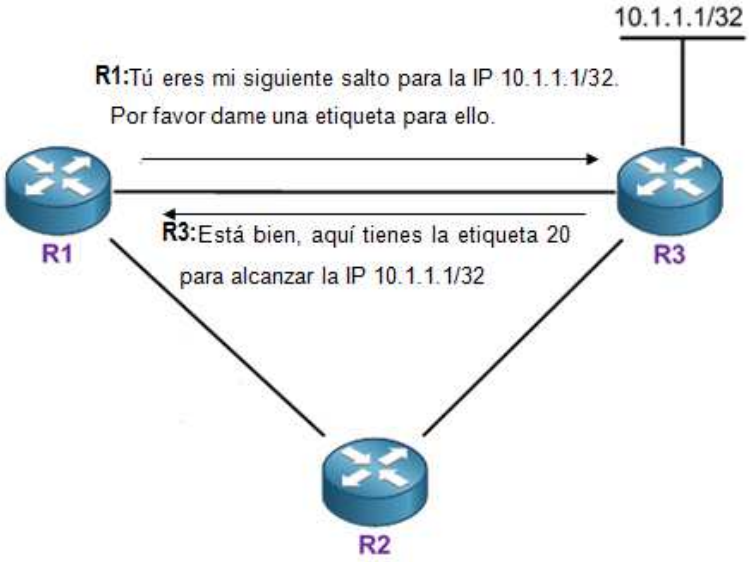


Figura 1.7: Downstream bajo demanda

El Plano de Datos es orientado a conexión, puede aplicar a servicios y protocolos de ATM, Frame Relay y redes Ethernet. Es responsable de añadir etiquetas y borrarlas de los paquetes IP. Simultáneamente reenvía los paquetes de acuerdo a la tabla de reenvío de etiquetas. El Plano de Control es no orientado a la conexión y es responsable de distribuir las etiquetas, creando la tabla de reenvío de etiquetas y creando o borrando los LSP`s.

En la figura 1.8 se puede visualizar la arquitectura MPLS mostrando tanto el plano de datos como el de control.

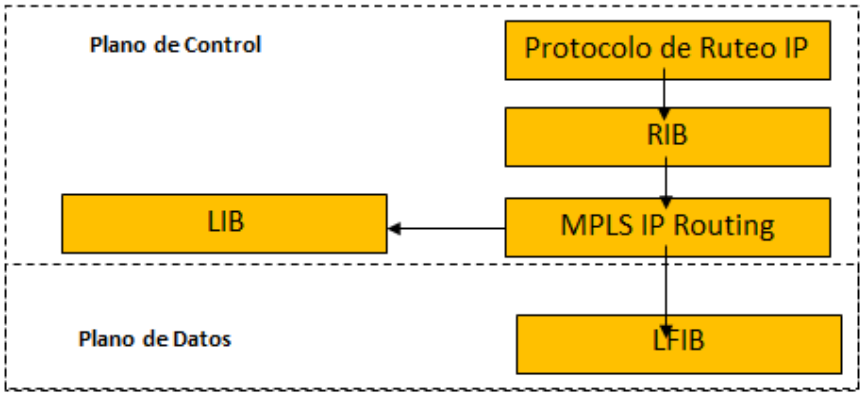


Figura 1.8: Arquitectura MPLS [5]

A continuación se detallan los componentes más importantes de la estructura MPLS:

- **FIB (Forwarding Information Base – Base de Reenvío de información):** es una copia de la tabla de enrutamiento; incluyendo etiquetas de interfaces MPLS y se la utiliza para el reenvío de paquetes capa 3 y añadir la etiqueta para interfaces de salida.
- **LIB (Label Information Base – Base de Información de Etiqueta):** las etiquetas aprendidas por LDP son almacenadas y ligadas a las interfaces. Los LSR`s anuncian las etiquetas asignadas a sus pares adyacentes; los pares usan la información de la etiqueta recibida para asociar la etiqueta del próximo salto.
- **LFIB (Label Forwarding Information Base – Base de Información de Reenvío de Etiqueta):** contiene la tabla de enrutamiento de etiquetas así como la información del reenvío IP de las FIB y la información de etiquetas de las LIB.

1.1.6 ESTABLECIMIENTO DE UN LSP [6]

MPLS localiza etiquetas por paquetes y establece un LSP. Después, MPLS puede reenviar los paquetes. Las etiquetas son localizadas y distribuidas por el downstream LSR a un upstream LSR. El primero clasifica los FEC de acuerdo a una tabla de ruteo IP y asigna las etiquetas a un FEC específico. Después, el segundo notifica al primero a través de un protocolo de aviso de etiquetas para configurar una tabla de reenvío de etiquetas y un LSP. Los LSP se clasifican en:

- LSP Dinámico: Es configurado por el protocolo de ruteo y por el LDP.
- LSP Estático: Es configurado por el administrador.

1.1.6.1 Establecimiento de un LSP Estático

Se puede asignar etiquetas manualmente para configurar un LSP estático. Funciona de tal manera que el valor de la etiqueta que sale del nodo de upstream

es igual al valor de la etiqueta que entra del nodo de downstream. La disponibilidad de un LSP estático lo hace válido solo para el nodo local y no para todo el LSP.

1. Al ingreso: Un LSP estático es configurado, y la interfaz de salida del ingreso es activada con MPLS. Si la ruta es alcanzable, el estado del LSP es arriba. Una ruta alcanzable significa que toda la ruta existe, que la dirección destino y la dirección del siguiente salto coinciden en la tabla local de ruteo.
2. En el envío: Las interfaces de entrada y salida están activadas en modo MPLS. Si las interfaces están arriba en la capa física y en la capa enlace entonces el LSP está arriba.
3. A la salida: La interfaz de entrada a la salida es activada con MPLS. Si la interfaz de entrada está arriba en la capa física y enlace entonces el LSP está activo.

En la figura 1.9 se presenta un diagrama de flujo que resume de una manera más clara lo antes expuesto.

Hay que considerar que un LSP estático es configurado sin un LDP o un control de intercambio de paquetes. Por lo tanto el LSP estático tiene un costo bajo y puede ser aplicable a redes pequeñas con una topología simple y estable.

1.1.6.2 Establecer un LSP Dinámico

Estos LSP´s son configurados automáticamente por el LDP. Los siguientes LDP´s son aplicables a una red MPLS:

- **LDP:** El LDP es especialmente definido para la distribución de etiquetas. Este no está directamente asociado con protocolos de ruteo pero indirectamente usa información de enrutamiento.

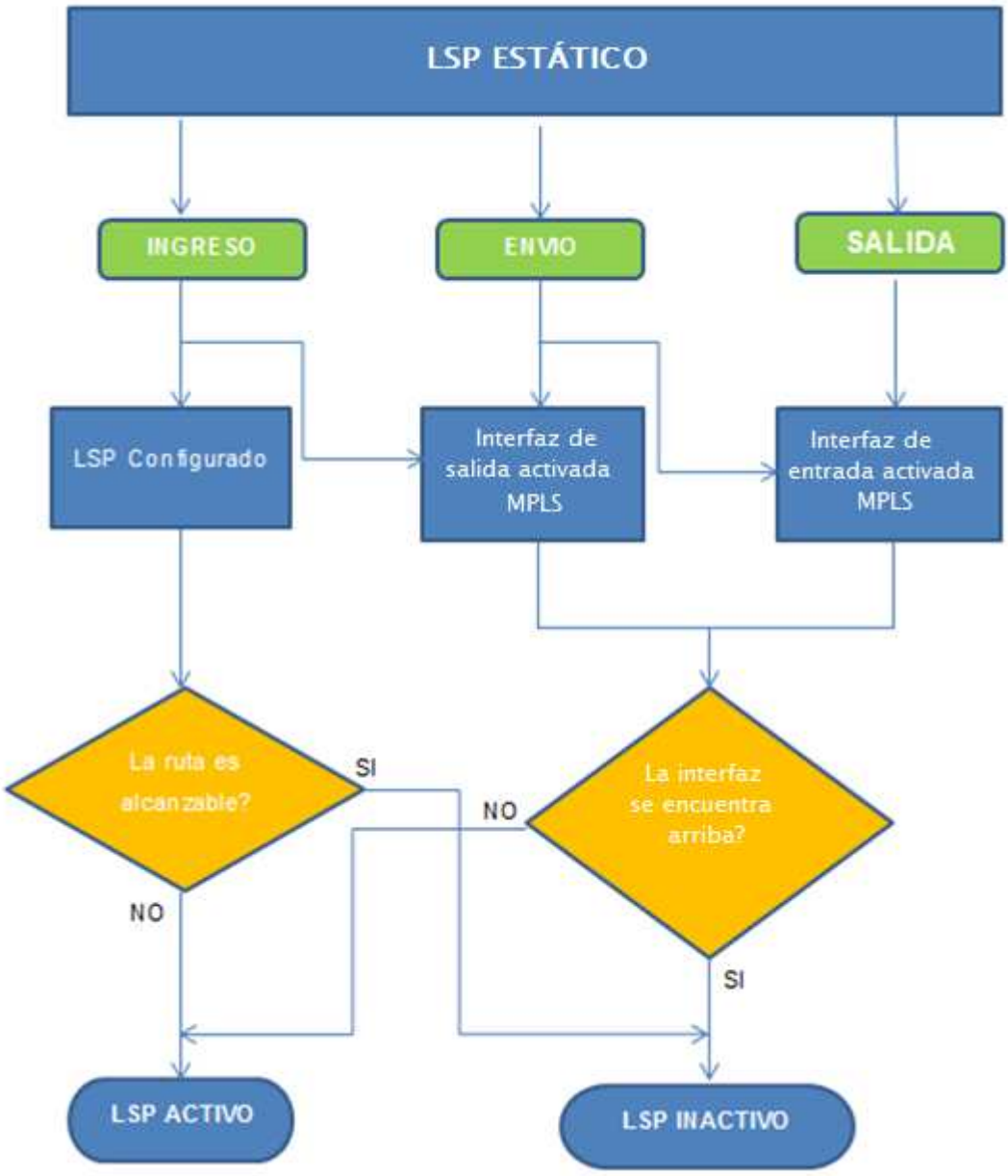


Figura 1.9: Diagrama de Flujo del LSP estático

- **RSVP-TE (Resource Reservation Protocol - Traffic Engineering – Protocolo de Reserva de Recursos – Ingeniería de Tráfico):** Se encarga de la reserva de recursos como canales o rutas en MPLS para después realizar la transmisión, trabaja en la capa de transporte. Es un protocolo de control de red. Un RSPV extendido es llamado RSPV-TE, es usado para configurar los túneles TE.
- **MP-BGP:** Tenemos este caso cuando el protocolo BGP permite intercambiar rutas dentro de una misma VPN.

1.1.7 REENVÍO EN MPLS [5] [6] [7]

1.1.7.1 Conceptos Básicos

- **ID de túnel:** Provee una interfaz común entre diferentes capas; el sistema automáticamente localiza el ID de cada túnel. El túnel solo tiene validez localmente. Este tiene una longitud de 32 bits que puede variar de acuerdo al tipo de túnel.
- **NHLFE (Next Hop Label Forwarding Entry – Entrada de Reenvío de Etiqueta del Siguiente Salto):** Se encarga de guiar los paquetes de la MPLS que se van a reenviar. Contiene la siguiente información:
    - ID de túnel.
    - Interfaz de salida.
    - Siguiente salto.
    - Etiqueta de salida.
    - Operación de etiquetas.
- **ILM (Incoming Label Map – Mapa de Etiquetas Entrantes):** Indica el mapeo entre las etiquetas; entre una etiqueta de entrada y las entradas NHLFE. Contiene la siguiente información:
    - D de túnel.
    - Etiqueta de entrada.
    - Interfaz de entrada.
    - Operación de etiqueta.
- **FTN (FEC hacia NHLFE):** Indica el mapeo entre una FEC y una entrada NHFLE, es usado para paquetes no etiquetados.

1.1.7.2 Proceso de reenvío

Un LSP cuyo FEC es identificado por la dirección destino es configurado en la red MPLS. Se reenvía de la siguiente manera:

1. Al ingreso recibe un paquete IP destinado a una dirección. Luego se asigna una etiqueta y lo reenvía.

2. El nodo de tránsito recibe el paquete etiquetado e intercambia las etiquetas.
3. El penúltimo router de tránsito recibe el paquete retira la etiqueta y reenvía el paquete al nodo de salida, este paquete es transmitido como un paquete IP.
4. Después, el nodo de salida recibe el paquete IP y lo reenvía a la dirección mencionada en el paso 1.

1.1.7.3 Flujo de reenvío

Cuando un paquete IP entra a un dominio MPLS, el router de ingreso busca en el FIB a que ID de túnel corresponde la dirección IP de destino; si la ID de túnel es 0x0 el paquete se envía a través del enlace IP, pero si es distinto de 0x0 se envía a través de un LSP. La figura 1.10 muestra el funcionamiento de un flujo de reenvío en MPLS.

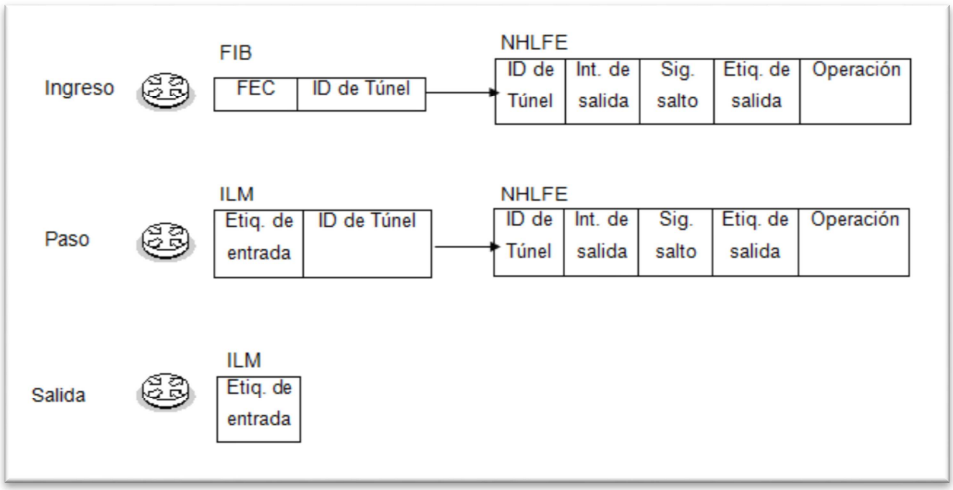


Figura 1.10: Flujo de reenvío MPLS [5]

Un paquete MPLS es reenviado a través de la red por un LSP de la siguiente manera:

1. El router de ingreso busca en las tablas FIB (Forwarding Information Base) y NHFLE para reenviar paquetes MPLS.

2. El router de tránsito busca en las tablas ILM y NHLFE para reenviar el paquete MPLS.
3. El router de salida busca en la tabla ILM para reenviar los paquetes MPLS.

1.1.7.3.1 Reenvío en el router de ingreso

El router de ingreso procesa de la siguiente manera los paquetes MPLS:

1. Busca en la FIB y encuentra el ID de túnel correspondiente a la dirección IP destino.
2. Encuentra el NHLFE correspondiente a ese ID de túnel en el FIB, y asocia la entrada FIB con la entrada NHLFE.
3. Chequea la NHLFE por información acerca de la interfaz de salida, siguiente salto, etiqueta de salida, y el tipo de operación de etiqueta. El tipo de operación de etiqueta es PUSH.
4. Procesa el campo EXP de acuerdo a la QoS y al TTL, luego envía encapsulado el paquete IP al siguiente salto.

1.1.7.3.2 Renvío en los routers de paso

1. Chequea la tabla ILM correspondiente a una etiqueta MPLS y encuentra el token.
2. Encuentra el NHFLE correspondiente al token en la tabla ILM.
3. Chequea el NHFLE para obtener información acerca de la interfaz de salida, siguiente salto, tipo de operación de la etiqueta.
4. Los paquetes MPLS son procesados de acuerdo al valor específico de la etiqueta.

1.1.7.3.3 Reenvío en el router de salida

Cuando recibe el paquete, chequea la tabla ILM para revisar el tipo de operación de la etiqueta. Al mismo tiempo procesa el campo EXP y TTL.

1.1.8 APLICACIONES DE MPLS [1] [6]

1.1.8.1 VPN Basada en MPLS

Es una red privada montada sobre un medio compartido, la base de este modelo es de pares, los routers de backbone o de paso reciben y mantienen la información de las VPNs conectadas a ellos. Al usar MPLS no se necesita conocer información del cliente.
Esta red integra una rama de una red privada a través de un LSP para formar una red unificada. Se tiene dos tipos de elementos:

- **CE:** Customer Edge – Cliente de Borde, es un nodo de frontera en la red del cliente que puede ser un router, un switch o un host.
- **PE:** Provider Edge – Proveedor de Borde, es un nodo de frontera en la red de servicios del proveedor.

1.1.8.2 PBR a un LSP

Esto significa seleccionar una ruta de acuerdo a una política definida por un usuario, para seguridad y balanceo de carga. En una red MPLS los paquetes IP que cumplen con la política pueden ser filtrados y reenviados a través de un LSP específico.

1.2 PROTOCOLO DE IP VERSIÓN 6 (IPV6)

1.2.1 ORIGEN [3]

La evidente falta de direcciones IP`s crea la necesidad de poder desarrollar un nuevo protocolo; y es ahí cuando la IETF (Internet Engineering Task Force – Fuerza de Tareas de Ingeniería de Internet) comienza a trabajar en lo que en primera instancia se denominó IPng (Internet Protocol Next Generation – Siguiente Generación del Protocolo de Internet) y que hoy en día se lo llama PROTOCOLO IPV6.

El espacio de direcciones que IPV4 nos presenta es de 32 bits (2^{32} direcciones) y por otro lado IPV6 nos ofrece un espacio de 128 bits (2^{128} direcciones). Pero este no es el único inconveniente que este nuevo protocolo soluciona.

La enorme evolución de las Tecnologías de la Información ha hecho que nuevas tecnologías puedan llegar a ser soportadas en IPV4 tales como Calidad de Servicio (QoS), Seguridad (IPsec), Movilidad, tablas de enrutamiento, entre otras, las cuales de manera individual funcionan sin ningún problema ni complejidad pero a la hora de juntarlas se vuelven un dolor de cabeza o algo realmente inmanejable.

El reducido espacio de IPV4 y la falta de organización al entregar las direcciones IP sin ningún tipo de optimización hacen que las cuatro mil millones de direcciones se estén agotando; algo que nunca se imaginó que iba a ocurrir.

La razón de utilización de direcciones IP por parte de los usuarios está pasando de 10:1 a 1:1 y en pocos meses esta tendencia se invertirá. Algunos ISP`s optan por asignar a sus clientes direcciones IP privadas mediante mecanismo de NAT[7] (Network Address Traslation – Traducción de Dirección de Red) pero esto no se puede tomar como una solución definitiva ya que el NAT cambia la dirección de la cabecera IP y no permitiría el manejo de aplicaciones como:

- RTP y RTCP (Protocolo de Transporte de Tiempo Real y Protocolo de Control de Tiempo Real): utilizan UDP con asignación dinámica de puertos.
- Autenticación Kerberos: se necesita la dirección fuente para la autenticación.
- Multicast.

“El camino de IPV4 a IPV6 no es una cuestión de transición ni de migración, sino de evolución, de integración, pero se trata de una evolución disruptora, rompedora, y al mismo tiempo necesaria.” [8]

[7] Es un sistema que se utiliza para asignar una red completa (o varias redes) a una sola dirección IP.
[8] Foro IPV6, Tutorial de IPV6, Pag. 5.

1.2.2 CARACTERÍSTICAS PRINCIPALES [2] [3]

De forma resumida las principales características del Protocolo IPV6 son las siguientes:

- Mayor espacio de direcciones (2^{128}).
- Autoconfiguración “Plug & Play”.
- IPsec (Internet Protocol Security – Protocolo de Seguridad de Internet): usando la cabecera de autenticación y de extensión.
- Calidad de Servicio (QoS) y Clase de Servicio (CoS).
- Multicast: envío de un mismo paquete a un grupo de receptores.
- Anycast: envío de un paquete a un receptor dentro de un grupo.
- Movilidad.
- Multi-homing: técnica usada para aumentar la confidencialidad de la conexión a Internet.
- Paquetes con carga de datos (útil) de más de 65535 bytes.
- Enrutamiento más eficiente en el backbone de una red debido a una jerarquía de direccionamiento basada en agregación.
- Paquetes IP eficientes y extensibles que evitan fragmentación en routers, alineados a 64 bits y con cabecera de longitud fija.

1.2.3 ESPECIFICACIONES DE IPV6 [2] [3] [8]

1.2.3.1 Cabecera de un paquete IPV4

En la figura 1.11 se puede observar el formato de la cabecera de un paquete IPV4.

A continuación se detallan los campos de la cabecera:

- **Versión (4 bits):** describe el formato de la cabecera; en este caso es IPV4 (0100).

- **Tamaño Cabecera (4 bits):** longitud de la cabecera en palabras de 32 bits; el tamaño mínimo es 5 y el máximo de 15**.**
- **Tipo de servicio (8 bits):** permite al host indicar a la subred el tipo de servicio que quiere. Son posibles varias combinaciones de confiabilidad y velocidad.
- **Longitud total (16 bits):** es el tamaño total en octetos del datagrama, incluyendo el tamaño de la cabecera y de los datos.
- **Identificador (16 bits):** es necesario para que el host destino determine a qué datagrama pertenece un fragmento recién llegado. Todos los fragmentos de un datagrama contienen el mismo valor de identificación.
- **Flags - Banderas (3 bits):** utilizado para especificar valores relativos a la fragmentación de paquetes.
- **Posición de Fragmento (13 bits):** en paquetes fragmentados indica la posición, en unidades de 64 bits, que ocupa el paquete actual dentro del datagrama original.
- **Tiempo de vida (8 bits):** es un contador que sirve para limitar la vida del paquete.
- **Protocolo (8 bits):** indica el protocolo de siguiente nivel utilizado en la parte de datos del datagrama.
- **Suma de control de cabecera (16 bits):** Se recalcula cada vez que algún nodo cambia alguno de sus campos (por ejemplo, el Tiempo de Vida). El método de cálculo -intencionadamente simple- consiste en sumar en complemento a 1 cada palabra de 16 bits de la cabecera (considerando valor 0 para el campo de suma de control de cabecera) y hacer el complemento a 1 del valor resultante.
- **Dirección IP origen (32 bits):** dirección IP de donde proviene el paquete IP.
- **Dirección IP destino (32 bits):** dirección de destino del paquete IP.
- **Opciones y Relleno (32 bits):** campos no obligatorios y variables.

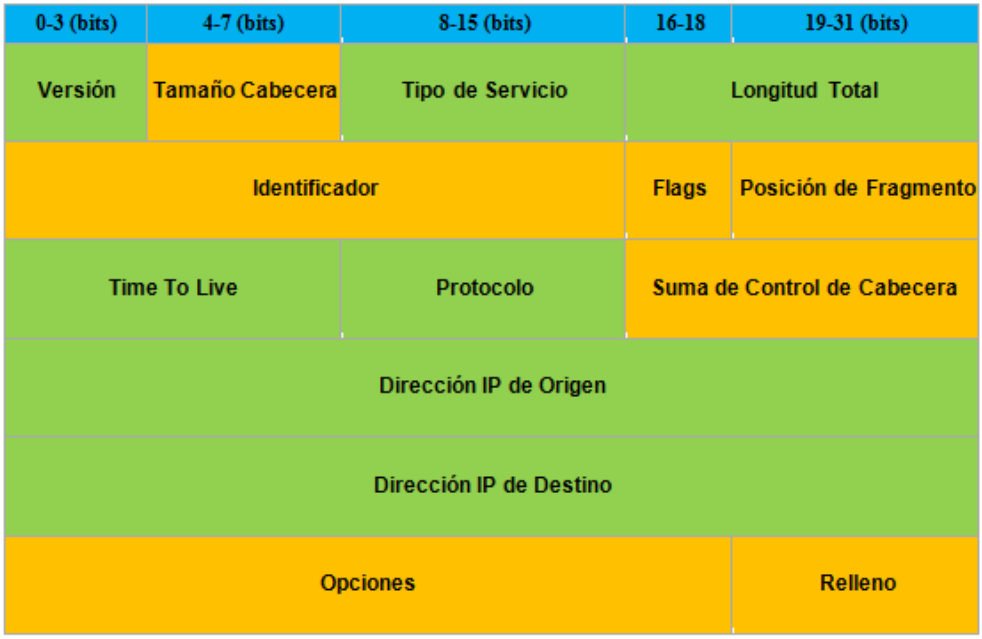


Figura 1.11: Cabecera IPV4 [8]

1.2.3.2 Cabecera de un paquete IPV6

En la figura anterior se ha delimitado con colores los campos que van a desaparecer en IPV6 y los modificados de la siguiente manera:

CAMPO MODIFICADO
CAMPO QUE DESAPARECE

El motivo de que se eliminen algunos campos es debido a la innecesaria redundancia y entonces se pasa de tener 12 campos en IPV4 a tener tan solo 8 en IPV6. La figura 1.12 muestra la cabecera IPV6.

A continuación se detallan los campos de la cabecera IPV6:

- **Versión (4 bits):** en este caso es V6 (0110).
- **Clase de Tráfico (8 bits):** también denominado Prioridad o Clase es el equivalente en IPV4 al Tipo de Servicio.
- **Etiqueta de Flujo (20 bits):** sirve para permitir tráfico con requisitos de tiempo real (voz, video, etc).

- **Longitud de la Carga Útil (16 bits):** o también llamado tamaño de los datos, especifica la longitud de los datos del paquete IPV6 sin incluir la cabecera.
- **Siguiente cabecera (8 bits):** campo que identifica el tipo de cabecera que le sigue inmediatamente a la cabecera básica de IPV6.
- **Límite de saltos (8 bits):** campo sin signo y disminuye en uno por cada nodo que reenvía al paquete; cuando éste llega a cero se descarta el paquete.
- **Dirección IP origen (128 bits):** dirección IP de donde proviene el paquete IP.
- **Dirección IP destino (128 bits):** dirección de destino del paquete IP.

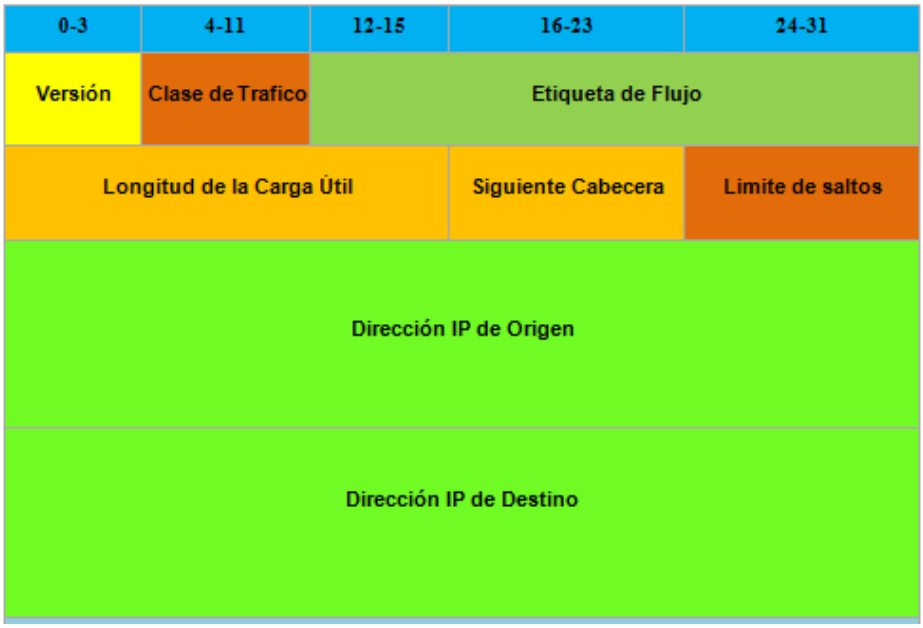


Figura 1.12: Cabecera IPV6 [8]

1.2.4 CABECERAS DE EXTENSIÓN IPV6 [2] [8] [9]

La cabecera estándar en IPV6 es de tamaño fijo y en algunas ocasiones se requiere ampliarla con las “cabeceras de extensión”, que permiten dar servicios adicionales como: reserva de recursos en red, fragmentación, etc.

Estas cabeceras de extensión están situadas entre la cabecera de IPV6 y las de nivel superior utilizando el campo “siguiente cabecera”; las mismas no son

procesadas ni examinadas a lo largo de la ruta salvo en el nodo de destino, a excepción de la cabecera de extensión de "**opciones de salto a salto"** en la cual viaja información que debe ser procesada en todos los nodos.

La arquitectura de las cabeceras de extensión se muestra en la figura 1.13.

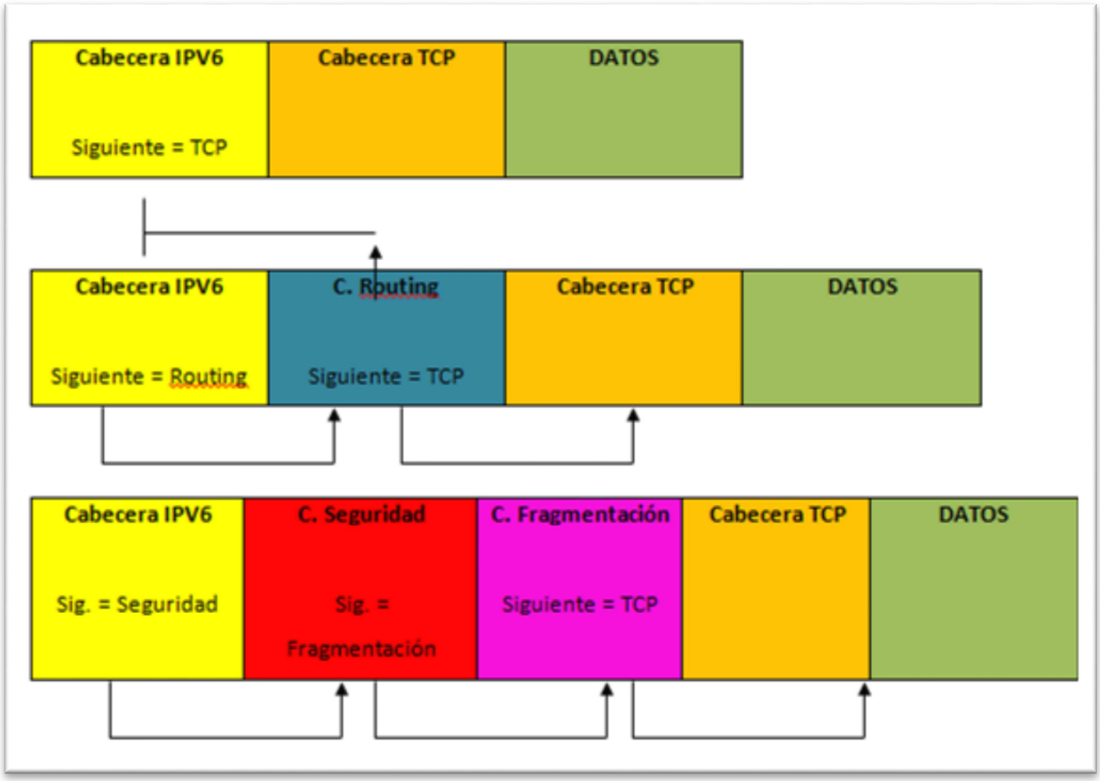


Figura 1.13: Cabeceras de extensión IPV6 [8]

El tamaño de las cabeceras de extensión para poder ser alineadas con la cabecera IPV6 deberá ser múltiplo de 8 octetos.

1.2.4.1 Tipos de cabecera de extensión

Actualmente se definen 6 clases de cabecera de extensión:

- **Opciones de Salto a Salto:** cabecera de extensión IPv6 que contiene opciones que deben ser procesadas por todos los nodos.

- **Enrutamiento:** cabecera de extensión IPv6 que contiene la lista de enrutadores total o parcial de la ruta a seguir.
- **Fragmentación:** Cabecera de extensión IPv6 enviada por el nodo origen, que contiene la información necesaria para el re-ensamblado por parte del nodo destino.
- **Autenticación:** Verificación de la autenticidad del emisor (RFC-1827 y RFC-1825).
- **Cabecera seguridad del encapsulado de la carga útil**: información sobre los tipos de mecanismos de seguridad utilizados para garantizar los servicios de confidencialidad e integridad del contenido cifrado en el campo datos del datagrama (RFC-1827 y RFC-1825).
- **Cabecera de Opciones para destino**: información opcional que debe ser procesada por el destino final del datagrama.

1.2.4.2 Orden de las cabeceras de extensión

Es importante recordar el orden propuesto tanto para las cabeceras de extensión como para las cabeceras de los paquetes tal como se especifica en el RFC 2460:

1. Cabecera IPV6.
2. Cabecera opciones de salto a salto.
3. Cabecera opciones de destino.
4. Cabecera de enrutamiento.
5. Cabecera de fragmentación.
6. Cabecera de Autenticación.
7. Cabecera seguridad del encapsulado de la carga útil.
8. Cabecera opciones de destino.
9. Cabecera de capa superior.

Las cabeceras de extensión aparecerán solo una vez, con excepción de la cabecera “opciones de destino” que aparecerá justo antes de la “cabecera de enrutamiento” y antes de la “cabecera de capa superior”.

1.2.4.3 Opciones de la cabecera de extensión

La figura 1.14 corresponde a las cabeceras de opciones salto a salto y de encaminamiento las cuales tienen un número variable de opciones.

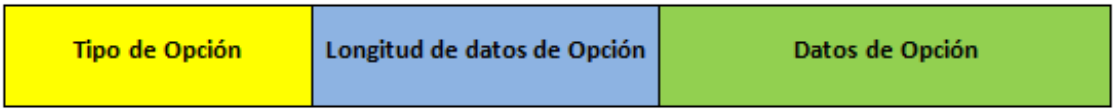


Figura 1.14: Opciones de cabecera de extensión IPV6 [8]

- **Tipo de Opción:** campo de 8 bits (2 bits de acción + 1 bit de modificación de encaminado + 5 bits de tipo de opción); identifica el tipo de opción.
- **Longitud de datos de Opción:** campo de 8 bits; valor entero sin signo el cual especifica la longitud en octetos del campo “Datos de Opción”.
- **Datos de Opción:** campo de longitud variable el cual corresponde a los datos específicos del campo “Tipo de opción”.

Para el campo “Tipo de Opción” se utilizan los 5 bits menos significativos para especificar una opción en particular; si el nodo IPV6 no reconoce el tipo de acción, los 2 bits de más alto orden especifican las acciones a tomar en base a la tabla 1.1.

El bit de modificación de encaminado se utiliza para indicar si los “datos de opción” modifican o no el encaminado hacia el destino final del paquete tal como se indica en la tabla 1.2.

1.2.4.4 Cabecera opciones salto a salto

Esta cabecera se encuentra presente en aquellos paquetes IPV6 que llevan un valor de cero en el campo “cabecera siguiente” y se utiliza para llevar información opcional a todos los nodos que conforman el camino que recorre el paquete. El formato se muestra en la figura 1.15.

Bits de acción	Acción
00	Ignorar esta opción y continuar procesando la cabecera.
01	Descartar el paquete completo.
10	Sin tener en cuenta si el destino es multicast o no descartar el paquete y devolver al origen un ICMP con código 2 (problema de parámetro), señalando “tipo de opción desconocido”.
11	Descartar el paquete y enviar un ICMP con código 2 (problema de parámetro) a la dirección de origen siempre y cuando la dirección de destino no sea multicast.

Tabla 1.1: Bits de acción [2]

Bit de modificación	Campo de datos de Opción	Autenticación
0	No cambia el encaminamiento.	No se excluyen los cálculos de autenticación.
1	Cambia el encaminamiento.	Se excluyen los cálculos de autenticación.

Tabla 1.2: Bits de modificación [2]

Figura 1.15: Cabecera de opciones salto a salto [8]

- **Cabecera siguiente:** campo de 8 bits que indica el tipo de cabecera que está a continuación de ésta.
- **Longitud de cabecera:** campo de 8 bits sin signo y de valor entero; especifica la longitud de la cabecera en octetos y excluye el primer octeto en este valor.

- **Opciones:** campo de longitud variable; la longitud de la cabecera completa es un entero múltiplo de 64 bits y se debe tener un tamaño que permita la alineación del paquete; para ello se podrá utilizar Pad1 y PadN.

1.2.4.4.1 Pad1 y PadN:

Debido a que las opciones individuales pueden no tener un tamaño necesario para cubrir la trama de n*8 octetos será necesario utilizar opciones de relleno, las cuales están representadas mediante la expresión **xn + y**, donde **x** representa el número de octetos a desplazar a partir del comienzo de la cabecera e **y** representa el número de octetos a desplazar.

Por ejemplo: 4x+2 significa un desplazamiento de 4 octetos a partir del inicio del paquete y adicionalmente 2 octetos más. Cuando es necesario alinear opciones a la cabecera contenedora existen 2 opciones de relleno:

- La opción Pad1 no dispone de campos de longitud ni de datos de la opción y se la utiliza cuando es necesario añadir un único octeto al área de opciones de una cabecera.
- Cuando se requiere más octetos de relleno es necesario utilizar la opción PadN, la cual está compuesta por un primer octeto de 1s y otro octeto donde se define el campo “longitud de datos de opción” y un único campo de tamaño N-2 octetos compuestos de ceros.

1.2.4.5 Cabecera de enrutamiento

Se tienen 2 tipos de cabeceras de enrutamiento las cuales se detallan a continuación:

1.2.4.5.1 Cabecera de enrutamiento Genérica

Esta cabecera es utilizada por el origen para realizar una lista de los nodos intermedios que existen hacia el destino por donde el paquete IPV6 va a pasar. La cabecera de enrutamiento se encuentra determinada por una “cabecera siguiente” que tiene un valor 43. El formato para la cabecera de enrutamiento genérica se puede apreciar en la figura 1.16.

Figura 1.16: Cabecera de enrutamiento genérica [8]

- **Cabecera Siguiente:** campo de 8 bits; determina el tipo de cabecera que tendrá la que le sigue a la cabecera de Enrutamiento; su valor es de 43.
- **Longitud de Extensión:** campo de 8 bits entero y sin signo el cual determina la longitud en unidades de 8 octetos de la cabecera de enrutamiento y no incluye los primeros 8 octetos.
- **Tipo de Enrutamiento:** campo de 8 bits el cual identifica una variante en particular de la cabecera de Enrutamiento.
- **Segmentos Restantes:** campo de 8 bits sin signo y entero el cual delimita el número de nodos intermedios previamente listados que faltan ser visitados por el paquete antes que llegue a su destino.
- **Datos Específicos del Tipo:** campo de longitud variable el cual tiene un formato definido por el tipo de enrutamiento y es un múltiplo entero de 64 bits.

Cuando un nodo encuentra una Cabecera de Enrutamiento con valor “Tipo de Enrutamiento desconocido” el nodo se comportará de acuerdo al valor que tenga el campo “Segmento Restante” de la siguiente manera:

a) Si el valor es cero, se debe ignorar la cabecera y proceder a procesar la siguiente cabecera.

b) Si el valor es diferente de cero, el nodo debe descartar el paquete y enviará un mensaje ICMP[9] con código 0 (problema de parámetro) hacia el origen.

Si un nodo intermedio determina que el paquete va a ser remitido hacia un enlace cuyo MTU[10] es menor que el tamaño del paquete mismo, el nodo debe descartar el paquete y enviar al origen un mensaje ICMP “Paquete demasiado grande”.

1.2.4.5.2 Cabecera de enrutamiento Tipo 0

La particularidad de la cabecera de enrutamiento tipo 0 es que la misma no se procesa en cada nodo sino únicamente en el nodo destino; el formato de esta cabecera se visualiza en la figura 1.17.

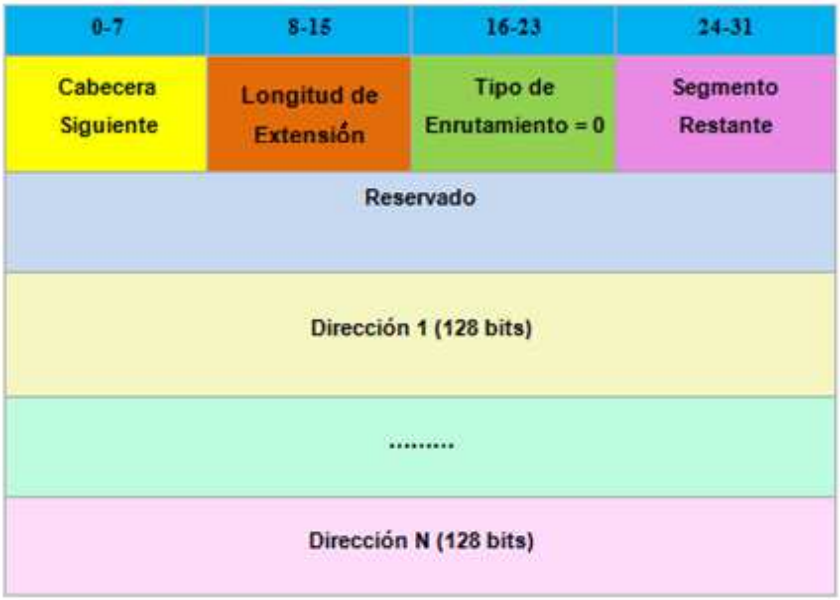


Figura 1.17: Cabecera de enrutamiento Tipo 0 [8]

- **Cabecera Siguiente:** campo de 8 bits; determina el tipo de cabecera que tendrá la que le sigue a la cabecera de Enrutamiento.
- **Longitud de Extensión:** campo de 8 bits entero y sin signo el cual determina la longitud en unidades de 8 octetos de la cabecera de

[9] El Protocolo de Mensajes de Control de Internet es el sub protocolo de control y notificación de errores del Protocolo de Internet (IP).
[10] Es un parámetro que indica el tamaño máximo que debe tener un datagrama para que sea transmitido por una interfaz IP sin que necesite ser fragmentado en unidades más pequeñas.

enrutamiento y no incluye los primeros 8 octetos. La longitud de extensión es 2 veces el número de direcciones en la cabecera.

- **Tipo de enrutamiento:** campo de 8 bits cuyo valor es cero.
- **Segmentos Restantes:** campo de 8 bits sin signo y entero el cual delimita el número de nodos intermedios previamente listados que faltan ser visitados por el paquete antes que llegue a su destino.
- **Reservado:** campo de 32 bits reservado el cual es inicializado en cero en la transmisión para ser ignorado en la recepción.
- **Dirección 1…N:** vector de direcciones de 128 bits, numerados desde 1 hasta N.

1.2.4.6 Cabecera de Fragmentación

Esta cabecera es utilizada por el nodo origen para poder transportar paquetes con un MTU (Maximun Transmit Unit) más grande que el de la ruta hacia su destino. La fragmentación solo se la realiza por los nodos origen a diferencia de IPV4 que lo realiza en cada nodo intermedio. La cabecera de fragmentación es identificada por un valor de 44 de la cabecera siguiente (se encuentra precediéndola) y su formato es mostrado en la figura 1.18.

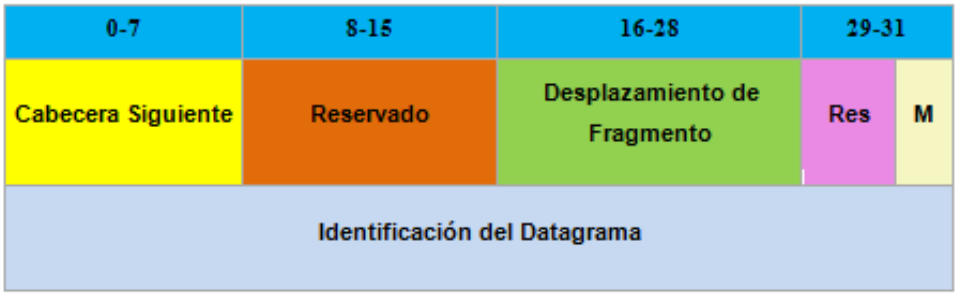


Figura 1.18: Cabecera de fragmentación [8]

- **Cabecera siguiente:** campo de 8 bits que identifica el tipo de cabecera inicial de la parte fragmentable del paquete original.
- **Reservado:** campo de 8 bits reservado el cual es inicializado en cero en la transmisión para ser ignorado en la recepción.

- **Desplazamiento de Fragmento:** campo de 13 bits de valor entero y sin signo; identifica el desplazamiento en unidades de 8 octetos de los datos que le siguen a esta cabecera; relativo al comienzo de la parte fragmentable del paquete original.
- **Res:** campo de 2 bits reservado el cual es inicializado en cero en la transmisión para ser ignorado en la recepción.
- **Bandera M:** campo de 1 bit el cual si su valor es 1 quiere decir que existen más fragmentos y si es 0 indica que es el último fragmento.
- **Identificación del Datagrama:** campo de 32 bits que define la identificación del fragmento la cual es diferente de cualquier otro paquete enviado recientemente con la misma dirección origen y destino.

1.2.4.6.1 Paquete original

El paquete sin fragmentar (grande) es denominado “paquete original” y consta de dos partes:

- **Parte no fragmentable:** conformada por la cabecera IPV6 más cualquier cabecera de extensión y debe procesarse por los nodos intermedios hasta llegar al destino.
- **Parte fragmentable:** es el resto del paquete mismo, es decir cualquiera de las cabeceras de extensión que necesite ser procesada por el nodo en el destino, más la cabecera de capa superior y los datos.

1.2.4.7 Cabecera Opciones de Destino

La cabecera Opciones de Destino es usada para llevar información opcional que necesita ser examinada solamente por el(los) nodo(s) destino del paquete. La cabecera Opciones de Destino es identificada por un valor Cabecera Siguiente de 60 en la cabecera inmediatamente precedente, la figura 1.19 muestra el formato de la cabecera opciones de destino.

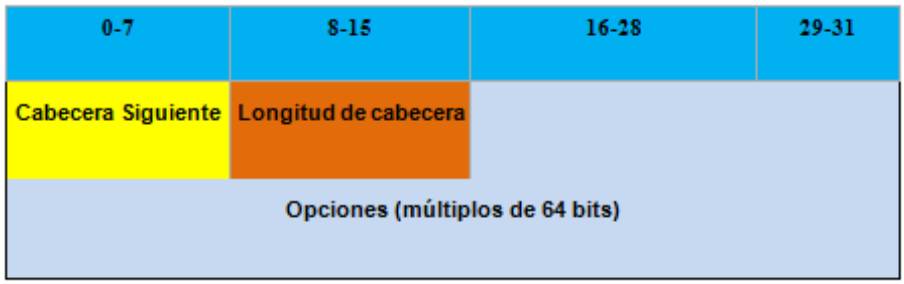


Figura 1.19: Cabecera opciones de destino [3]

- **Cabecera Siguiente:** campo de 8 bits. Identifica el tipo de cabecera que sigue inmediatamente a la cabecera Opciones de Destino. Utiliza los mismos valores que el campo Protocolo del IPv4.
- **Longitud de Cabecera:** campo sin signo de 8 bits; la longitud de la cabecera Opciones de Destino viene en unidades de 8 octetos, no incluye los primeros 8 octetos.
- **Opciones:** Campo de longitud variable, de longitud tal que la cabecera Opciones de Destino completa es un entero múltiplo de 8 octetos de largo. Contiene uno o más opciones codificadas TLV[11],

1.2.4.8 Cabecera No Hay Siguiente

El valor 59 en el campo Cabecera Siguiente de una cabecera IPv6 o de cualquier cabecera de extensión indica que nada hay siguiendo esa cabecera. Si el campo Longitud de la Carga Útil de la cabecera IPv6 indica la presencia de octetos más allá del final de una cabecera cuyo campo Cabecera Siguiente contiene 59, esos octetos deben ignorarse, y pasarse inalterados si el paquete se reenvía.

1.2.5 DIRECCIONAMIENTO IPV6 [2] [5] [9] [10] [11]

Los routers que soportan IPv6 ya no realizan la fragmentación[12]; si el dispositivo recibe un mensaje ICMP "demasiado grande", retransmite el paquete de descubrimiento MTU con una MTU más pequeña, este proceso se repite hasta

[11] Se denomina tipo-longitud-valor o valores de longitud tipo a un formato de representar información, de forma que haya información que pueda tener presencia opcional y longitud variable.
[12] Técnica utilizada para dividir los datagramas IP en fragmentos de menor tamaño.

que el dispositivo recibe una respuesta que el paquete de descubrimiento llegó intacto.

Un proceso de descubrimiento se utiliza para determinar la MTU óptima para su uso durante una sesión dada. En este proceso de detección, el dispositivo de IPv6 origen intenta enviar un paquete del tamaño que se especifica en las capas IP superiores, por ejemplo, las capas de transporte y aplicación.

Una dirección IPv6 aumenta el número de bits por un factor de 4, del 32 a 128, proporcionando un gran número de nodos direccionables. La figura 1.20 muestra una comparación entre la dirección IPV4 & IPV6 en cuanto a los bits.

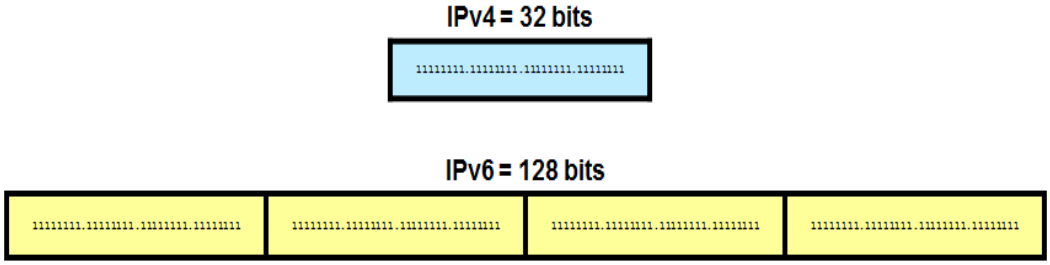


Figura 1.20: bits de direccionamiento IPV4 vs IPV6 [2]

1.2.5.1 Especificaciones de una dirección IPV6

La dirección IPv6 de 128 bits se escribe con números hexadecimales; en concreto, se compone de 8 segmentos de 16 bits separados por dos puntos entre cada conjunto de cuatro dígitos hexadecimales (16 bits).

Se denomina formato "hexadecimal coloned" y se lo representa como **x:x:x:x:x:x:x:x**, donde **x** es un campo hexadecimal de 16 bits por lo que cada x representa a cuatro dígitos hexadecimales. Una dirección IPV6 puede ser la siguiente: 2035:0001:2BC5:0000:0000:087C:0000:000A.

1.2.5.2 Abreviación de direcciones IPV6

Los principales 0`s dentro de cada conjunto de cuatro dígitos hexadecimales se pueden omitir de la siguiente manera:

- **09C0** = **9C0**
- **0000** = **0**

Un par de dos puntos ("::") se puede utilizar, una vez dentro de una dirección, para representar cualquier número ("un montón") de 0`s sucesivos. En la figura 1. 21 se puede observar un ejemplo de cómo se abrevian las direcciones IPV6.

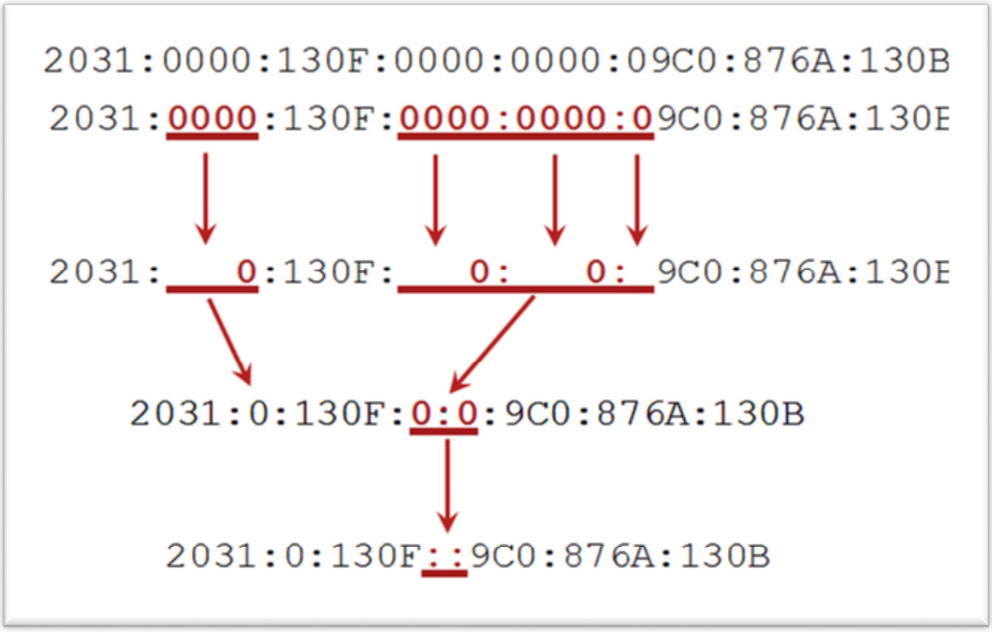


Figura 1.21: Ejemplo de abreviación IPV6

1.2.5.3 Direccionamiento IPV6 en una red empresarial

Una dirección IPv6 se compone de dos partes:

- **Un prefijo de subred:** representa la red a la que está conectada la interfaz. Generalmente de 64-bits de longitud.
- **Un ID de interfaz:** a veces llamado un identificador local o una ficha. Generalmente 64-bits de longitud.

La figura 1.22 muestra el formato de una dirección IPV6 en una red empresarial.

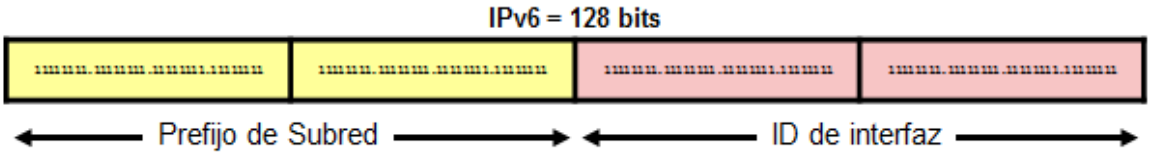


Figura 1.22: Dirección IPV6 en una red empresarial [2]

1.2.5.3.1 Prefijo de Subred

IPv6 utiliza la notación CIDR "/ longitud-prefijo" para indicar el número de bits de la dirección IPv6 representa la subred. La sintaxis es dirección-ipv6 / longitud-prefijo en donde:

- **Dirección IPv6:** es la dirección IPv6 de 128 bits.
- **/ longitud-prefijo:** es un valor decimal que representa cuantos de los más contiguos bits a la izquierda de la dirección componen el prefijo.

La figura 1.23 muestra un ejemplo del prefijo de subred.

Figura 1.23: Ejemplo de prefijo de subred [9]

La longitud del prefijo es casi siempre /64; sin embargo, las reglas IPv6 permiten prefijos cortos o más largos. Aunque prefijos menores a /64 se pueden asignar a un dispositivo (por ejemplo, /60), se considera mala práctica sin aplicación real.

1.2.5.3.2 Identificadores de interfaces

Las direcciones IPv6 en un enlace deben ser únicas; a pesar de que todas comparten el mismo prefijo de subred de 64 bits, se hacen únicas por el ID de interfaz. Debido a que la longitud de prefijo es fija y conocida (64-bits), los hosts

IPv6 pueden crear automáticamente una dirección IPv6 única. Por ejemplo, los siguientes protocolos de capa 2 pueden crear dinámicamente la dirección de ID de interfaz IPv6:

- Ethernet.
- PPP.
- HDLC.
- NBMA, Frame Relay.

1.2.5.4 Direcciones IPV6 especiales

La tabla 1.3 especifica las direcciones IPV6 especiales con su respectiva descripción.

Dirección IPV6	Descripción
::/0	Utilizada para especificar una ruta por defecto; equivalente a la IP quad-zero (0.0.0.0).
::/128	Dirección no especificada y se asigna inicialmente a un host cuando se resuelve primero su dirección de enlace local.
::1/128	Dirección de loopback, equivalente a 127.0.0.0 en IPV4.
FE80::/10	Dirección unicast de enlace local.
FF00::/8	Direcciones Multicast.
Demás direcciones	Direcciones Unicast Globales.

Tabla 1.3: Direcciones IPV6 especiales [10]

1.2.6 ÁMBITOS DE DIRECCIONES IPV6 [2] [9] [10] [11]

Los tipos de direcciones tienen ámbitos bien definidos de destino; los cuales se pueden ver en la figura 1.24.

- Dirección Link-Local.
- Dirección Unique-Local.
- Dirección Unicast Global.

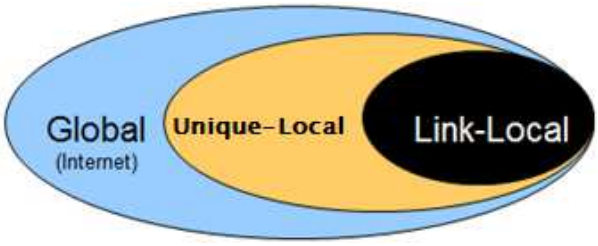


Figura 1.24: Ámbitos de direcciones IPV6 [2]

1.2.6.1 Direcciones Unique-Local

En 1993, el RFC 1884 reservó el bloque **FEC0::/20** para direcciones site –local. Sin embargo, una definición insuficiente del término "site" llevo a la confusión sobre las reglas de enrutamiento resultantes; por lo que el RFC 3879 eliminó este rango de direcciones y en octubre del 2005 en el RFC 4193 fue publicado, reservando el bloque de direcciones **FC00::/7** para uso en redes IPv6 privadas y asociando el término **"Direcciones Unique-Local"**. El bloque de direcciones **FC00::/7** se encuentra dividido en dos grupos /8:

- El bloque FC00::/8 no se encuentra definido todavía.
- El bloque FD00::/8 se encuentra definido por prefijos /48, formado mediante el establecimiento de los 40 bits menos significativos del prefijo a una cadena de bits generada de forma aleatoria. El resultado es el formato FDxx:xxxx:xxxx:: para un prefijo en este rango. El RFC 4193 ofrece una sugerencia para generar el identificador aleatorio y así obtener un resultado de calidad mínima si el usuario no tiene acceso a una buena fuente de números randómicos.

1.2.6.2 Múltiples direcciones IP por interfaz

Una interfaz puede tener múltiples direcciones IPv6 configuradas y habilitadas en forma simultánea; sin embargo, debe tener una dirección local de enlace (link-local). Por lo general, una interfaz se le asigna una dirección link-local y una (o más) direcciones IPv6 globales, adicionalmente una interfaz también puede ser configurada para soportar simultáneamente las direcciones IPv4 e IPv6.

Por ejemplo, una interfaz Ethernet puede tener:

- Dirección link-local (FE80::21B:D5FF:FE5B:A408).
- Dirección unicast global (2001:8:85A3:4289:21B:D5FF:FE5B:A408).

1.2.6.3 Dirección IPV6 Link-Local (enlace-local)

Las direcciones Link-Local se utilizan para la configuración automática de direcciones, el descubrimiento de vecinos, el descubrimiento de enrutadores, y por muchos protocolos de enrutamiento. Se crean dinámicamente utilizando un prefijo local de vínculo de **FE80::/10** y un identificador de interfaz de 64 bits tal como lo muestra la figura 1.25.
Son únicas sólo en el enlace, y no se pueden enrutar fuera del mismo.

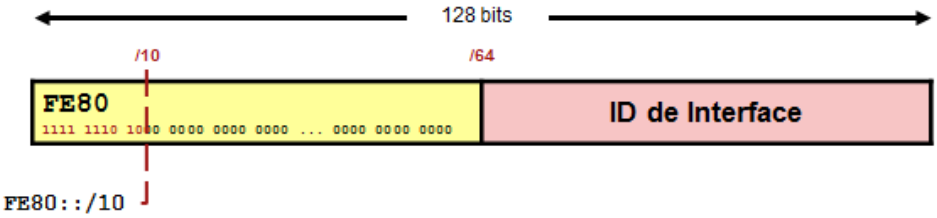


Figura 1.25: Dirección IPV6 Link-Local [2]

Los paquetes con un destino de enlace local deben permanecer en el enlace donde han sido generados.

En una comunicación con una dirección Link-Local, la interfaz de salida debe ser especificada por cada interfaz está conectada a **FE80::/ 10**. Por ejemplo, si se hace ping a la dirección Link-Local de los vecinos, se nos pedirá introducir la interfaz desde la que desea hacer el ping.

Un ejemplo de una dirección IPV6 de tipo Link-Local se puede observar en la figura 1.26.

```
R1# show ipv6 interface loopback 100
Loopback100 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::222:55FF:FE18:7DE8
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:8:85A3:4290:222:55FF:FE18:7DE8, subnet is 2001:8:85A3:4290::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF18:7DE8
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 31238)
  Hosts use stateless autoconfig for addresses.
R1#
```

Figura 1.26: Ejemplo de dirección IPV6 Link-Local [11]

1.2.6.4 Dirección IPV6 Unicast Global

Una dirección del tipo Unicast[13] Global es una dirección IPv6 del prefijo global unicast (**2001::/16**). La estructura permite la agregación de prefijos de enrutamiento para reducir el número de entradas de la tabla de enrutamiento global. Las direcciones unicast globales se agregan hacia arriba a través de las organizaciones y, finalmente, a los ISP´s.

La dirección Unicast Global normalmente consiste en:

- Un prefijo de enrutamiento global de 48 bits.
- Un ID de subred de 16 bits.
- Un ID de interfaz de 64 bits.

Tal y como se muestra en la figura 1.27.

13 Se basa en un proceso de envío de una información en una o más unidades de datos (datagramas IP) desde una máquina origen a una única máquina destinataria o receptor final.

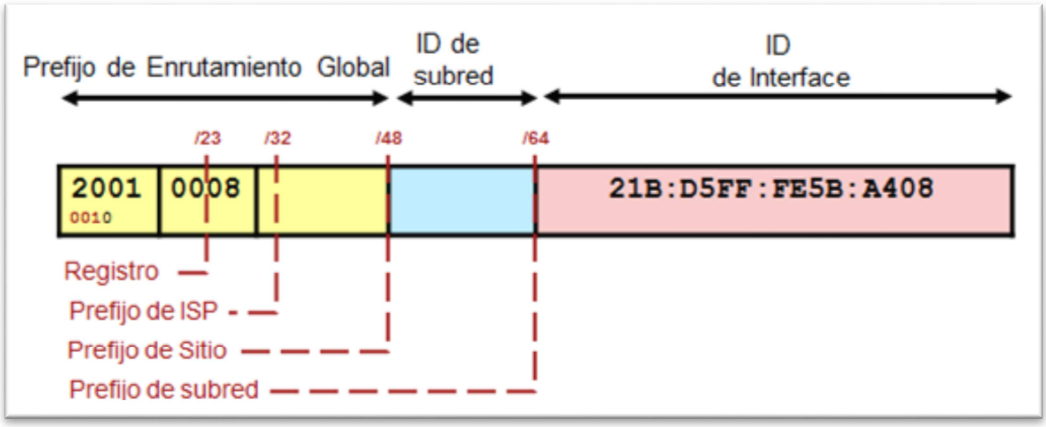


Figura 1.27: Ejemplo de trama IPV6 Link-Local [11]

El prefijo actual mundial de enrutamiento según IANA (Internet Assigned Numbers Authority)[14] utiliza el rango que comienza con binario 0010 (**2000::/3**). Las direcciones con el prefijo desde 2000::/3(001) al E000::/3 (111) están obligados a tener un ID de interfaz de 64 bits. El ID de subred puede ser utilizado por una organización para crear su propia jerarquía de direccionamiento local. Un ejemplo de dirección IPV6 del tipo Unicast Global se puede observar en la figura 1.28.

1.2.6.5 Dirección IPV6 Multicast

Multicasting es la base de muchas de las funciones de IPv6 y es un reemplazo para la dirección de difusión (broadcast). Se definen por el prefijo FF00::/8. Una interfaz puede pertenecer a cualquier cantidad de grupos multicast.

El segundo octeto de la dirección contiene el prefijo y banderas transitorias (tiempo de vida), y la extensión de la dirección multicast; así como se muestra en la figura 1.29.

[14] Autoridad de Asignación de Números de Internet: Entidad que supervisa la asignación global de Dirección IP, la asignación de Números de Sistemas Autónomos, la gestión de la zona radicular en el Domain Name System (DNS), los tipos de medios, y otros símbolos y números relacionados con el Protocolo de Internet.

```
R1# show ipv6 interface loopback 100
Loopback100 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::222:55FF:FE18:7DE8
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:8:85A3:4290:222:55FF:FE18:7DE8, subnet is 2001:8:85A3:4290::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF18:7DE8
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 31238)
  Hosts use stateless autoconfig for addresses.
R1#
```

Figura 1.28: Ejemplo de dirección IPV6 Unicast Global [11]

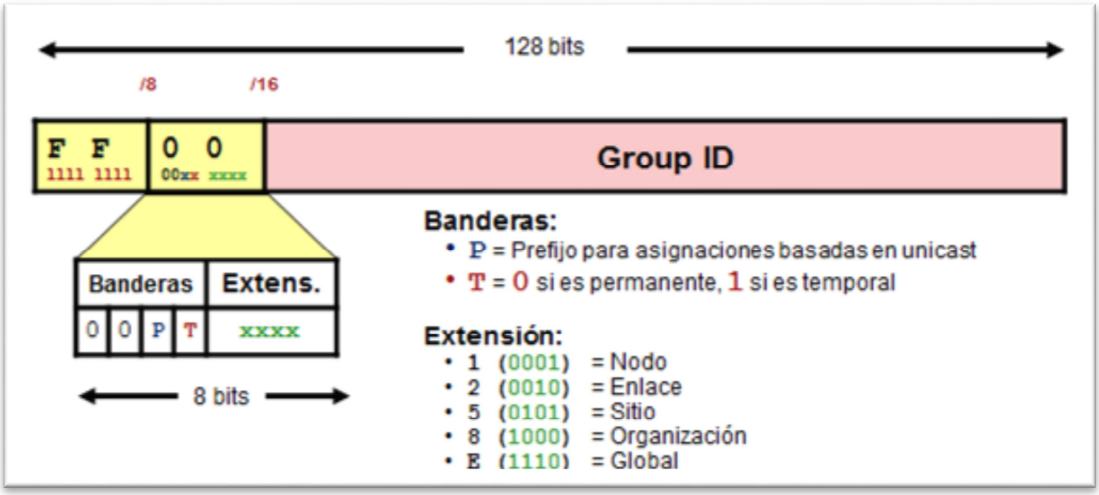


Figura 1.29: dirección IPV6 Multicast [10]

Las direcciones multicast FF00:: a FF0F:: tienen la bandera T en 0 y por tanto son permanentes y reservadas. Por ejemplo: Una dirección multicast que comienza con FF02 :: / 16 es una dirección permanente; el ejemplo presentado en la figura 1.30 muestra una dirección multicast.

```
R1# show ipv6 interface loopback 100
Loopback100 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::222:55FF:FE18:7DE8
  No Virtual link-local address(es):
  Global unicast address(es):
    2001:8:85A3:4290:222:55FF:FE18:7DE8, subnet is 2001:8:85A3:4290::/64 [EUI]
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF18:7DE8
  MTU is 1514 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is not supported
  ND reachable time is 30000 milliseconds (using 31238)
  Hosts use stateless autoconfig for addresses.
R1#
```

Figura 1.30: Ejemplo de dirección IPV6 Multicast [10]

1.2.6.5.1 Direcciones IPV6 Multicast Reservadas

La tabla 1.4 muestra las direcciones IPV6 Multicast Reservadas, así como su descripción.

Direcciones Multicast Reservadas	Descripción
FF02::1	Todos los nodos en un enlace.
FF02::2	Todos los routers en un enlace.
FF02::9	Toda la información de RIP de los routers en un enlace.
FF02::1:FFxx:xxxx	Todas las direcciones multicast utilizadas para autoconfiguración de hosts y descubrimiento de vecinos.
FF05::101	Todos los servidores NTP[15]

Tabla 1.4: direcciones IPV6 Multicast especiales [2]

[15] Protocolo de Internet ampliamente utilizado para transferir el tiempo a través de una red. NTP es normalmente utilizado para sincronizar el tiempo en clientes de red a una hora precisa.

1.2.6.6 Dirección IPV6 Anycast

IP versión 6 define un nuevo tipo de direcciones, conocido como direcciones “anycast”, que permite a un paquete ser enrutado a uno de un número de nodos diferentes, todos respondiendo a la misma dirección. Las direcciones anycast pueden ser asignadas a una o más interfaces de red; con la red entregando cada paquete hacia su dirección hasta la interfaz más cercana basada en la noción de distancia determinada por el protocolo de enrutamiento en uso.

Los usos de las direcciones anycast están en evolución, pero dichas direcciones ofrecen el potencial para un numero de servicios importantes. Por ejemplo, una dirección anycast puede ser utilizada para permitir a los nodos acceder a uno de una colección de servidores proveyendo un servicio bien conocido, sin un manual de configuración en cada nodo de la lista de servidores; o una dirección anycast puede ser usada en una ruta de origen para forzar el enrutamiento a través de un ISP, sin limitar el enrutamiento a un router especifico proveyendo acceso a ese ISP.

1.2.6.6.1 Formato de direcciones Anycast

Dentro de cada subred, los 128 valores de identificador más altos son reservados para la asignación como direcciones de subred anycast.

La construcción de una dirección anycast reservada depende en el tipo de direcciones IPv6 utilizadas dentro de una subred, tal como lo indica el prefijo de formato en las direcciones. En particular, para los tipos de direcciones IPv6 con 64 bits para el campo identificador de interfaz, el bit universal/local debe ser puesto en cero “0” (local) en todas las direcciones anycast reservadas, para indicar que el identificador de interfaz en la dirección no es globalmente único.

Específicamente, para direcciones IPv6 con 64 bits en el campo identificador de interfaz, en la figura 1.31 se muestran como son conformadas las direcciones anycast:

64 bits	57 bits	7 bits
PREFIJO DE SUBRED	1111110111…111	IDENTIFICADOR ANYCAST
	Campo de identificador de interfaz	

Figura 1.31: Ejemplo de dirección IPV6 anycast

Para otro tipo de direcciones IPv6, el identificador de interfaz no está en el formato EUI-64 y puede tener un valor diferente de 64 bits. Las direcciones anycast se conforman de la siguiente manera ver, figura 1.32

n bits	121-n bits	7 bits
PREFIJO DE SUBRED	1111111111…111	IDENTIFICADOR ANYCAST
	Campo de identificador de interfaz	

Figura 1.32: Anycast EUI-64

El prefijo de subred aquí consiste de todos los campos de la dirección IPv6 excepto el campo de identificador de interfaz. El campo identificador de interfaz se encuentra formado por un identificador anycast de 7 bits, con los bits restantes llenados todos con unos. El identificador anycast identifica las direcciones anycast reservadas.

1.2.6.6.2 Direcciones Anycast reservadas

La tabla 1.5 presenta los identificadores anycast para las direcciones anycast reservadas:

DECIMAL	HEXADECIMAL	DESCIPCIÓN
127	7F	Reservado
126	7E	Anycast móvil IPv6
0-125	00-7D	Reservado

Tabla 1.5: Direcciones IPV6 Anycast reservadas

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO 1

LIBROS

[1] **Peter J. Welcher,** *"Introduction to MPLS"*. Otoño 2007.

[2] **Cisco Networking Academy,** *"CCNP ROUTE: Implementing IPv6 in the Enterprise Network"*. Otoño 2010.

TESIS

[3] **Hinojosa** Lopez, Mayra Alexandra*;* **Herrera** Merchan, Fabricio Fernando, "Diseño de una red MPLS utilizando el protocolo IPV6 para proveedores de servicios de Telecomunicaciones". EPN. Julio 2009.

[4] **Hidalgo** Llumiquinga Carlos Luis; **Laguapillo** Muñoz David Alejandro, "Diseño e implementación de un laboratorio que permita emular y probar servicios IP y MPLS de la red Backbone Cisco de la Corporación Nacional de Telecomunicaciones CNT". EPN. Noviembre 2011.

PDF's, RFC's

[5] **ROSEN E., VISWANATHAN A., CALLON R.,** *"Multiprotocol Label Switching Architecture",* RFC 3031. Enero 2001

[6] **ROSEN E., REKHTER Y.,** *"BGP/MPLS VPN`s",* RFC 2547. Marzo 1999

[7] **MORGAN, LOVERING***, "ISCW Exam Certification Guide",* Verano 2007

[8] **DEERING S., HINDEN R.,** *"Internet Protocol, Version 6 (IPV6)",* RFC 2460. Diciembre 1998

[9] **ANONIMO,** *"IPv6 Headers At-a-Glance"*
URL:http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd80260042.pdf Consultado el 2 de Marzo de 2013

INTERNET

[10] **ANONIMO,** *"Cisco IOS IPv6 Multicast Introduction".*
URL:http://www.cisco.com/en/US/tech/tk828/technologies_white_paper09186a0080203e90.shtml consultado el 17 de marzo de 2013

[11] **ANONIMO**, *"Planning Guide / Roadmap Toward IPv6 Adoption"*
URL:http://www.cio.gov/documents_details.cfm/uid/1F4376CF-2170-9AD7-F24F363D0A04637E/structure/Enterprise%20Architecture/category/IPv6
Consultado el 17 de marzo de 2013

[12] **ANONIMO**, *"MPLS Básico y en detalle"*

CAPÍTULO 2

ANÁLISIS DE LA SITUACIÓN ACTUAL DE LA RED MPLS DE LA CNT ZONA PICHINCHA

2.1 INTRODUCCIÓN [3] [40]

La red MPLS de la CNT es una de las más robustas en el Ecuador; cuenta con un backbone[16] en topología anillo mediante el cual se tiene una gran redundancia. La red trabaja con tecnología de punta teniendo más de 10.000 km de Fibra Óptica para todo el territorio ecuatoriano además de utilizar equipos CISCO tanto para el borde como para el acceso.

Los servicios que la CNT brinda a sus usuarios gracias a esta red son:

- Servicios pagados Triple Play como: video bajo demanda, Internet de alta velocidad, telefonía IP, televisión y telefonía móvil.
- Enlaces de datos e Internet corporativos a bajo costo.
- Masificación de servicio de Banda Ancha para Internet.

Las características principales de la red MPLS actual en la CNT zona Pichincha son:

- Proveer una calidad de servicio (QoS) garantizado.
- Proveer anchos de banda en el orden de los Kbps y Mbps.
- Redundancia, lo cual minimiza los tiempos de no disponibilidad.
- Escalabilidad, garantizando el crecimiento de la red a nivel nacional.

En lo referente a la zona Pichincha para la red actual hay 3 nodos principales que son: IÑAQUITO, MARISCAL y QUITO CENTRO, de los cuales nacen y se derivan los diferentes nodos para las diferentes provincias del país.

[16] Conducto principal que permite comunicar segmentos de red entre sí.

2.2 MODELO DE RED JERÁRQUICO [1]

El diseño de una red de tipo jerárquico sigue a un modelo en el cual la misma se divide en tres capas independientes. Cada una de las capas cumple una función específica la cual define su rol dentro de la red general. Para facilitar el rendimiento de la red así como la escalabilidad; la separación de las diferentes funciones existentes de la red hace que el diseño de la misma se vuelva modular. El modelo de tres capas de CISCO es generalmente el más utilizado y es así como el backbone IP/MPLS de CNT lo tiene como su referente.

El modelo jerárquico típico se separa en tres capas: capa de acceso, capa de distribución y capa de núcleo, las cuales permiten la agregación y filtrado de tráfico así como implementación de redundancia a nivel de núcleo y distribución.

En la figura 2.1 se puede observar la red MPLS Pichincha en su totalidad de acuerdo al modelo jerárquico detallado anteriormente.

2.2.1 CAPA DE NÚCLEO (CORE)

La capa núcleo del diseño jerárquico es el backbone de alta velocidad de la internetwork[17]. La capa núcleo es esencial para la interconectividad entre los dispositivos de la capa de distribución, por lo tanto, es importante que el núcleo tenga una disponibilidad del por lo menos el 90% y tenga alta redundancia, esta redundancia se refiere a nivel físico, usando tarjetas diferentes y redundantes dentro del mismo equipos; también se tiene redundancia a nivel de conexiones, esto es si el equipo falla por completo la conexión ira por otro router P ya que los routers PE están conectados a diferentes Ps. 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.

[17] Posibilidad de trabajo en redes a través de medios masivos de comunicación, el diagrama en su tamaño original se encuentra en el ANEXO 2. Las IPs son falsas debido a cuestiones de seguridad.

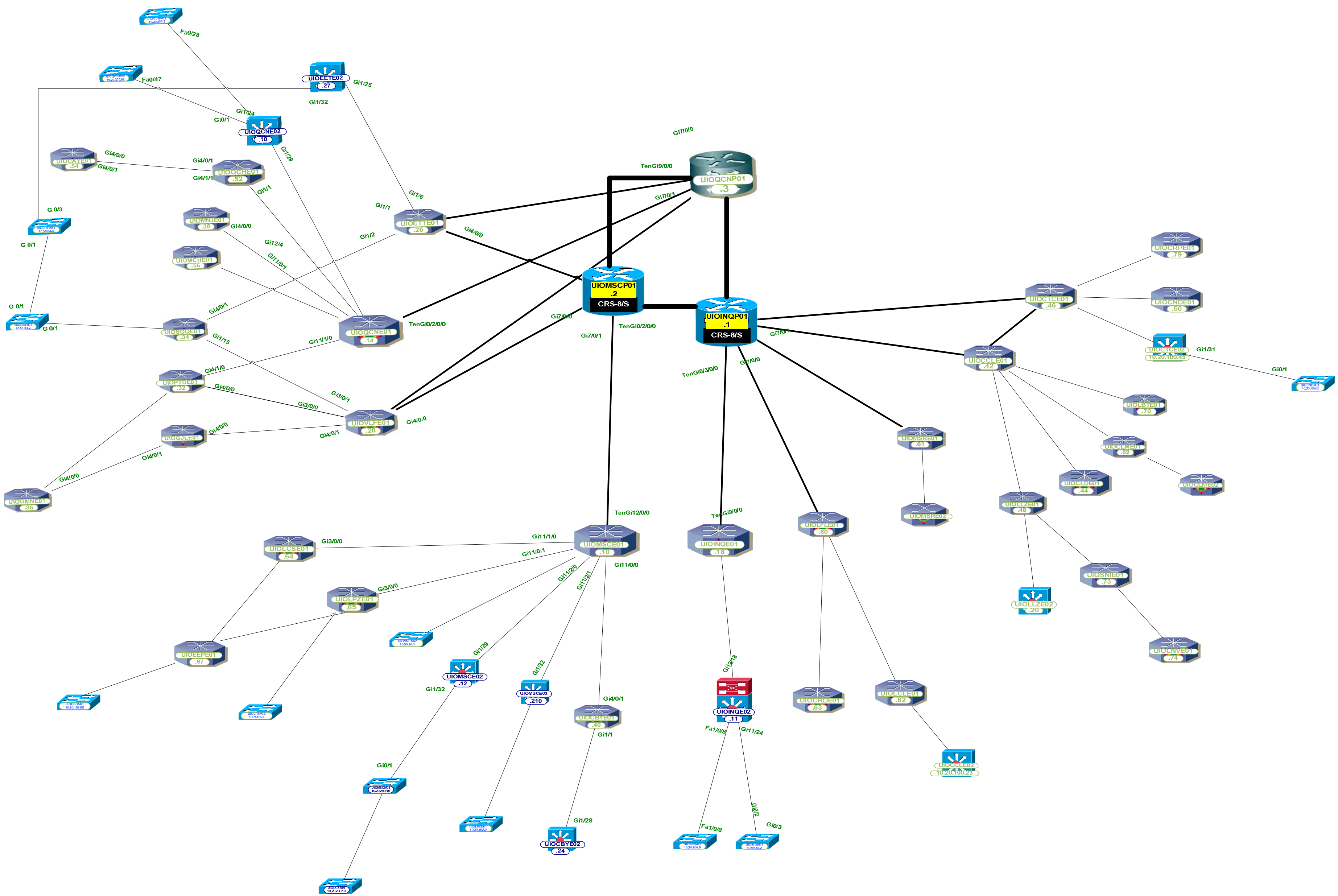


Figura 2.1: Diagrama de red CNT MPLS zona Pichincha [2]

El core de la red MPLS Pichincha se encuentra conformado por tres equipos CISCO CRS-8/S (MARISCAL, IÑAQUITO Y QUITO CENTRO) correspondientes al modelo stand-alone[18]; en la figura 2.2 se observa el diagrama de red de los equipos de core.

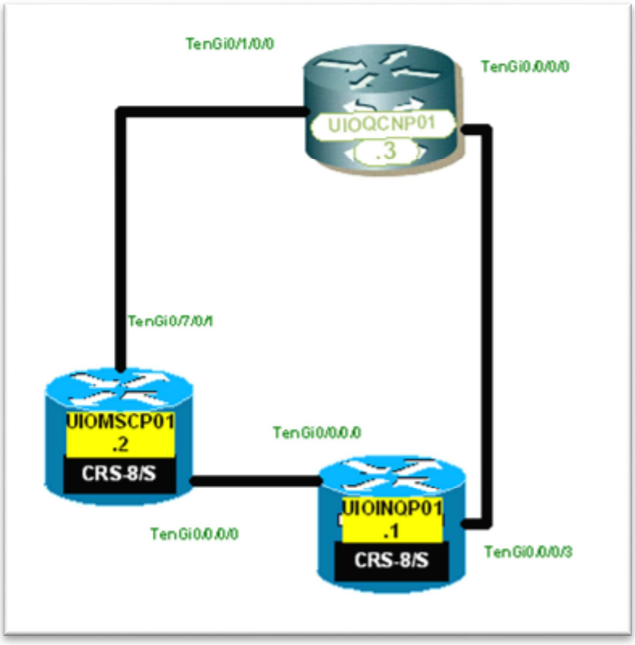


Figura 2.2: Diagrama de CORE CNT MPLS ZONA PICHINCHA [2]

Se puede observar la topología tipo anillo diseñada desde el core; esto con el objetivo de redundancia; los tres equipos principales de la red MPLS son nombrados de acuerdo al nodo donde se encuentran físicamente; y son sumamente importantes ya que de ellos se derivan los demás nodos a nivel provincial y nacional.

2.2.1.1 Nomenclatura y direccionamiento

En la tabla 2.1 se presenta el nombre de los sitios, la nomenclatura asignada a los equipos y el direccionamiento IP de gestión de los equipos de CORE.

En la tabla 2.2 se presenta las interconexiones de los equipos de Core, especificando la interfaz origen y destino:

[18] Terminales que necesitan estar conectadas a la red para funcionar.

EQUIPO	NOMENCLATURA	IP GESTIÓN
MARISCAL SUCRE	UIOMSCP01	11.56.0.2/32
IÑAQUITO	UIOINQP01	11.56.0.1/32
QUITO CENTRO	UIOQCNP01	11.56.0.3/32

Tabla 2.1: Nomenclatura y direccionamiento de equipos de Core de CNT Pichincha[19]

ORIGEN	INTERFAZ ORIGEN	DESTINO	INTERFAZ DESTINO
UIOMSCP01	TenGigE0/0/0/0	UIOINQP01	TenGigE0/0/0/0
UIOINQP01	TenGigE0/0/0/3	UIOQCNP01	TenGigE0/0/0/0
UIOQCNP01	TenGigE0/1/0/0	UIOMSCP01	TenGigE0/7/0/1

Tabla 2.2: Interconexión nodos de Core

2.2.2 CAPA DE DISTRIBUCIÓN

Antes de que los datos recibidos por los switches de acceso sean transmitidos hacia la capa de core, estos pasan por la de distribución. La capa de distribución cumple la función de controlar el tráfico de la red utilizando políticas así como la de trazar los dominios de broadcast mediante el enrutamiento de las funciones de las VLAN`s[20].

Normalmente, los switches de la capa de distribución son dispositivos que presentan alta disponibilidad y redundancia para poder asegurar la fiabilidad de los mismos.

En la red MPLS zona Pichincha de la CNT, la capa de Distribución utiliza routers del modelo CISCO c7600, que se representan en la figura 2.3.

[19] Las direcciones IP`s son solo de referencia, por cuestiones de seguridad no se puede indicar las originales.
[20] Red de área local virtual o LAN virtual es una red de área local que agrupa un conjunto de equipos de manera lógica y no física.

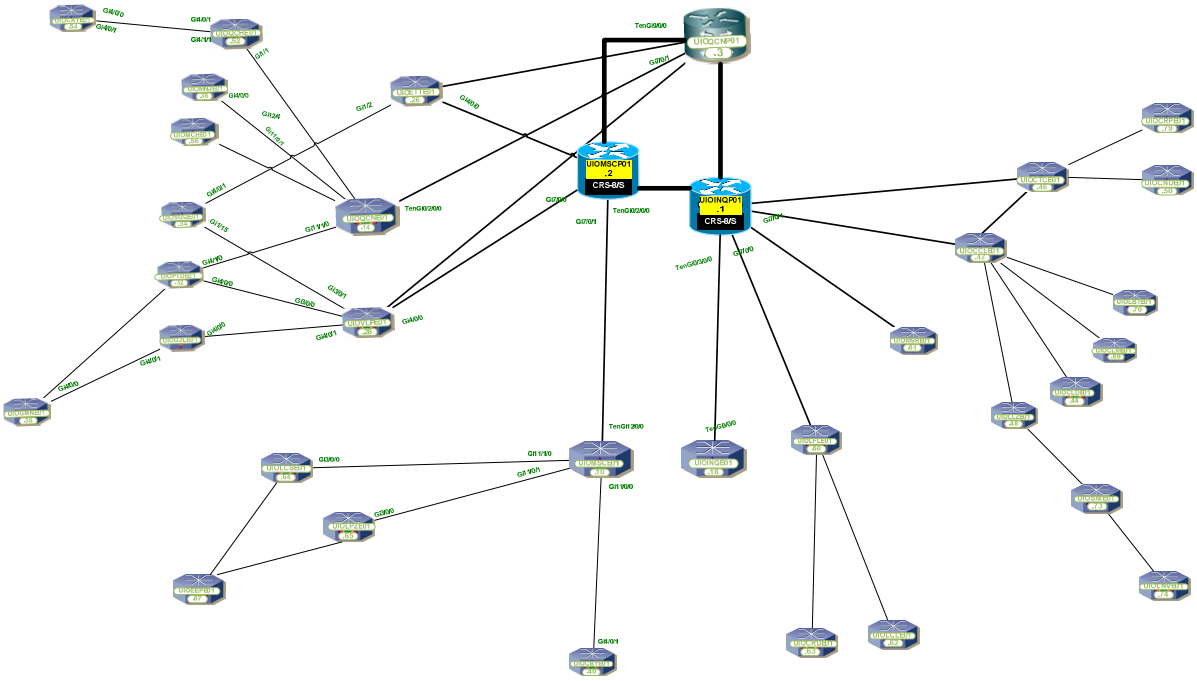


Figura 2.3: Diagrama de DISTRIBUCIÓN CNT MPLS ZONA PICHINCHA [2]

El router Cisco 7600, posee un chasis modular de 4 ranuras y 5 estantes de unidades, lo que proporciona al cliente un rendimiento de Ethernet de n X 10 gigabits de gran disponibilidad y densidad. Este router de dimensiones reducidas puede acomodar tarjetas de línea desde DS0 a OC-48, así como obtener velocidades de 10/100/1000, y está diseñado para permitir a los proveedores de servicios desplegar VPNs[21] L2/L3 y servicios de triple play en pequeños puntos de presencia (points of presence , POPs) y accesos a Internet, o para empresas que necesiten ampliar sus redes en el extremo.

2.2.2.1 Nomenclatura y direccionamiento de la capa de Distribución

A continuación se presenta la tabla 2.3 detallando la nomenclatura y direccionamiento IP de interconexión, para los equipos de la capa de distribución de la red MPLS zona Pichincha de la CNT.

[21] Una Red Privada Virtual (VPN) conecta los componentes de una red sobre otra red.

NODO	HOSTNAME	IP GESTIÓN	MARCA	MODELO	NODO SUPERIOR	INTERFAZ UPLINK	IP INTERFAZ	MEDIO DE TX
COLLALOMA	UIOCLME01	11.56.4.69	CISCO	CISCO7606	UIOCCLE01	Gig 1/2	11.76.442.10	Fibra
CONDADO	UIOCNDE01	11.56.4.50	CISCO	CISCO7609	UIOCTCE01	Gig 4/0/0	11.76.446.2	Fibra
LA BOTA	UIOLBTE01	11.56.4.70	CISCO	CISCO7606	UIOCCLE01	Gig 3/0/0	11.76.442.26	Fibra
CALDERON	UIOCLDE01	11.56.4.44	CISCO	CISCO7609	UIOCCLE01	Gig 3/0/1	11.76.442.14	Fibra
LA LUZ	UIOLLZE01	11.56.4.48	CISCO	CISCO7609	UIOCCLE01	Gi1/0	11.76.442.18	Fibra
MONTESERRIN	UIOMSRE01	11.56.4.61	CISCO	CISCO7606	UIOINQP01	Gig 11/0/0	11.76.41.141	Fibra
LA FLORIDA	UIOLFLE01	11.56.4.60	CISCO	CISCO7606	UIOINQP01	Gig 3/1/0	11.76.41.146	Fibra
CARONDELET	UIOCRDE01	11.56.4.63	CISCO	CISCO7606	UIOLFLE01	Gig 3/0/0	11.76.460.2	Fibra
LA CAROLINA	UIOLCLE01	11.56.4.62	CISCO	7606-S	UIOLFLE01	Gi0/13	11.76.460.6	Fibra
SAN ISIDRO	UIOSNIE01	11.56.4.73	CISCO	CISCO7606	UIOLLZE01	Gig 4/0/0	11.76.448.1	Fibra
LOS NEVADOS	UIOLNVE01	11.56.4.74	CISCO	CISCO7606	UIOLLZE01	Gig 4/1/1	11.76.448.6	Fibra
IÑAQUITO	UIOINQE01	11.56.4.18	CISCO	CISCO7613	UIOINQP01	TenGigE0/2/0/1	11.76.41.158	Fibra
COTOCOLLAO	UIOCTCE01	11.56.4.46	CISCO	CISCO7609	UIOINQP01	Gig 4/0/0	11.76.41.10	Fibra
VILLAFLORA	UIOVLFE01	11.56.4.28	CISCO	7609	UIOMSCP01	Gi0/13	11.76.42.5	Fibra
EST. TERRENA	UIOETTE01	11.56.4.26	CISCO	CISCO7609	UIOQCNP01	Gi0/7/0/0	11.76.43.10	Fibra
SANGOLQUI	UIOSGQE01	11.56.4.34	CISCO	7609	UIOVLFE01	Gi3/0	11.76.428.10	Fibra
PINTADO	UIOPTDE01	11.56.4.32	CISCO	CISCO7609	UIOVLFE01	Gi4/0	11.76.428.2	Fibra
GUAJALO	UIOGJLE01	11.56.4.30	CISCO	CISCO7609	UIOVLFE01	Gi2/0	11.76.428.6	Fibra
CUMBAYA	UIOCBYE01	11.56.4.40	CISCO	CISCO7609	UIOMSCE01	Gig 0/5/0/8	N/A	Fibra
ESC. ESPEJO	UIOEEPE01	11.56.4.67	CISCO	CISCO7606	UIOLPZE01	Gi5/1	11.76.465.5	Fibra

Tabla 2.3: Nomenclatura y direccionamiento de interconexión para equipos de Distribución. Pg. 1 de 2

NODO	HOSTNAME	IP GESTIÓN	MARCA	MODELO	NODO SUPERIOR	INTERFAZ UPLINK	IP INTERFAZ	MEDIO DE TX
GUAMANI	UIOGMNE01	11.56.4.36	CISCO	7609	UIOGJLE01	Gi0/13	11.76.430.1	Fibra
MARISCAL	UIOMSCE01	11.56.4.10	CISCO	CISCO7613	UIOMSCP01	TenGigE0/0/0/2	11.76.42.12	Fibra
QUITO CENTRO	UIOQCNE01	11.56.4.14	CISCO	CISCO7613	UIOQCNP01	TenGigE0/2/0/0	11.76.43.12	Fibra
MONJAS	UIOMNJE01	11.56.4.38	CISCO	CISCO7609	UIOQCNE01	Gi4/0	11.76.414.22	Fibra
QUINCHE	UIOQCHE01	11.56.4.52	CISCO	7609	UIOQCNE01	Gi0/13	11.76.414.10	Fibra
CAYAMBE	UIOCAYE01	11.56.4.54	CISCO	CISCO7609	UIOQCHE01	Gig 4/1/1	11.76.452.2	Fibra
MACHACHI	UIOMCHE01	11.56.4.56	CISCO	CISCO7609	UIOQCNE01	Gig 4/0/0	11.76.414.6	Fibra

Tabla 2.3: Nomenclatura y direccionamiento de interconexión para equipos de Distribución. Pg. 2 de 2

2.2.3 CAPA DE ACCESO

La capa de acceso concentra las diferentes tecnologías de Útima Milla como: xDSL (Digital Subscriber Line – Linea Digital de Subscriptor), xPON (Passive Optical Networks – Redes Ópticas Pasivas), WiMax (Worldwide Interoperability for Microwave Access – Interoperabilidad Mundial para Accesos de Microondas), entre otras; con el propósito de proveer acceso al resto de la red con dispositivos finales (PC`s, impresoras, teléfonos IP, etc.).

El principal objetivo de la capa de acceso es el de aportar un medio de conexión de los dispositivos a la red y a la vez controlar cuáles de estos pueden comunicarse en red; en el caso de CNT poder conectar los diferentes clientes con cualquier servicio que estos tengan contratado.

Esta capa de acceso puede incluir routers, switches, puentes, hubs y puntos de acceso inalámbricos mediante los cuales se pueden implementar mecanismos de conmutación y transporte para VLAN`s basadas en 802.1Q y 802.1ad. Dentro de la red de CNT se tienen tres tipos de nodos de acceso cuyas características se detallan a continuación:

2.2.3.1 Nodos de Acceso 7606-S [27]

La familia de routers Cisco 7606-S despliegan un alto rendimiento en características IP/MPLS, así como servicios IP escalables y personalizados en el borde de la red. Cuentan con dos fuentes de alimentación DC de 2700 W. Estas fuentes trabajan en redundancia 1:1. Cada nodo tendrá un número necesario de tarjetas y módulos, dependiendo la cantidad de puertos WAN (10 y 1 Gbps) y las interfaces LAN se colocan en tarjetas de 48 puertos.

Al proporcionar un rendimiento y fiabilidad, el Cisco 7606 ofrece 96 Mpps en el reenvío distribuido, con opciones para los procesadores de rutas redundantes y fuentes de alimentación. La inclusión de dos puertos Gigabit Ethernet de Cisco Supervisor 2 con la tarjeta de conmutación multicapa característica 2 (MSFC-2).

2.2.3.2 Nodos de Acceso ME6524 [25]

El switch Cisco ME 6524 es un equipo que optimiza espacio y energía y adicionalmente permite de forma rentable configurar servicios basados en hardware como Multiprotocol Label Switching (MPLS) VPN, Enrutamiento Encapsulado Genérico (GRE), NetFlow, NAT[22], PAT[23] y VRF`s gracias al IOS modular que contiene.

2.2.3.3 Nodos de Acceso ME3800X [5]

El Cisco ME 3800X es un switch con plataforma para todas las funciones de agregación diseñado expresamente para el negocio móvil, y los mercados residenciales. Con bajo consumo de energía y servicio de gran escala, este switch está optimizado para la agregación de pequeñas y remotas aplicaciones POP, por lo que es una opción muy rentable.

En la figura 2.4 se presenta el diagrama de los equipos de acceso para la red CNT Pichincha.

2.2.3.4 Nomenclatura y direccionamiento de la capa de Acceso

La tabla 2.4 presenta la nomenclatura y direccionamiento IP de interconexión para los equipos de la capa de acceso de la red MPLS zona Pichincha de la CNT.

2.3 CARACTERÍSTICAS DE LOS EQUIPOS DE LA RED MPLS ZONA PICHINCHA DE LA CNT E.P. [6 - 17], [26], [28]

El backbone de la red MPLS de CNT es la parte medular para la comunicación de enlaces de VOZ, INTERNET, DATOS y VIDEO, es por ello que cuenta con el mejor equipamiento en cuanto a disponibilidad, robustez y redundancia. Los

[22] *Network Address Translation* o Traducción de Dirección de Red. Estándar para la utilización de una o más direcciones IP para conectar varias computadoras a una red (especialmente Internet).
23 *Port Address Translation* o Traducción de dirección de puerto. Traduce las direcciones IP privadas a la dirección de la interfaz.

equipos con que cuenta la red MPLS son de marca CISCO y en la tabla 2.5 se presentan los modelos que actualmente están siendo utilizados por CNT.

2.4 CONFIGURACIÓN DE EQUIPOS PARA LA RED MPLS ZONA PICHINCHA

En el presente capítulo se detalla la configuración actual de la red MPLS de CNT Zona Pichincha tanto para equipos de Core como de Acceso así también como los protocolos de enrutamiento y configuración de usuarios finales.

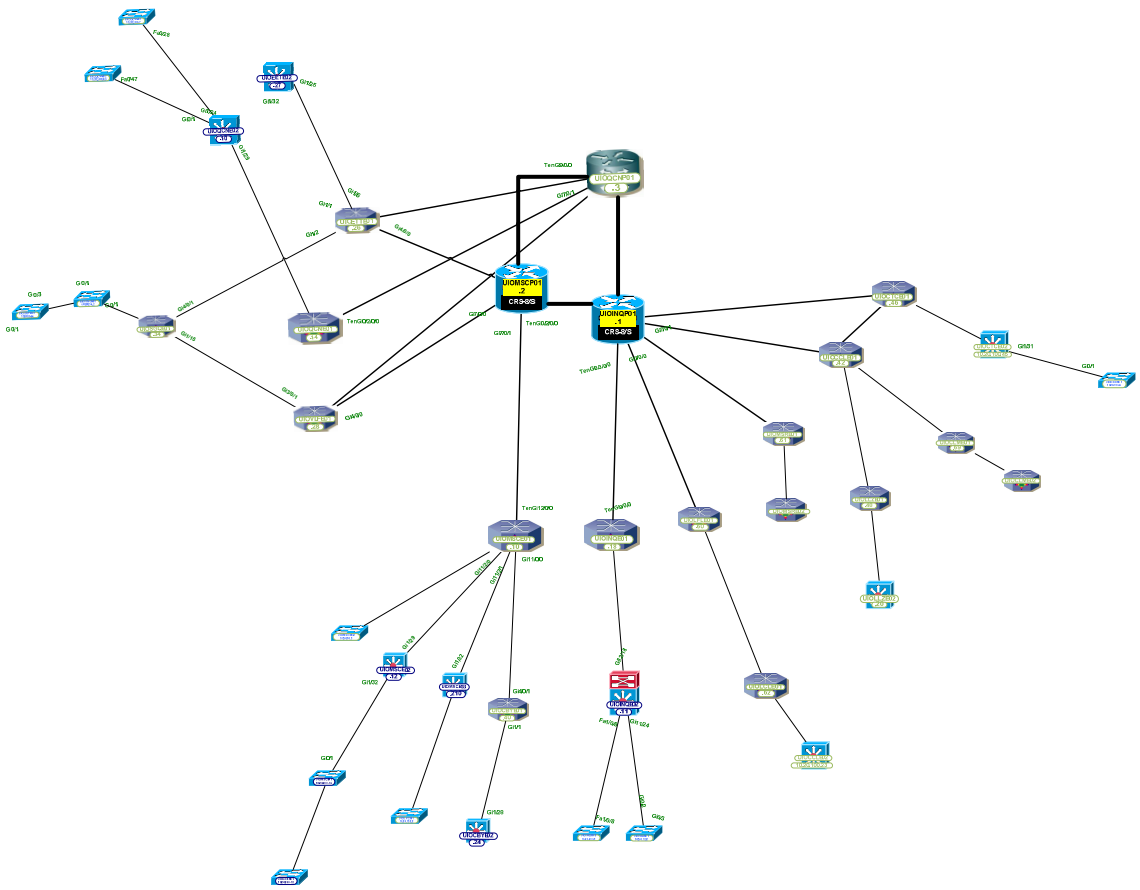


Figura 2.4: Diagrama de equipos de acceso MPLS CNT zona Pichincha

NODO	HOSTNAME	IP GESTIÓN	MODL.	NODO SUP.	INT. UPLINK	IP INTERFAZ	MEDIO DE TX
COTOCOLLAO	UIOCTCE02	11.24.100.45	ME6524	UIOCTCE01	Te0/2	11.76.446.10	Fibra
CARCELEN	UIOCCLE02	11.24.100.23	ME6524	UIOLCLE01	Te0/2	11.76.442.30	Fibra
IÑAQUITO	UIOINQM01	10.50.18.2	C3560	UIOINQE02	Gi11/23	N/A	Fibra
LA LUZ	UIOLLZE02	11.56.4.49	ME380x	UIOLLZE01	Te0/2	11.76.448.10	Fibra
IÑAQUITO	UIOINQE02	11.24.100.11	ME6524	UIOINQE01	Gi12/18	11.76.418.22	Fibra
MARISCAL	UIOMSCE03	11.24.100.210	ME6524	UIOMSCE01	Gi1/32	N/A	Fibra
MARISCAL	UIOMSCM02	10.50.10.3	C3560	UIOMSCE01	Gig 0/25	N/A	Fibra
CUMBAYA	UIOCBYE02	11.56.4.41	ME380x	UIOCBYE01	Te0/2	11.76.440.2	Fibra
LA PAZ	UIOLPZM02	11.1.65.196	ME340X	UIOLPZE01	Gi0/1	N/A	Fibra
MARISCAL	UIOMSCE02	11.24.100.12	ME6524	UIOMSCE01	Gig 11/2/0	N/A	Fibra
UIOCENTRO	UIOQCNE02	11.24.100.10	ME6524	UIOQCNE01	Gi5/2	N/A	Fibra
E.TERRENA	UIOETTE02	11.56.4.27	ME6524	UIOETTE01	Gi0/7/0/0	11.76.426.2	Fibra
UIOCENTRO	UIOQCNM01	11.74.10.2	C3560	UIOQCNE02	Gig 1/24	N/A	Fibra

Tabla 2.4: Nomenclatura y direccionamiento de interconexión de equipos de acceso.

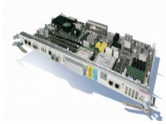
MODELO	DESCRIPCIÓN	CAPACIDAD	CANTIDAD EN LA RED	TARJETAS	
CRS 	1. Funcionamiento del sistema continuo.	92 Tbps	3	RP 	• Soporta los protocolos: CDP , direccionamiento IPV4 e IPV6, ICMP (Internet Control Message Protocol), BGPv4, OSPFv2, OSPFv3, IS-IS. • Cuenta con un puerto Ethernet 10/100/1000 (conector RJ45) y dos puertos Ethernet 10/100/1000 (conector 1000BASE-LX, SPF) para conectividad con el plano de control.
	2. Flexibilidad y longevidad del servicio.			MSC	• Reenvío de la capa 3 del motor del CRS-1 con una tasa de rendimiento líder en la industria de alambre a 40 Gbps. • Procesamiento adicional de Clase de Servicio (CoS), Multicast, Ingeniería de tráfico (TE) y rendimiento de 40Gbps. • Soporta bastantes protocolos de reenvío, incluyendo IPv4, IPv6 y MPLS.
	3. Combina procesador Cisco Silicon Packet con la arquitectura de separacion de servicio Cisco.			PLIM 	• Contiene modulos ópticos. • Ofrece servicios de capa 1 y capa 2.

Tabla 2.5: Equipos de la red MPLS zona Pichincha de la CNT**.** Pg. 1 de 4

MODELO	DESCRIPCIÓN	CAPACIDAD	CANTIDAD EN LA RED	TARJETAS	
C7609-S 	1. Permite crear una infraestructura de red avanzada con como servicios triple-play.	720 Gbps	31	RSP 	• Alta escalabilidad, desempeño y rápida convergencia. • Conjunto completo de funciones IP para aplicaciones como MPLS VPN en capa 2 y 3 con QoS.
	2. Ideal para aplicaciones que requieren un alto desempeño como: líneas dedicadas, MPLS, y acceso Metro Ethernet.			ETHERNET SERVICES PLUS 	• Permite la priorización de servicios de voz, video datos y movilidad inalámbrica. • Cuentan con calidad jerárquica de servicio (QoS), VLANs, de significado local, aprendizaje de MAC`s, y hasta 16.000 instancias de servicios Ethernet por tarjeta.

Tabla 2.5: Equipos de la red MPLS zona Pichincha de la CNT**.** Pg. 2 de 4

MODELO	DESCRIPCIÓN	CAPACIDAD	CANTIDAD EN LA RED	TARJETAS	
ASR1000 	1. Capacidad de encendido instantaneo.	20 Gpbs	1	ROUTE PROCESSOR 	• Proporciona un procesdador redundante opcional. • Ofrece escalabilidad en cuanto a memoria.
	2. Redundancia de software en hardware no redundante.			PROCESADOR DE SERVICIOS EMBEBIDOS 	• Disponible en version de 5, 10 y 20 Gbps. • Maneja el procesador Quantum Flow Processor.
	3. Utiliza el poderoso procesador Cisco Quantum Flow.			PROCESADOR DE INTERFACE SPA 	• Facilita la priorización de los servicios triple-play. •Puede clasificar el trafico QoS basandose en la capa 2 o 3. •Permite la reutilizacion de adaptadores de puertos compartidos.

Tabla 2.5: Equipos de la red MPLS zona Pichincha de la CNT**.** Pg. 3 de 4

MODELO	DESCRIPCIÓN	CAPACIDAD	CANTIDAD EN LA RED	TARJETAS	
ME6500 	1. Viene con un software en base IP que incluye funciones de capa 2, RIP y EIGRP. 2. Ofrece caraterisctcas IPv4 y funcionalidad de MPLS e IPv6. 3. Cuenta con servicios de capa 2 como 802.1Q tunneling. 4. Ofrece mayor disponibilidad de servicios y seguridad integrada.	24 GBPS	10	N/ A	N/ A

Tabla 2.5: Equipos de la red MPLS zona Pichincha de la CNT**.** Pg. 4 de 4

2.4.1 CEF (CISCO EXPRESS FORWARDING – REENVÍO EXPRES DE CISCO) [29]

La tecnología IP CEF (Cisco Express Forwarding – Reenvío Exprés de Cisco) es una solución de capa 3 escalable y distribuida diseñado para conocer el rendimiento futuro del internet y la red empresarial. Representa el último avance dentro de las capacidades de enrutamiento del IOS de Cisco que incluye NetFlow Switching[24] y enrutamiento distribuido. CEF es también un componente clave en la arquitectura de enrutamiento de etiquetas de Cisco.

2.4.1.1 Habilitación de CEF o Dcef [18]

Se debe habilitar CEF cuando el router tenga procesadores de interfaz que no soporten dCEF. Para habilitar CEF, se utiliza el siguiente comando en el modo de configuración global:

```
Router(config)# ip cef
```

Se debe habilitar dCEF cuando se desee que la tarjeta de línea realice express forwarding para que el RP pueda manejar protocolos de enrutamiento o conmute paquetes desde procesadores de interfaces antiguas, para habilitar dCEF, se utiliza el siguiente comando desde el modo de configuración global:

```
Router(config)# ip cef distributed
```

Cuando se habilita CEF o dCEF globalmente, todas las interfaces que soportan CEF se habilitan por defecto; igualmente si se desea des habilitar CEF o dCEF en una interfaz en particular se lo puede realizar de la siguiente manera:

```
Router(config-if)# no ip route-cache cef
```

[24] Protocolo de red desarrollado por Cisco para recolectar información sobre tráfico IP.

Cuando se deshabilita CEF o dCEF, el IOS de Cisco conmuta los paquetes recibidos en la interfaz utilizando el siguiente camino de conmutación más rápido. En el caso de dCEF, el siguiente más rápido camino de conmutación es CEF.

2.4.1.2 CEF en la red MPLS zona Pichincha de CNT

A continuación se presenta el CEF configurado en la red MPLS zona Pichincha de la CNT. En la figura 2.5 se muestra la configuración CEF para el router UIOINQE01.

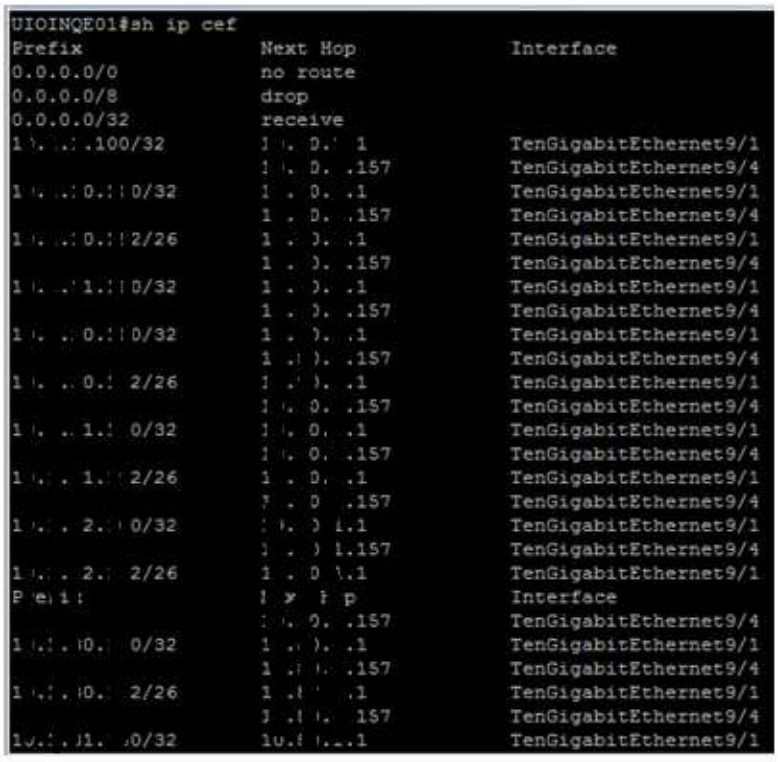


Figura 2.5: Configuración CEF para el router UIOINQE01[25]

2.4.2 CONFIGURACIÓN DE MPLS EN MODO TRAMA (FRAME MODE) [18]

En MPLS modo trama (frame-mode), los routers corriendo MPLS intercambian paquetes IP puros, así como los paquetes IP etiquetados uno con el otro en un dominio MPLS. En un dominio MPLS, la conmutación de etiquetas se la realiza

[25] Por motivos de seguridad se ocultan las IP`s.

mediante el análisis de la cabecera de la trama y luego realizando imposición de etiqueta (push), disposición de etiqueta (POP), o de intercambio de etiqueta dependiendo la ubicación de los LSR`s en la red.

2.4.2.1 Configuración de Interfaz Loopback [19]

Se puede especificar una interfaz a nivel de software para simular una interfaz física; a ésta la llamamos interfaz de loopback, la cual puede ser configurada en todas las plataformas Cisco. Una interfaz de loopback es una interfaz virtual que siempre se encuentra activa y permite que sesiones como BGP y RSRB (remote source-route bridging) se mantengan igualmente activas inclusive si la interfaz de salida se encuentra caída.

En la figura 2.6 se presenta la configuración de la interfaz Loopback 100 de un equipo de borde en la red MPLS Pichincha. Este mismo esquema se maneja para los diferentes equipos en la red.

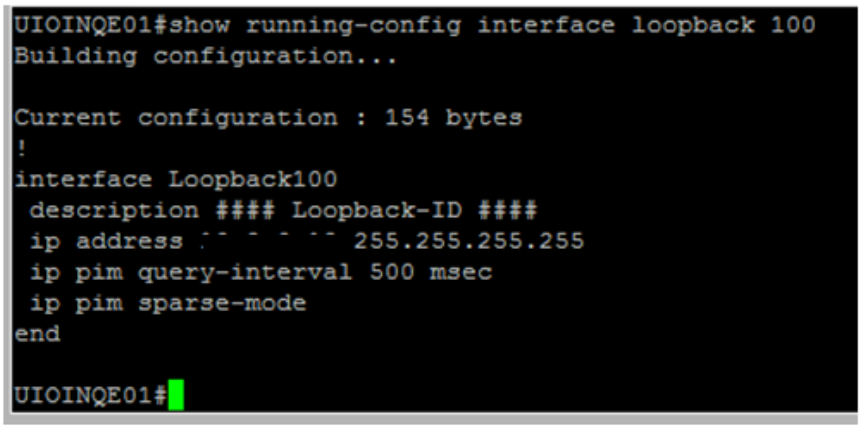


Figura 2.6: Configuración de Loopback en CNT

2.4.2.2 Configuración de MPLS en una interfaz frame-mode

Se debe habilitar MPLS tanto globalmente como en las interfaces físicas del router que se desee que participen en el reenvío MPLS. El comando **mpls ip** habilita

conmutación mediante etiquetas de paquetes IPv4 de acuerdo con los caminos enrutados normalmente. Cuando este comando es ejecutado, LDP´s hello y keepalives son enviados y recibidos en las interfaces habilitadas con MPLS.

En la figura 2.7 se puede visualizar la configuración de una interfaz entre dos equipos de borde.

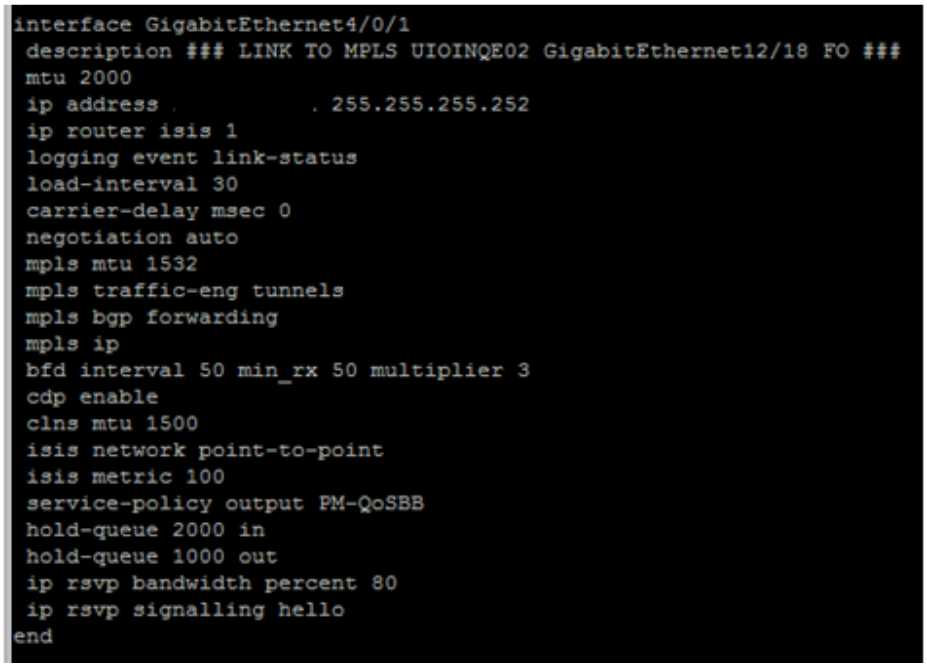


Figura 2.7: Configuración de interfaz de interconexión en CNT

Dentro de la configuración se puede detallar lo siguiente:

- **description:** añade una descripción a la interfaz, en este caso la interfaz Gigabit Ethernet 4/0/1 sirve de interconexión con el equipo UIOINQE02.
- **mtu:** se define el tamaño del mtu permitido en la interfaz (2000).
- **ip address:** dirección IP y máscara designada a la interfaz.
- **ip router isis:** habilitación del protocolo de enrutamiento IS-IS, del cual se hablará más adelante.

- **logging event link status:** se configura para mostrar en los logs cuando la interfaz cambio de estado (up/down).
- **load-interval 30:** se configura para mostrar la carga de la interfaz en un período de 30 segundos.
- **carrier-delay msec 0:** hace que el router realice la señalización automática cuando la interfaz pasó a estado down; por defecto esto toma 2 segundos.
- **negotiation auto:** el tipo de negociación de la inetrface esta configurado de manera automática.
- **mpls mtu:** indica que tan grande puede ser un paquete etiquetado en la interfaz.
- **mpls traffic-eng tunnels:** habilita señalización de ingeniería de tráfico en la interfaz.
- **mpls bgp forwarding:** esto está diseñado para etiquetas asignadas en BGP; este comando aparece en la interfaz luego de haber ejecutado el comando send-label en la configuración BGP.
- **mpls ip:** habilita MPLS en la interfaz.
- **cdp enable:** habilita el protocolo CDP en la interfaz.
- **clns mtu:** establece el tamaño del MTU del paquete para la interfaz.
- **Isis network point-to-point:** este comando se lo utiliza para configurar el protocolo IS-IS para operar como si la interfaz subyacente fuera una interfaz punto a punto.
- **Isis metric:** establece la métrica de nivel 1 en la interfaz; en este caso es 100 ya que es la velocidad de la interfaz.

2.4.3 LDP (LABEL DISTRIBUTION PROTOCOL – PROTOCOLO DE DISTRIBUCIÓN DE ETIQUETAS) [20]

El protocolo de distribución de etiquetas (LDP) proporciona los medios para los LSR`s para solicitar, distribuir y liberar la información de los prefijos de etiqueta hacia los demás routers en una red. LDP permite a los LSR`s descubrir pares potenciales y

establecer sesiones LDP con ellos con el propósito de intercambiar información de las etiquetas.

2.4.3.1 Configuración de LDP en la red MPLS zona Pichincha

La figura 2.8 presenta la configuración de LDP en un equipo de borde.

```
UIOINQE01#sh run | inc ldp
mpls ldp neighbor 1    .0. 8 password 7 044926165E745C1E5F4D53
mpls ldp neighbor 1    .0. 1 password 7 061422311D1B1949534344
mpls ldp neighbor 1    .0. 0 password 7 061422311D1B1949534344
mpls ldp neighbor 1    0.1 0.25 password 7 05192B1F70195E594F5141
mpls ldp neighbor 1    0.1 0.11 password 7 14053F1B5D513A7B727C65
mpls ldp neighbor 1    .0. 5 password 7 0833615E584C1547445F5A
mpls ldp neighbor 1    0.1 0.33 password 7 05192B1F70195E594F5141
mpls ldp neighbor 1    .0. 7 password 7 0833615E584C1547445F5A
mpls ldp neighbor 1    .0.  password 7 111B341546471B5C527E7D
mpls ldp neighbor 1    .0. 3 password 7 0833615E584C1547445F5A
mpls ldp neighbor 1    .30 100 password 7 105C24095442025B5A507C
mpls ldp neighbor 1    .0.  password 7 0833615E584C1547445F5A
mpls ldp neighbor 1    .99 100 password 7 0214294B5A531F711A1A5F
mpls ldp neighbor 1    .0. 9 password 7 044926165E745C1E5F4D53
mpls ldp neighbor 1    .14 .100 password 7 120B2807435E1C547C7F72
mpls ldp graceful-restart
snmp-server enable traps mpls rfc ldp
snmp-server enable traps mpls ldp
mpls ldp router-id Loopback100 force
```

Figura 2.8: Configuración LDP en red MPLS CNT

La configuación en los demas PE´s es básicamente la misma y los parámetros configurados se detallan a continuación:

mpls ldp neighbor 11.56.4.48 password 7 044926165E745C1E5F4D53: Se configura el vecino de IP 11.56.4.48 con encripción propietaria de CISCO.

mpls ldp graceful-restart: habilita al router para proteger los enlaces LDP y el estado de reenvío MPLS durante la interrupción del servicio.

mpls ldp router-id Loopback100 force: especifica el ID que LDP utiliza para formar sesiones. Si no definimos la interfaz, el proceso LDP crea la sesión usando la

loopback con la IP mayor. La palabra opcional force indica que el ID LDP se activará sin necesidad de reiniciar el router.

2.4.3.3.1 Verificación de la Configuración LDP

Con los comandos siguientes se puede comprobar que las sesiones LDP se encuentran correctamente configuradas:

- **show mpls ldp discovery detail:** se lo utiliza para verificar que la contraseña LDP en cada vecino se encuentra configurada; en la figura 2.9 se puede observar la configuración actual.
- **show mpls ldp neighbor detail:** despliega la información detallada de cada vecino tal y como lo muestra la figura 2.10.

2.4.4 PROTOCOLO DE ENRUTAMIENTO IS-IS (INTERMEDIATE SYSTEM TO INTERMEDIATE SYSTEM) [21] [31]

El protocolo IS-IS es un protocolo de tipo estado de enlace que aunque fue desarrollado para implementar direcciones CLNP[26] se lo adaptó para dar soporte al enrutamiento IP. La terminología en este protocolo es distinta que la IP y las equivalencias se presentan a continuación:

- HOST = End System (ES).
- ENRUTADOR = Intermediate System (IS).

2.4.4.1 Configuración de ISIS en la red MPLS zona Pichincha

La figura 2.11 presenta la configuración del protocolo IS-IS en un PE de la red MPLS de CNT en Pichincha.

[26] ConnectionLess Network Protocol (CLNP): Protocolo utilizado por OSI para transportar datos e indicación de errores en el nivel de red. CLNP es similar a IP y no proporciona detección de errores en la transmisión de datos, delega en el nivel transporte esta función.

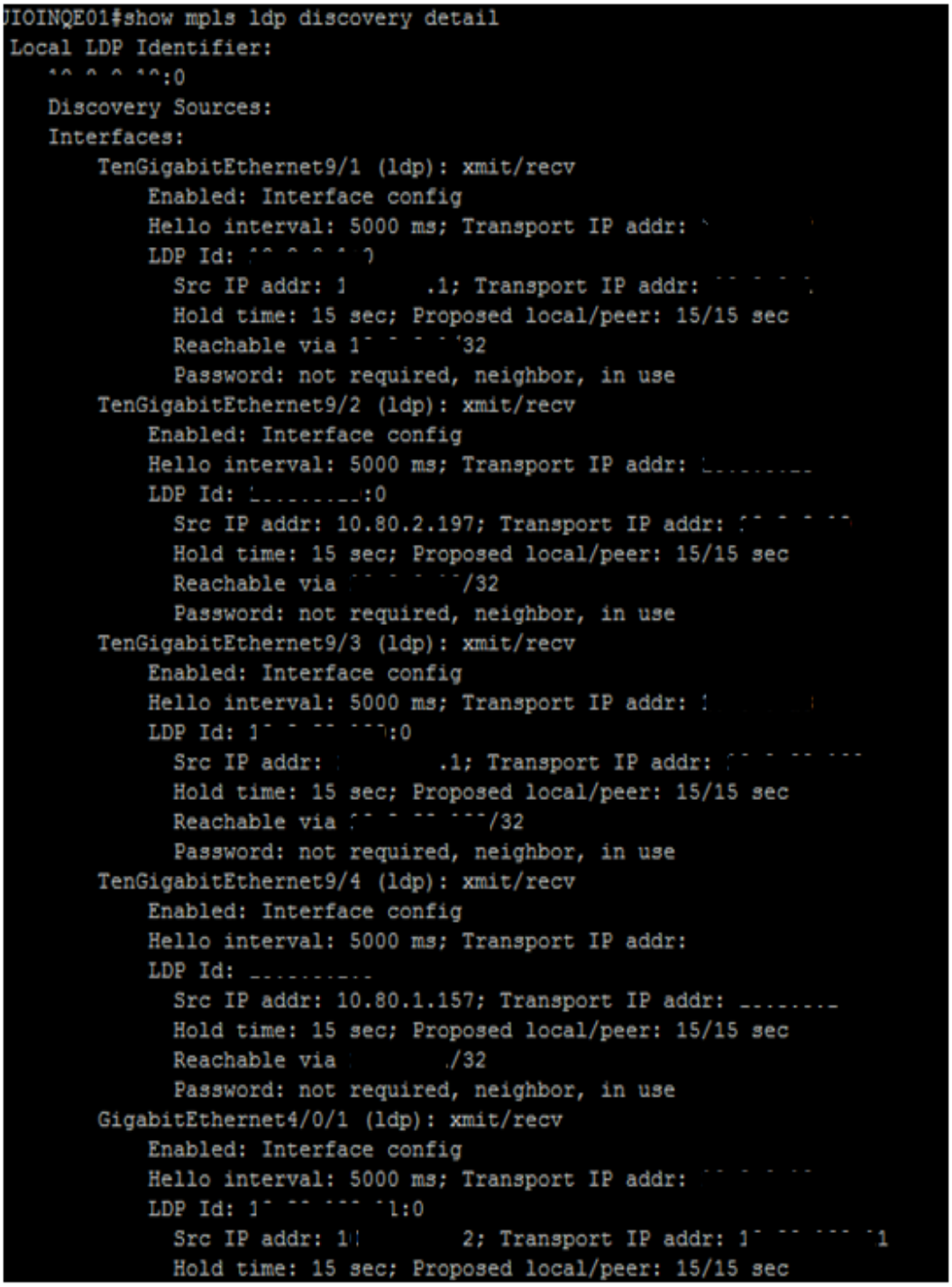


Figura 2.9: Contraseñas LDP en red MPLS CNT

Figura 2.10: Vecinos LDP en red MPLS CNT

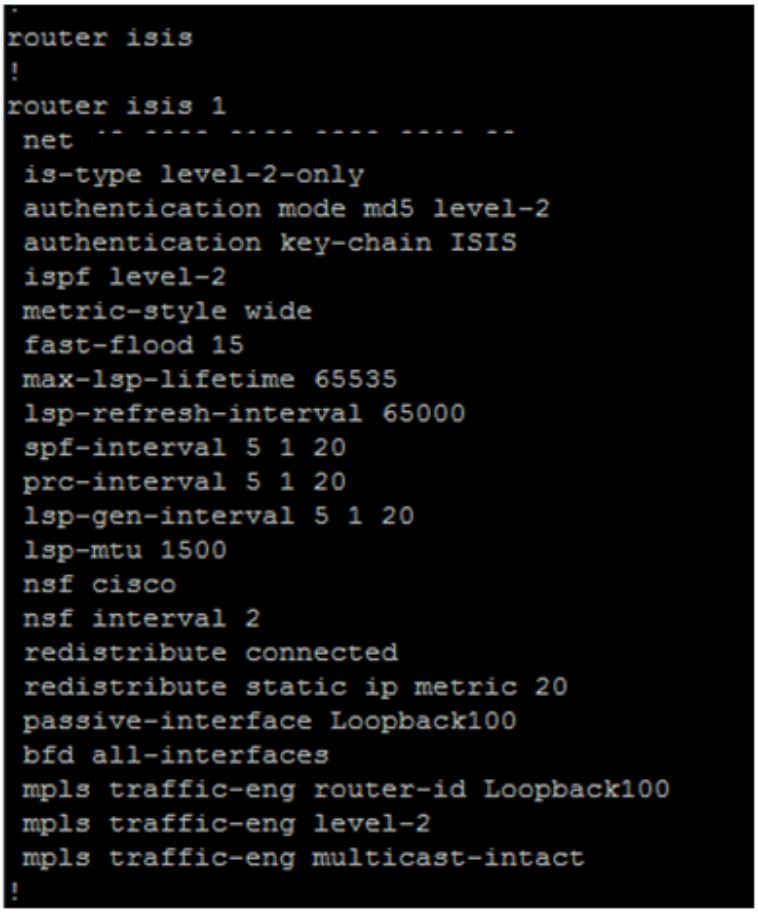


Figura 2.11: Configuración IS-IS en MPLS CNT

router isis 1: se define la etiqueta del área de enrutamiento; en este caso la 1.

net: este comando configura la dirección NSAP (Network Service Access Point) para el proceso de enrutamiento.

is-type level-2-only: se utiliza para configurar el router para operar como un router de nivel dos (inter-área).

authentication key-chain ISIS: forma de autenticación predeterminada y creada anteriormente, esta llave tiene como nombre ISIS.

ispf level-2: añade ispf de nivel 2 al protocolo IS-IS.

metric-style wide: configura el router para generar y aceptar solo TLV´s* “new-style”.

fast-flood 15: determina el número de LSP´s para mejorar el tiempo de convergencia.

max-lsp-lifetime 65535: el máximo tiempo de vida de un LSP.

spf-interval 5 1 20 / prc-interval 5 1 20: comandos recomendados para rápida convergencia.

lsp-gen-interval 5 1 20: determina el número de segundos entre generación de LSP´s.

lsp-mtu 1500: tamaño del mtu definido para los LSP´s.

nsf cisco: característica propietaria de CISCO (Nonstop Forwarding).

nsf interval 2: se asegura que el tráfico de capa 2 no sea interrumpido.

redistribute connected: redistribuye las rutas que tienen IP habilitadas en una interfaz.

redistribute static ip metric 20: redistribuye rutas IP estáticas.

passive-interfaz Loopback100: hace que la interfaz Loopback100 actúe como interfaz pasiva, es decir no envía paquetes IS-IS en ella.

bfd all-interfaces: se habilita Bi-directional Forwarding Detection (BFD) en todas las interfaces.

mpls traffic-eng router-id Loopback100: configuración de ingeniería de tráfico en la interfaz loopback100.

2.4.5 BORDER GATEWAY PROTOCOL – PROTOCOLO DE PUERTA DE ENLACE DE BORDE (BGP) [32]

BGP es un protocolo de enrutamiento entre sistemas autónomos. Un sistema autónomo es una red o grupo de redes bajo una administración y políticas de enrutamiento comunes. BGP es utilizado para intercambiar información de enrutamiento en el internet y es el protocolo utilizado entre ISP`s.

Los clientes se conectan al ISP, y el ISP utiliza BGP para intercambiar rutas entre los clientes y los ISP`s. Cuando BGP se utiliza entre sistemas autónomos (AS), nos referimos al protocolo como BGP Externo (EBGP).

2.4.5.1 Configuración de BGP en la red MPLS zona Pichincha de CNT

La configuración de BGP de un PE para la red MPLS zona Pichincha se muestra en la figura 2.12; los demás equipos siguen el mismo tipo.

Dentro de la configuración de BGP se tienen los grupos de address-family (familia de direcciones), en las cuales se puede configurar sesiones de enrutamiento que utilizan direcciones IPv4, en la figura 2.13 se presentan los vecinos de una familia de direcciones.

router bgp 28006: definición del protocolo BGP con el número de proceso 28006; éste se mantendrá en todos los PE`s.

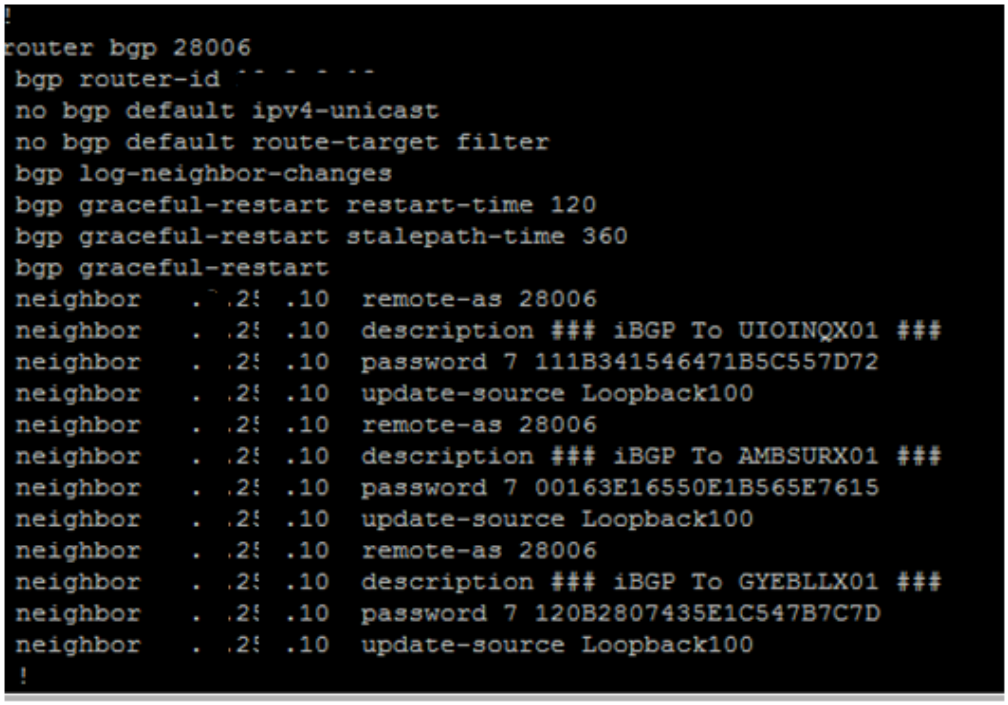


Figura 2.12: Configuración de BGP en MPLS CNT

bgp router-id 11.56.4.18: configuración manual del ID del protocolo, en este caso corresponde a la IP de gestión del equipo (11.56.4.18).

no bgp default ipv4-unicast: prepara el router para ser multiprotocolo y no solo anunciar familias de direcciones IPv4 que por defecto viene configurada.

no bgp default route-target filter: habilta la conmutación del psewdowire en un sistema autónomo de borde.

bgp log-neighbor-changes: permite mostrar en el log del router los cambios ocurridos entre vecinos bgp.

bgp graceful-restart restart-time 120: define el tiempo máximo de publicación a los vecinos.

bgp graceful-restart stalepath-time 360: define el tiempo máximo de espera para el mensaje End-of-RIB* de un vecino que se ha reiniciado antes de eliminar las rutas aprendidas.

bgp graceful-restart: habilita la funcionalidad de reinicio del protocolo en el router y también avisa de éste a sus vecinos.

neighbor 11.1.255.100 remote-as 28006: crea una entrada para un equipo par en la tabla de vecindad del bgp 28006.

neighbor 11.1.255.100 description: añade una descripción del vecino creado.

neighbor 11.1.255.100 password 7 111B341546471B5C557D72: autenticación de la conexiónn BGP entre vecinos.

neighbor 11.1.255.100 update-source Loopback100: configura el origen de la actualización de las rutas; en este caso, la encargada será la interfaz Loopback 100.

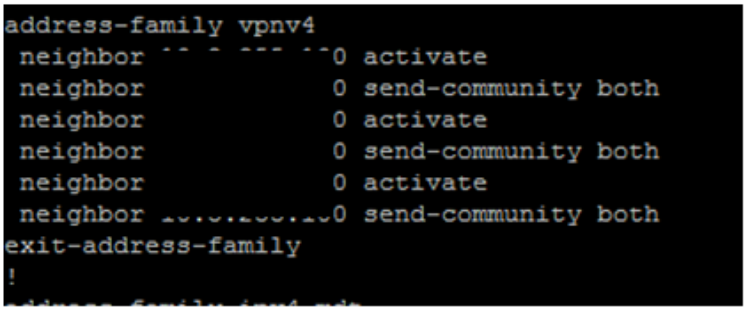


Figura 2.13: Configuración de familia de direcciones (address family) BGP

Para la configuración de clientes en los equipos, los mismos utilizan una VRF[27] la cual es única para cada uno, dependiendo de cuantos puntos de interconexión se

[27] Virtual routing and forwarding – Enrutamiento y Reenvío Virtual (VRF) es una tecnología de routers basada en IP que les permite crear y operar varias instancias de una tabla de enrutamiento al mismo tiempo.

tenga. Para que las rutas entre los puntos sean conocidas, se utiliza igualmente el protocolo BGP tal como se muestra en la figura 2.14.

```
address-family ipv4 vrf CYRANO
 no synchronization
 redistribute connected
 redistribute static
exit-address-family
```

Figura 2.14: Configuración de familia de direcciones (address family) BGP con VRF

2.4.6 CALIDAD DE SERVICIO (QoS) [33]

Una red de comunicaciones forma la columna vertebral de cualquier organización exitosa. Estas redes transportan un gran número de aplicaciones y datos, incluyendo vídeo de alta calidad y sensibles al retardo de datos tales como voz en tiempo real. Las aplicaciones de banda ancha estrechan las capacidades de red y recursos, pero también complementan, agregan valor y mejoran todos los procesos de negocio.

2.4.6.1 Configuración de QoS en la red MPLS zona pichincha de CNT [2]

En la tabla 2.6 se muestran los diferentes tipos de clase de servicio utilizados en la red MPLS zona Pichincha. En las figuras 2.15 y 2.16 se presenta la configuración actual de las políticas de servicio para la red MPLS de CNT.

Clases	Aplicación
Control de la red	Enrutamiento.
	Gestión de red.
	Voz.
VoIP	Video interactivo.
	Señalización de voz.
	Streaming de video.

Clases	Aplicación
Datos críticos	Datos críticos.
	Datos transaccionales.
Datos no críticos	Datos masivos.
	Mejor esfuerzo.
Defecto	Por defecto.

Tabla 2.6: Tipos de Clase de Servicio en MPLS CNT

A continuación se muestran las políticas que se implementan:

- Manejo de congestión en colas de salida.
- Se define la clase CM-VoIP como prioritaria.
- Limitación del 10% del ancho de banda en la cola prioritaria.
- Asignación de anchos de banda mínimos garantizados al resto de las clases de la siguiente manera:
    - Clase CM - Video: 30%
    - Clase CM – Control red: 3%
    - Clase CM – Datos críticos: 10%
    - Clase CM – Datos no críticos: 20%
    - Clase default: 15%

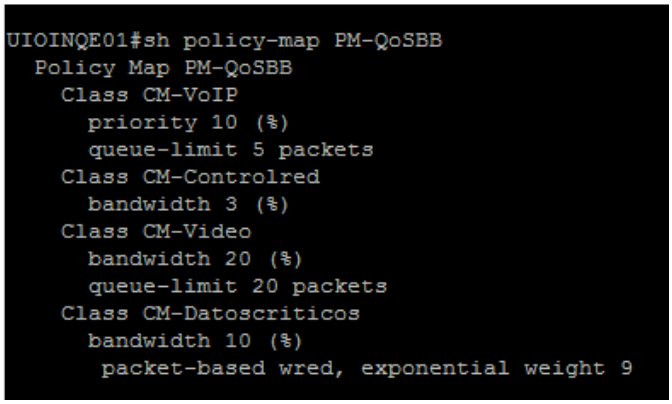


Figura 2.15: Politicas de servicio para MPLS CNT

```
UIOINQE01#sh class-map

 Class Map match-any CM-VoIP (id 1)
   Match mpls experimental topmost 5
   Match ip  precedence 5

 Class Map match-all 396Mbps (id 2)
   Match any

 Class Map match-all copp-class-fragments (id 3)
   Match access-group name copp-fragmented

 Class Map match-all 9Mbps (id 4)
   Match any

 Class Map match-any CM-Controlred (id 5)
   Match mpls experimental topmost 6  7
   Match ip  precedence 6  7

 Class Map match-all 4Mbps (id 6)
   Match any

 Class Map match-all 336Mbps (id 7)
   Match any

 Class Map match-all 100Mbps (id 8)
   Match any

 Class Map match-all 1Mbps (id 9)
   Match any

 Class Map match-all 2Mbps (id 10)
   Match any

 Class Map match-all 3Mbps (id 11)
   Match any
```

Figura 2.16: Clases de servicio para MPLS CNT

2.4.6.2 Configuración de clientes

Cada cliente que requiera contratar un servicio provisto por CNT ya sea de Datos, Internet o Telefonía y que necesite de IP´s en este caso de versión 4 para su funcionamiento, se configurarán en la red MPLS a nivel de capa 3. Para esto cada uno de ellos utiliza una VRF la cual es única por cada cliente dependiendo del servicio contratado, de esta manera tenemos:

- **vrf netcnt / netdef:** utilizada por clientes corporativos para el servicio de internet.
- **vrf voipxxx:** utilizada por clientes corporativos para servicios de voz.
- **vrf datxxxx:** utilizada por clientes corporativos para servicio de datos.

Cuando se habla de VRF es casi como un sinónimo de VPN MPLS. Las VRF´s son comúnmente utilizadas por proveedores de servicio dentro de una nube MPLS con múltiples clientes. La característica más interesante de esto es que se permite la creación de múltiples tablas de enrutamiento dentro de un router. Esto significa que la superposición de direcciones IP de clientes diferentes es posible.

Para configurar un cliente con su VRF es necesario seguir los procedimientos siguientes:

- **Configuración de vrf:** en la figura 2.17 se muestra la declaración y configuración de la VRF.

```
ip vrf CYRANO
 description CYRANO
 rd 172:19
 route-target export 172:100
 route-target import 172:100
!
!
```

Figura 2.17: Configuración de VRF para MPLS CNT

ip vrf CYRANO: se declara la VRF; en este caso el nombre de la misma es CYRANO.

description CYRANO: se utiliza el comando para añadir una descripción a la VRF.

rd 172:19: se crea una tabla VRF especificando una ruta diferenciadora o route distinguisher. Se ingresa un número de sistema autónomo y un número arbitrario; en este caso 172:19.

route target: crea una lista de comunidades para el destino de la ruta; éstas pueden ser importadas o exportadas.

- **Configuración de address-family en BGP:** para que la VRF del cliente, así como la tabla de enrutamiento se pueda propagar por la red MPLS se necesita configurar dentro del BGP un “address-family” como se muestra en la figura 2.18:

```
router bgp 28006
 !
 address-family ipv4 vrf CYRANO
  no synchronization
  redistribute connected
  redistribute static
 exit-address-family
!
```

Figura 2.18: Configuración de address family para un cliente en la red MPLS CNT

address-family ipv4 vrf: se configuran sesiones de enrutamiento que utilizan prefijo de dirección IPv4, y se especifica CYRANO como la VRF a asociar las consecuentes configuraciones.

no synchronization: habilita el router para anunciar una ruta de red sin esperar a que IGP lo haga.

redistribute: redistribuye las rutas ya sean estáticas, RIP, OSPF o las directamente conectadas.

- **Configuración de interfaz:** se procede a configurar el cliente en capa 3, como se muestra en la figura 2.19, asignando una IP privada; la misma que por lo general tiene una máscara de 32 bits ya que solo dos IP´s por circuito se configurarían; una en la red MPLS y la otra en el equipo terminal del cliente.

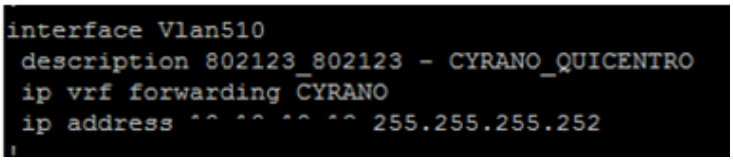


Figura 2.19: Configuración de interfaz para un cliente MPLS CNT

ip vrf forwarding CYRANO: se añade la VRF CYRANO a la interfaz correspondiente; en este caso la vlan 510.

2.4.6.1.1 Conectividad entre clientes

En las figuras 2.20 y 2.21 se puede observar la aplicación de los puntos anteriormente configurados. Se tiene conectividad entre la matriz de un cliente y su sucursal, demostrando de esta manera el correcto funcionamiento de la red.

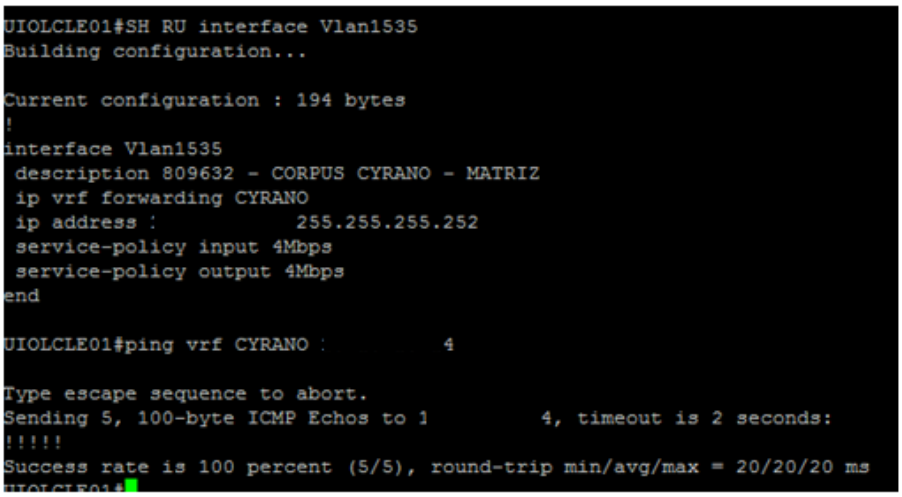


Figura 2.20: Conectividad del cliente desde Matriz hasta sucursal.

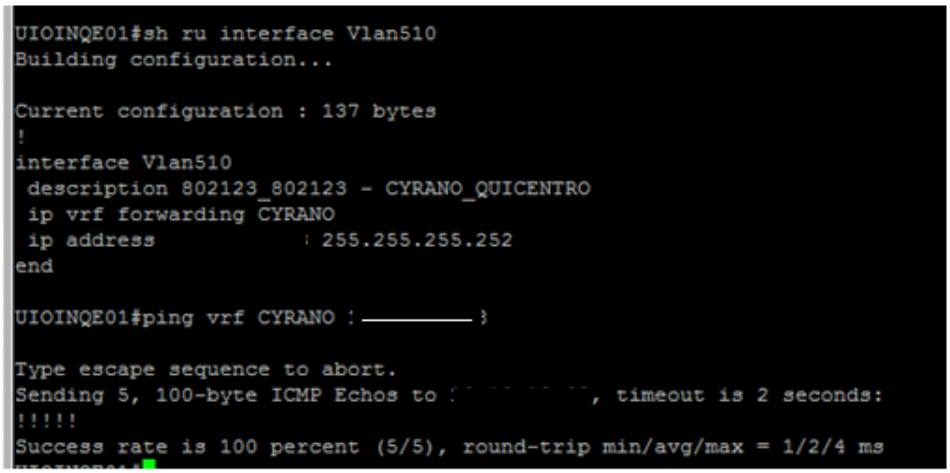


Figura 2.21: Conectividad del cliente desde sucursal hasta Matriz.

2.5 DESCRIPCIÓN DE LAS DIRECCIONES IPv4 DISPONIBLES EN ECUADOR

2.5.1 INTRODUCCIÓN [37]

El Director Ejecutivo de LACNIC, Raúl Echeberría, en la reunión del Registro de Direcciones de Internet para América Latina y el Caribe que se desarrolla en Quito hasta el 11 de mayo de 2012, indicó que en el 2015 habrá 120 millones de nuevos usuarios de Internet y especificó que en Ecuador serán 3,5 millones nuevos usuarios en 3 años y medio.

Dijo que cuando se acaben las direcciones de protocolo denominado IPv4, el cual es utilizado en la mayoría de conexiones de acceso a la internet, se van a presentar diversas situaciones: existirá pequeños bloques de esas direcciones para asignar a los nuevos operadores, como apoyo para desarrollar sus redes sobre IPv6 y las grandes operadoras van a tener que optimizar las direcciones IPV4 que ya tienen. Con relación al crecimiento de internet en Latinoamérica indicó que estamos en una

etapa de muy buen crecimiento con un 40% de acceso promedio de penetración de la Región.[28]

2.5.2 LACNIC [38]

LACNIC, el Registro de Direcciones de Internet para América Latina y Caribe, es una organización no gubernamental internacional establecida en Uruguay en el año 2002. Es responsable de la asignación y administración de los recursos de numeración de Internet (IPv4, IPv6), Números Autónomos y Resolución Inversa, entre otros recursos para la región de América Latina y el Caribe. Es uno de los 5 Registros Regionales de Internet en el mundo.

LACNIC contribuye al desarrollo de Internet en la región mediante una política activa de cooperación, promoviendo y defendiendo los intereses de la comunidad regional y colaborando en generar las condiciones para que Internet sea un instrumento efectivo de inclusión social y desarrollo económico para todos los países y ciudadanos de América Latina y el Caribe.

2.5.3 CANTIDAD DE DIRECCIONES IPV4 ACTUALMENTE DISPONIBLES Y UTILIZADAS EN ECUADOR. [39]

Siendo que el consumo diario de direcciones IP públicas es abismal; no es posible definir un número exacto de direcciones IP´s disponibles ya que éstas van variando a medida que pasan los segundos. Por lo que LACNIC ha repartido la cantidad total por países otorgándoles un porcentaje. En la figura 2.22 se puede observar la división de países con su respectivo porcentaje para un número de distribución total de 558080 direcciones IP con máscara de 24 bits al 22 de marzo del 2013.

---

28 http://www.supertel.gob.ec/index.php?option=com_content&view=article&id=535:lacnic-xvii-en-ecuador-existiran-35- millones-de-nuevos-usuarios-de-internet-en-3-anos-y-medio&catid=69:lacnicxvii&Itemid=331

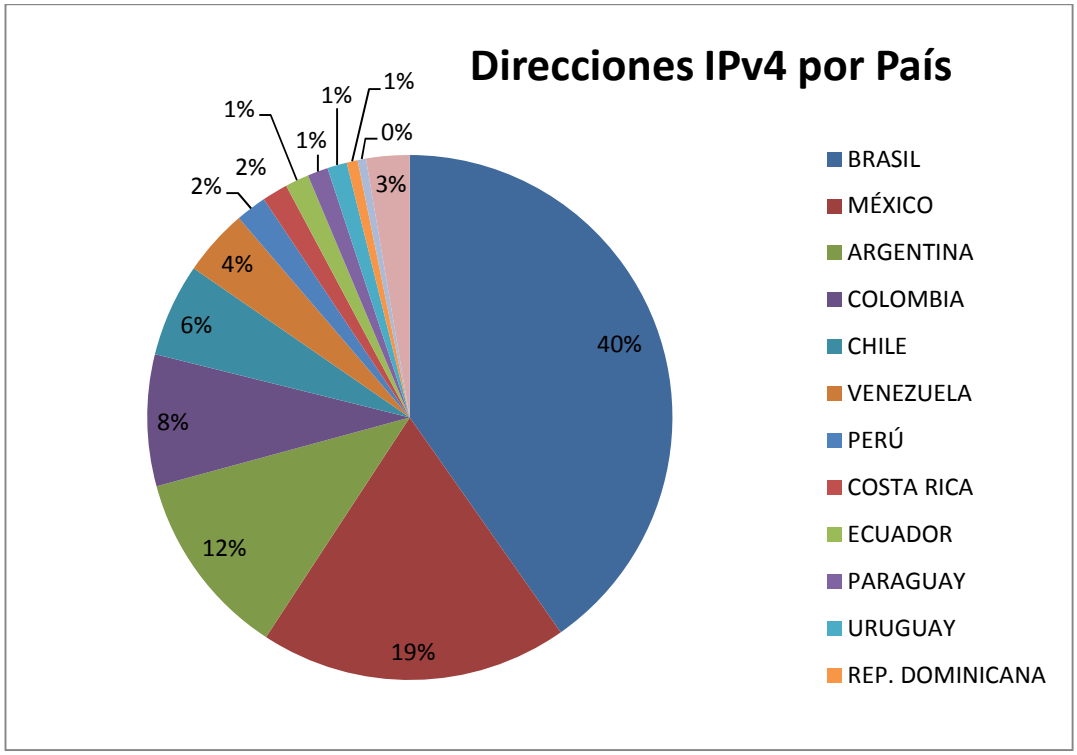


Figura 2.22: Distribución de las asignaciones de IPv4 por país. [39]

La tabla 2.7 se obtiene a partir del gráfico anterior.

PAÍS	PORCENTAJE	IP`S DISPONIBLES
BRASIL	40,24%	224571,392
MÉXICO	18,97%	105867,776
ARGENTINA	11,56%	64514,048
COLOMBIA	8,11%	45260,288
CHILE	5,73%	31977,984
VENEZUELA	4,10%	22881,28
PERÚ	1,91%	10659,328
COSTA RICA	1,59%	8873,472
ECUADOR	**1,45%**	**8092,16**
PARAGUAY	1,27%	7087,61
URUGUAY	1,20%	6696,96
REP. DOMINICANA	0,69%	3850,752
BOLIVIA	0,51%	2846,208

PAÍS	PORCENTAJE	IP`S DISPONIBLES
OTROS	2,67%	14900,736
TOTAL	**100%**	**558080**

Tabla 2.7: Distribución de las asignaciones de IPv4 por país.

En donde se observa que Ecuador dispone de 8092,16 IP`s públicas disponibles al 22 de marzo del 2013.

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO 2

LIBROS

[1] **Cisco Networking Academy,** *"Cisco CCNA 3 Exploración, Conmutación y Conexión Inalámbrica de Lan, Version 4.0 en Español"*. Otoño 2010.

[2] Información proporcionada por O&M PLATAFORMAS IP-MPLS CNT EP.

TESIS

[3] **Freire** Freire, Carlos Hernán*;* **Peréz** Gutiérrez, Santiago Javier, "Análisis de factibilidad de migración de la red asynchronous transfer mode ATM de ANDINATEL a multi-protocol label switching MPLS". EPN. 2005.

[4] **Hidalgo** Llumiquinga Carlos Luis; **Laguapillo** Muñoz David Alejandro, "Diseño e implementación de un laboratorio que permita emular y probar servicios IP y MPLS de la red Backbone Cisco de la Corporación Nacional de Telecomunicaciones CNT". EPN. Noviembre 2011.

PDF's, RFC's

[5] **ANÓNIMO,** *"New Cisco ME 3800X Series Carrier Ethernet Switch Router"* **URL:**http://www.cisco.com/en/US/prod/collateral/switches/ps10905/ps10965/product_bulletin_c25-629133.pdf Consultado el 18 de Marzo de 2013

[6] **ANÓNIMO,** *"Cisco CRS-1 8-Slot Single-Shelf System"* **URL:**http://www.cisco.com/en/US/prod/collateral/routers/ps5763/ps6112/product_data_sheet0900aecd801d53a1.pdf Consultado el 20 de Marzo de 2013

[7] **ANÓNIMO,** *"Cisco CRS 8-Slot Line-Card Chassis Route Processor"*

URL:http://www.cisco.com/en/US/prod/collateral/routers/ps5763/ps6112/product_data_sheet0900aecd801d53aa.pdf Consultado el 20 de Marzo de 2013

[8] **ANÓNIMO,** *"Cisco Carrier Routing System"*
URL:http://www.cisco.com/en/US/prod/collateral/routers/ps5763/prod_brochure0900aecd800f8118.pdf Consultado el 22 de Marzo de 2013

[9] **ANÓNIMO,** *"Cisco CRS Carrier Routing System 16-Slot Line Card Chassis System Description"*
URL:http://www.cisco.com/en/US/docs/routers/crs/crs1/16_slot_lc/system_description/reference/guide/sysdsc.pdf Consultado el 22 de Marzo de 2013

[10] **ANÓNIMO,** *"SIP and SPA Product Overview"*
URL:http://www.cisco.com/en/US/docs/interfaces_modules/shared_port_adapters/install_upgrade/crs/crs1/installation/guide/crsinthw.pdf Consultado el 22 de Marzo de 2013

[11] **ANÓNIMO,** *"Enhanced Performance, Versatility, High Availability, and Reliability at the Provider Edge"*
URL:http://www.cisco.com/en/US/prod/collateral/routers/ps368/ps367/product_data_sheet0900aecd8057f3d2.pdf Consultado el 23 de Marzo de 2013

[12] **ANÓNIMO,** *"Cisco 7600 Series Route Switch Processor 720"*
URL:http://www.cisco.com/en/US/prod/collateral/routers/ps368/product_data_sheet0900aecd8057f3b6.pdf Consultado el 23 de Marzo de 2013

[13] **ANÓNIMO,** *"Cisco 7600 Series Ethernet Services Plus 20 and 40-Gbps Line Cards"*
URL:http://www.cisco.com/en/US/prod/collateral/routers/ps368/data_sheet_c78-49152.pdf Consultado el 23 de Marzo de 2013

[14] **ANÓNIMO,** *"Cisco ASR 1000 Series Route Processor"* **URL:**http://www.cisco.com/en/US/prod/collateral/routers/ps9343/product_bulletin_c25-443045.pdf Consultado el 23 de Marzo de 2013

[15] **ANÓNIMO,** *"Cisco ASR 1000 Series Embedded Services Processors"* **URL:**http://www.cisco.com/en/US/prod/collateral/routers/ps9343/product_bulletin_c25-449981.pdf Consultado el 17 de Marzo de 2013

[16] **ANÓNIMO,** *"Cisco ASR 1000 Series SPA Interfaz Processor"* **URL:**http://www.cisco.com/en/US/prod/collateral/routers/ps9343/product_bulletin_c25-443180.pdf Consultado el 19 de Marzo de 2013

[17] **ANÓNIMO,** *"Cisco ME 6500 Series Ethernet Switch"* **URL:**http://www.cisco.com/en/US/prod/collateral/switches/ps6568/ps6845/ps6846/product_data_sheet0900aecd8040657e.pdf Consultado el 18 de Marzo de 2013

[18] **ANÓNIMO,** *"Configuring Cisco Express Forwarding"* **URL:**http://www.cisco.com/en/US/docs/ios/12_2/switch/configuration/guide/xcfcefc.pdf Consultado el 17 de Marzo de 2013

[19] **ANÓNIMO,** *"Configuring Logical Interfaces"* **URL:**http://www.cisco.com/en/US/docs/ios/12_2/interfaz/configuration/guide/icflogin.pdf Consultado el 17 de Marzo de 2013

[20] **ANÓNIMO,** *"MPLS Label Distribution Protocol (LDP)"* **URL:**http://www.cisco.com/en/US/docs/ios/12_4t/12_4t2/ftldp41.pdf Consultado el 3 de Marzo de 2013

[21] **ANÓNIMO,** *"Introduction to Intermediate System-to-Intermediate System Protocol"*

URL: http://www.cisco.com/warp/public/cc/pd/iosw/prodlit/insys_wp.pdf Consultado el 30 de Marzo de 2013

[22] **ANÓNIMO,** *"Policing and Shaping Overview"* **URL:**http://www.cisco.com/en/US/docs/ios/12_2/qos/configuration/guide/qcfpolsh.pdf Consultado el 1 de Marzo de 2013

[23] **VARIOS AUTORES,** *"RFC 2475: An Architecture for Differentiated Services".* Diciembre. 1998

[24] **VARIOS AUTORES,** *"RFC 1633: Integrated Services in the Internet Architecture: an Overview"*. Junio. 1994.

[25] **ANÓNIMO,** *"Cisco ME 6524 Ethernet Switch"* **URL:**http://www.cisco.com/en/US/prod/collateral/switches/ps6568/ps6845/qa_c67_468636.pdf Consultado el 13 de Marzo de 2013

[26] **ANÓNIMO,** *"Cisco CRS SPA Interfaz Processor-800"* **URL:**http://www.cisco.com/en/US/prod/collateral/routers/ps5763/product_data_sheet0900aecd80280a68.pdf Consultado el 30 de Marzo de 2013

INTERNET

[27] **ANÓNIMO**, *"Cisco 7606 Internet Router".* **URL:** http://www.hardware.com/store/cisco/7606-2SUP720XL-2PS Consultado el 30 de Marzo de 2013

[28] **ANÓNIMO,** *"Cisco ASR 1000 Series Aggregation Services Routers"* **URL:** http://www.cisco.com/en/US/products/ps9343/index.html

Consultado el 21 de Marzo de 2013

[29] **ANÓNIMO,** *"Introducción a CEF".*
URL: http://librosnetworking.blogspot.com/2007/01/introduccin-cef.html

[30] **ANÓNIMO,** *"How To Configure Cisco Express Forwarding (CEF)".*
URL: https://supportforums.cisco.com/docs/DOC-5145
Consultado el 11 de Febrero de 2013

[31] **ANÓNIMO,** *"IS-IS - Intermediate System to Intermediate System"*
URL:http://www.redespracticas.com/enrutamiento/isis/intermediate/system/level-1/level-2/l1/l2/niveles/area/estado/enlace/mac/capa/2/clnp/clns/net/cisco/configuracion/ios/?pag=txtEnrutamientoISIScsco.php&Njs=t
Consultado el 18 de Mayo de 2012

[32] **ANÓNIMO,** *"Border Gateway Protocol"*
URL: http://docwiki.cisco.com/wiki/Border_Gateway_Protocol
Consultado el 30 de Julio de 2012

[33] **ANÓNIMO,** *"Quality of Service (QoS)"*
URL:http://www.cisco.com/en/US/products/ps6558/products_ios_technology_home.html
Consultado el 30 de Julio de 2012

[34] **ANÓNIMO,** *"Differentiated Services"*
URL:http://www.cisco.com/en/US/products/ps6610/products_ios_protocol_group_home.html
Consultado el 30 de Julio de 2012

[35] **ANÓNIMO,** *"Integrated Services"*

URL:http://www.cisco.com/en/US/products/ps6611/products_ios_protocol_group_home.html
Consultado el 3 de Agosto de 2012

[36] **ANÓNIMO,** *"Network Based Application Recognition (NBAR)"*
URL:http://www.cisco.com/en/US/products/ps6616/products_ios_protocol_group_home.html
Consultado el 22 de Octubre de 2012

[37] **ANÓNIMO,** *"LACNIC XVII: En Ecuador existirán 3,5 millones de nuevos usuarios de internet en 3 años y medio"*
URL:http://www.supertel.gob.ec/index.php?option=com_content&view=article&id=535:lacnic-xvii-en-ecuador-existiran-35-millones-de-nuevos-usuariosde-internet-en-3-anos-y-medio&catid=69:lacnicxvii&Itemid=331
Consultado el 30 de Julio de 2012

[38] **ANÓNIMO,** *"Acerca de LACNIC"*
URL: http://www.lacnic.net/web/lacnic/acerca-lacnic
Consultado el 30 de Julio de 2012

[39] **ANÓNIMO,** *"Estadísticas de Asignación de LACNIC"*
URL: http://www.lacnic.net/web/lacnic/estadisticas-asignacion
Consultado el 30 de Julio de 2012

[40] **ANÓNIMO,** *"Tecnología CNT"*
URL: https://www.cnt.gob.ec/index.php/tecnologia
Consultado el 13 de Febrero de 2012

[41] **ANÓNIMO,** *"Frame-Mode MPLS"*
URL:http://networks-baseline.blogspot.com/2012/05/frame-mode-mpls-in-frame-mode-mpls.html Consultado el 18 de Mayo de 2012

CAPÍTULO 3

ANÁLISIS Y PROPUESTA DE MÉTODOS DE MIGRACIÓN DE IPV4 A IPV6 EN REDES MPLS

Debido a que se espera que los dos protocolos IPV4 e IPV6 convivan durante un tiempo considerable y que la implementación de IPV6 sea paulatina, se analizarán varios mecanismos de convivencia y migración para los equipos de la red en estudio.

La clave para la transición, está en la red actual, es decir: los equipos instalados y su capacidad. Esto ayudará a que los elementos de la red que usen IPV6 se comuniquen con los equipos que aún tengan IPV4; y así hacer una migración paulatina.

A continuación se muestra un análisis de los principales métodos de migración, posterior a esto se indicará el flujo de migración a realizarse.

3.1 IPV6 SOBRE IPV4 [3]

Un paquete IPV6 es transmitido transparentemente después de haber sido encapsulado en un paquete IPV4.

Durante la transición de IPV4 a IPV6, las redes IPV4 han sido ampliamente desarrolladas mientras que las redes IPV6 están dispersas por el mundo. No es una solución económica unir estas redes aisladas con líneas privadas.

El método usual para este tipo de conexiones es la tecnología de túneles o VPNs sobre una red IPV4. Los diferentes tipos de túneles permiten varias opciones el

momento de interconectar las redes IPV6 aisladas. El primer paso para la implementación de estos túneles es la activación de Dual-Stack.

3.1.1 DUAL STACK RFC 4213 [2] [3]

Dual Stack se refiere a un stack de protocolos IPV4 e IPV6 en dispositivos terminales y nodos de red para permitir la comunicación entre IPV4 e IPV6 separadamente. Los nodos que soportan IPV4/IPV6 son llamados “nodos dual-stack”.

Dual stack nos ayuda con la implementación de túneles en el borde de la red, esto quiere decir que los equipos que realizan un túnel son capaces de soportar IPV4 e IPV6; pero al usar Dual-Stack, en una migración completa[29] se configurarán todos los equipos de la red para que soporten IPV4 e IPV6.

3.1.2 TIPOS DE TÚNELES IPV6 SOBRE IPV4 [1][5]

En la figura 3.1 se muestra el principio de funcionamiento de un túnel IPV6 sobre una red IPV4.

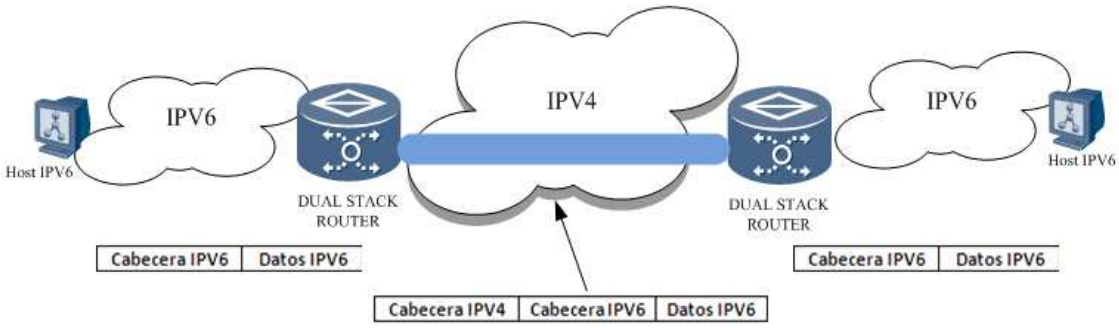


Figura 3.1: Diagrama esquemático de un túnel.

El túnel virtual que transmite paquetes IPV6 entre dispositivos de borde es llamado, un túnel IPV6 sobre IPV4.

[29] Dual-Stack Nativo.

Los túneles pueden ser clasificados de la siguiente manera:

- **Túnel 6 over 4**

Es un tipo de túnel IPV6 que se implementa sobre una red IPV4, para la implementación del mismo se usa 6to4 en los routers de borde. En la figura 3.2 se presenta el túnel 6 over 4.

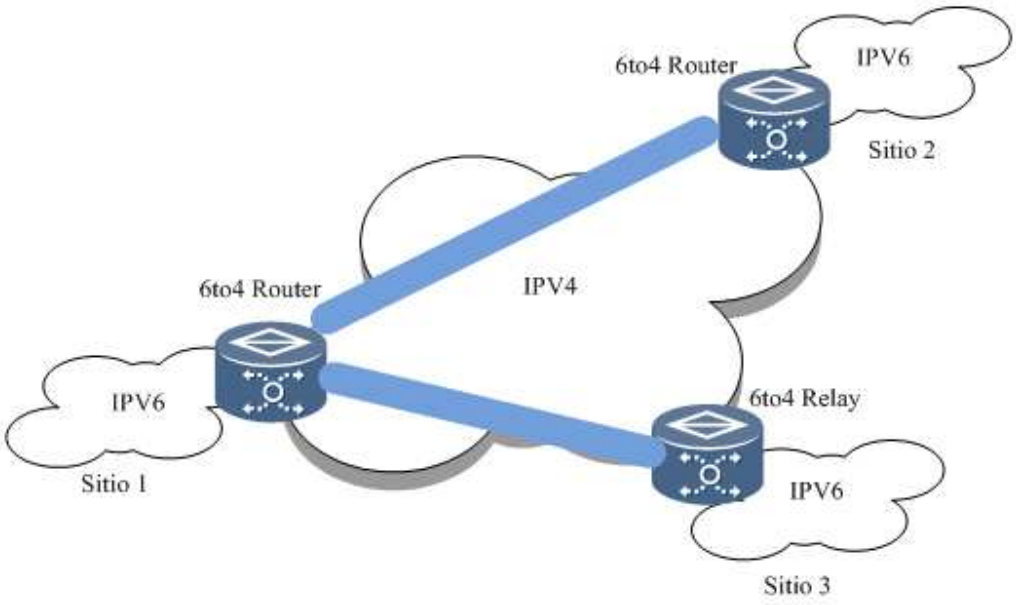


Figura 3.2: Diagrama esquemático de un Túnel 6over4

El túnel 6over4 define un método para generar una dirección IPv6 local a partir de una dirección IPv4, y un mecanismo para realizar un Descubrimiento de Vecinos (Neighbor Discovery) sobre IPv4. Cualquier host que quiera participar en 6over4 sobre una red IPv4 puede establecer una interfaz de red virtual IPv6.

- **Túnel ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)**

En la Figura 3.3 se observa un túnel ISATAP. Este túnel se configura de la siguiente manera:

- En ambos routers de borde se configura la interfaz “tunnel” especificando como origen las loopbacks de cada equipo.
- Después el router asigna los identificadores de interfaz automáticamente.

Para probar conectividad se configura EIGRPv6 (Enhanced Interior Gateway Routing Protocol Version 6) especificando el router vecino, esto dada la naturaleza NBMA de los túneles que no tienen destino específico.

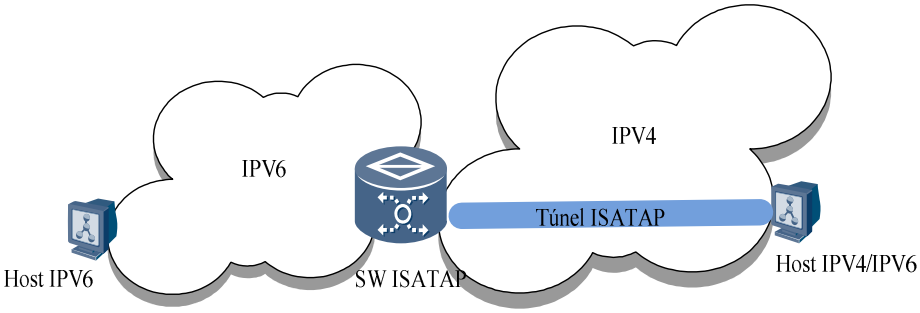


Figura 3.3 Diagrama esquemático túnel ISATAP

- **6PE (IPV6 Provider Edge)**

En la figura 3.4 se muestra la interconexión de diferentes routers usando 6PE.

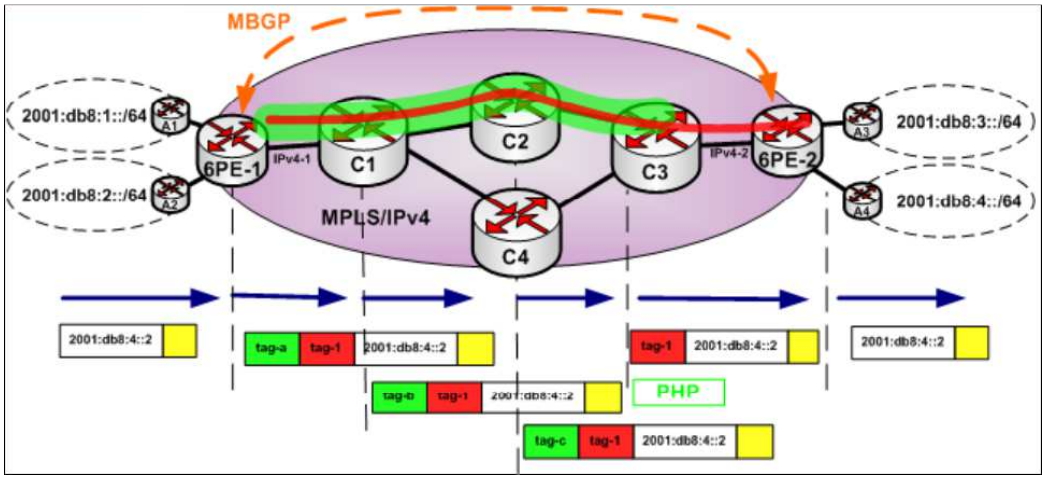


Figura 3.4 Diagrama de interconexión 6PE

6PE no usa VRFs ni túneles, éste comunica a los routers de borde en los que sea activado. No es una opción tan segura como 6VPE.

Los pasos para la configuración son:

- Configurar el Backbone utilizando OSPF 1 Area.
- Configurar LDP en el Backbone.
- Crear sesión IPv6 BGP malla completa entre los PEs.

- **6VPE (IPV6 Virtual Provider Edge)**

En la figura 3.5 se presenta el diagrama de red para un túnel 6VPE.

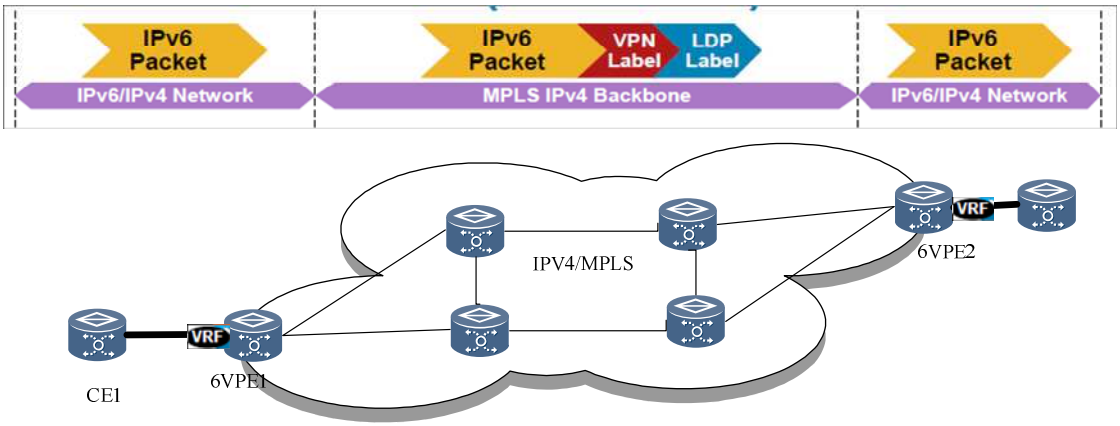


Figura 3.5 Diagrama de interconexión 6VPE

Para configurar 6VPE se siguen los siguientes pasos:

- Activar IPV6 routing e IPV6 CES.
- Configurar MP-BGP para el intercambio de rutas VPN.
- Configurar las tablas VRF IPV6.
- Configurar las interfaces VRF.
- Configurar los protocolos de ruteo IPV6 entre los CE-PE.

- Redistribuir los protocolos de ruteo entre CE-PE, y las rutas en la MP-BGP.

En la tabla 3.1 se analizará las principales características de los métodos descritos.

	Dual-Stack Nativo	**MPLS 6PE/6VPE**	**Túnel 6over4**
Costos de implementación.	IPV6 es activado en todos los nodos. Altos costos de implementación.	IPV6 es activado solo en routers PE. Costos de implementación bajos.	IPV6 es activado solo en routers PE o algún hardware necesita ser reemplazado.
Despliegue de protocolos.	IPV6 IGP/BGP operando en todos los routers IGP: OSPF/OSPFv3/ISIS multi-topology BGP: BGP/BGP4+	Los routers P no sufren cambios. MP-BGP entre PEs.	IGP: OSPF/ISIS BGP: BGP Tunnel: GRE tunnel/6over4 tunnel Un túnel puede ser OSPFv3/BGP4+.
Escalabilidad.	Ilimitada.	Ilimitada.	El túnel tiene N^2 conexiones, escalabilidad limitada.
Costos de Mantenimiento.	Se debe dar mantenimiento al nuevo protocolo en todos sus nodos.	Solo los PEs deben tener mantenimiento, con respecto a IPV6.	Se requiere muchos túneles, el mantenimiento es más complicado.
Servicios Soportados.	Unicast/Multicast.	Los servicio Multicast aún no son maduros, se soporta VPNs.	Servicios Multicast no muy bien desarrollados.
Seguridad.	Más riesgos de seguridad.	La seguridad en MPLS no es afectada.	Los túneles pueden ser atacados.

Tabla 3.1: Tabla de comparación entre dual Stack nativo, MPLS 6VPE y túneles 6over4

3.2 IPV4 SOBRE IPV6 [3]

Se pueden crear túneles en una red IPV6 para conectar sitios IPV4 aislados, así estos sitios pueden acceder a otros IPV4 a través de la red IPV6. Este no es el caso

de estudio para el presente proyecto debido a que la red de la CNT EP es una red MPLS IPV4.

Durante la transición de IPV4 a IPV6, las redes IPV6 son ampliamente desarrolladas, por lo que las redes IPV4 se vuelven aisladas. La figura 3.6 indica la estructura de un túnel IPV4 sobre una red IPV6.

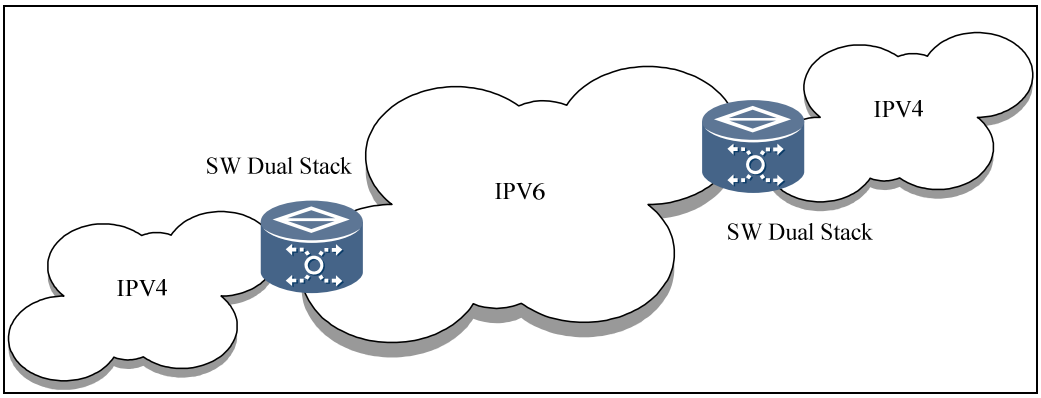


Figura 3.6 Diagrama de red de un túnel IPV4 sobre una red IPV6

3.3 ESTRATEGIA DE DESARROLLO

Para el escenario de CNT tenemos dos opciones de migración en las cuales se pueden aplicar cualquiera de los mecanismos de transición revisados anteriormente. A continuación se indican las opciones de migración para la red de CNT EP.

3.3.1 OPCIÓN 1: MIGRACIÓN DEL BACKBONE

Al usar esta opción, el backbone es convertido a dual stack (IPV4 e IPV6), y los servidores y clientes mantienen IPV4. Mientras cada región y servidor vaya migrando a IPV6, sus paquetes pueden viajar normalmente ya que el backbone es IPV6.

Dentro del backbone se debe mantener dos tipos de rutas, IPV4 e IPV6; los paquetes IPV6 irán a través del backbone como IPV6, y los paquetes IPV4 serán enviados

como paquetes IPV4. La figura 3.7 muestra el funcionamiento de dual stack en el backbone.

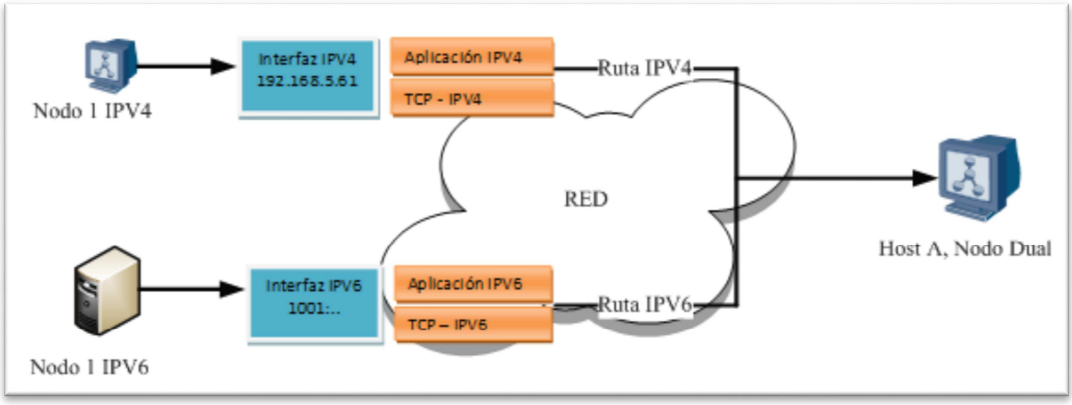


Figura 3.7 Modo Dual Stack en el Backbone

Ya sea un router o un host, pueden ser dual stack, un nodo dual stack puede correr el protocolo TCP/IP en IPV4 e IPV6. Esto es útil durante la transición a IPV6 ya que no todas las aplicaciones pueden ser convertidas a IPV6.

Así cada nodo puede enviar y recibir paquetes IPV4 e IPV6. Esta es una implementación muy común, y debe ser el primer paso de muchos para la migración a IPV6, incluso si no todos los dispositivos son migrados, como es el caso de la red MPLS de CNT EP. En la figura 3.8 se muestra la distribución lógica de los routers P de la red.

3.3.1.1 Ventajas de la migración del BackBone

- La conversión a IPV6 a nivel mundial ya ha comenzado, el 8 de Junio de 2012 fue el Lanzamiento Mundial de IPV6. Este método provee un punto de inicio para IPV6 y además es transparente para el usuario final.
- Las aplicaciones no necesitan ser convertidas, ya que es un método meramente dedicado a la red, tomando en cuenta que la conversión de aplicaciones será una de las áreas más difíciles y demorosas.

- Los grupos de soporte para operación y mantenimiento de red ganarán experiencia con IPV6 ya que uno de los grandes obstáculos de la migración es el conocimiento de los nuevos protocolos de IPV6.

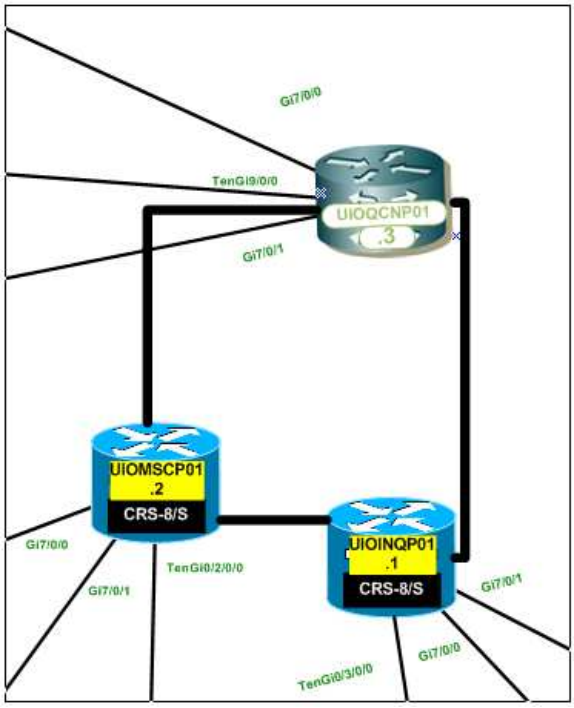


Figura 3.8 Diagrama lógico del core de la red CNT EP, Pichincha.[30]

3.3.1.2 Desventajas de la migración del BackBone

En las migraciones hay muchos riesgos involucrados y se puede mencionar los siguientes:

- Las migraciones de usuarios deben ser paulatinas y no migrar todos a la vez ya que si existe un problema muchos usuarios pueden verse afectados. De preferencia se deben cubrir las falencias antes de la implementación. Así mismo, mientras cada grupo de clientes es añadido, se debe ir corrigiendo los problemas que se presenten.

[30] Para diagrama completo refiérase a ANEXO 2.

- ¿Qué pasa si las rutas fallan?, como en IPV4 las rutas deben recuperarse ante fallas, pero los protocolos de enrutamiento de IPV6 no han sido probados ampliamente como lo han sido los de IPV4. No está claro que tan rápido ocurrirá la convergencia, si se crean lazos de rutas o si las tablas de rutas fallan puede ser un gran problema.
- Los routers que hacen la conversión generarán cuellos de botella.
- Se necesita realizar mucho más trabajo con respecto a configuraciones e implica más gastos debido a que más equipos dentro de la MPLS deben ser configurados como dual stack.

3.3.2 OPCIÓN 2: CONVERSIÓN DE EQUIPOS DE BORDE

En la figura 3.9 se presenta un esquema en la conversión de equipos de borde.

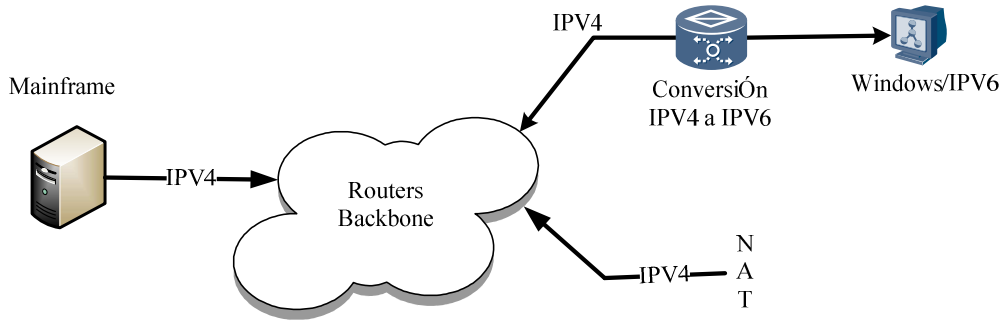


Figura 3.9 Conversión de equipos de borde

Los equipos de borde tendrán clientes IPV6 e IPV4, mediante el uso de túneles enviarán la información de clientes IPV6 sobre la MPLS IPV4 obteniendo el menor impacto en la red.

Los routers remotos deberán realizar la conversión de paquetes IPV6 a IPV4. Los paquetes IPV4 irán a través de la red y serán convertidos a IPV6 al final de la red.

La Figura 3.10 muestra como se comunicarán clientes remotos IPV6 sobre la MPLS que mantiene IPV4.

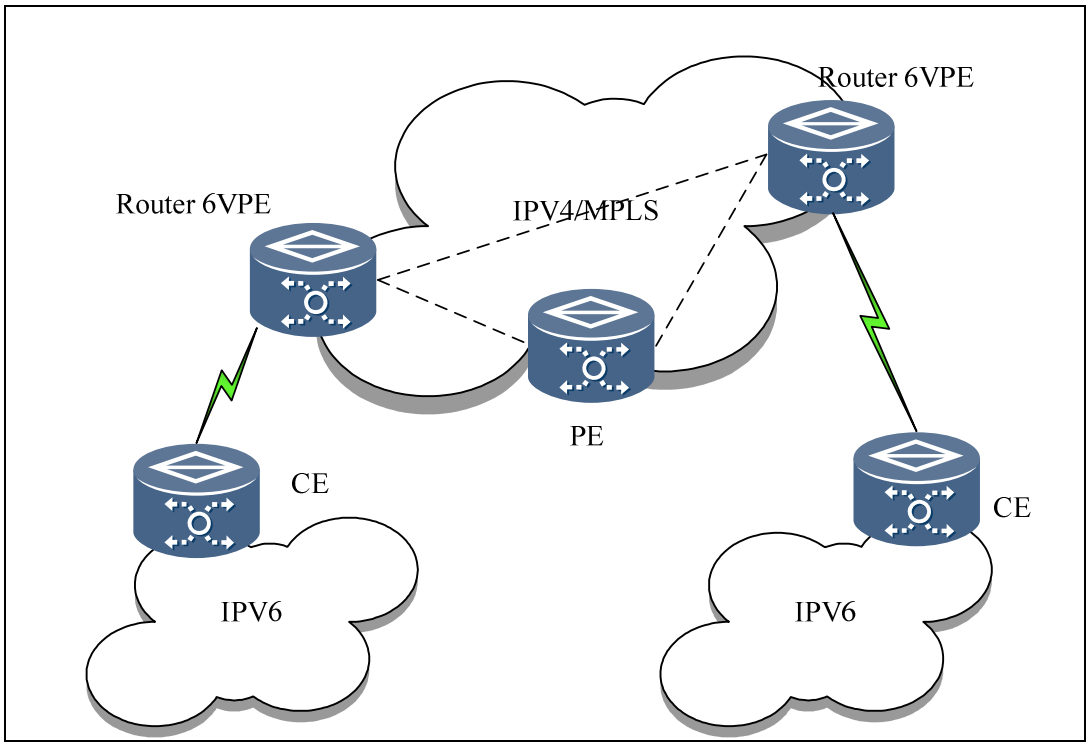


Figura 3.10: Diagrama de Conectividad entre equipos de borde

Los routers de backbone se mantendrán como IPV4 y sus respectivas rutas también. Todos los routers de los sitios remotos se conectan a los de backbone mediante IPV4.

Toda región o sitio remoto que desea usar IPV6 lo hará a través de túneles o un Gateway de traducción hacia el sitio remoto. Además se debe hacer una actualización de los routers para que puedan ser *dual-stack*, y configurarlos para que realicen túneles o traducciones. Políticas para usar métodos estándar de túneles deben ser situadas, así como traducciones y listas de acceso (ACL).

En la figura 3.11 muestra la distribución lógica de algunos de los routers PE de la red MPLS de la CNT EP.

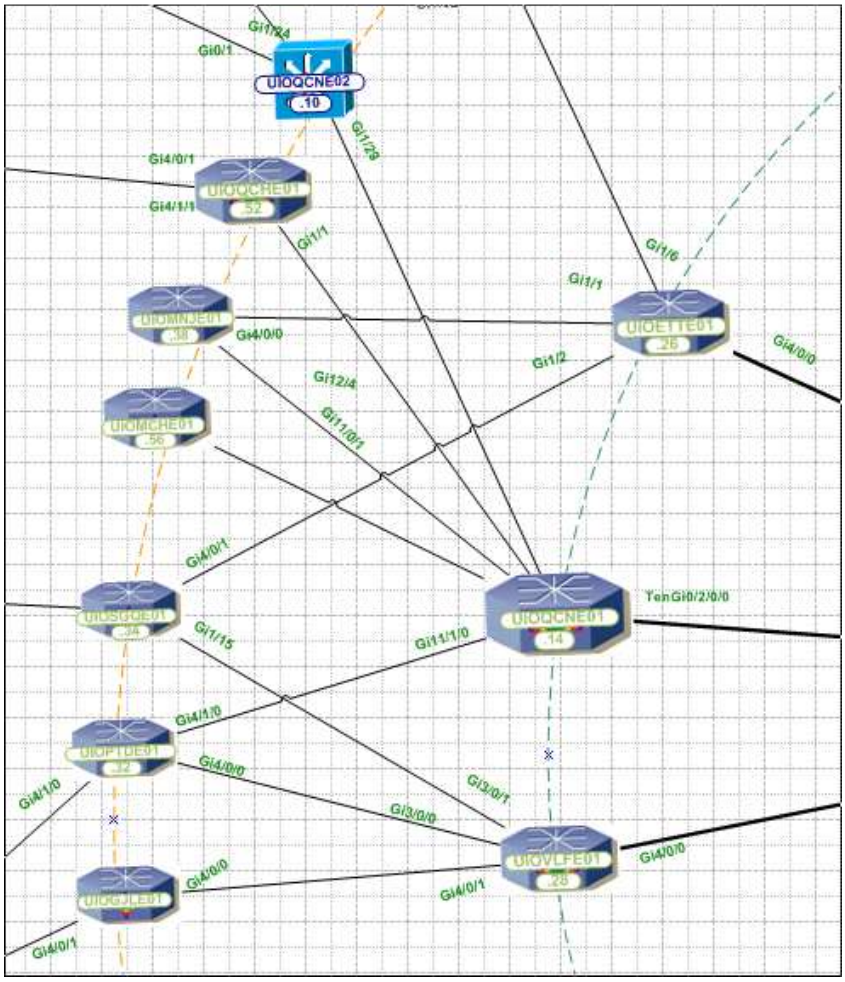


Figura 3.11: Diagrama lógico de los routers PE de IÑAQUITO de la red CNT EP, Pichincha.

3.3.2.1 Ventajas de la conversión de equipos de borde

- El hecho de que la conversión a IPV6 ya ha comenzado quiere decir, que este método facilitará la migración completa a IPV6.
- En esta propuesta, solo algunos routers remotos necesitan ser convertidos y así los routers de backbone pueden permanecer intactos. Pero si hay demasiadas regiones, esta ventaja puede volverse una desventaja, ya que se tendrá que migrar varios routers.

- El enrutamiento es menos complejo, se usa el mismo enrutamiento en el core; se puede usar rutas IPV4 a través de la red.
- No hay que cambiar las rutas en el backbone. Estos llevarán solo tráfico enrutado y la carga en el backbone es menos ya que los mismos no son responsables de la creación de rutas.
- El DNS se puede mantener como IPV4.

3.3.2.2 Desventajas de la conversión de equipos de borde

- Escalabilidad del túnel: Si muchos sitios con muchas aplicaciones empiezan a hacer túneles, entonces se añade una sobre cabecera que causará problemas.
- Actualmente, un sitio remoto puede hacer túneles IPV6 con paquetes IPV4 en su interior, y generar tráfico. Sin embargo, las operaciones de red y los firewalls no detectan esto.
- Los Firewalls de los sitios remotos no van a poder bloquear los paquetes apropiadamente o bloquear paquetes con protocolos importantes inapropiadamente.

3.4 PROPUESTA DE UNA METODOLOGÍA DE MIGRACIÓN [3][4][5]

Para cualquiera de los métodos descritos anteriormente, hay varios pasos que se deben elegir para este proceso. Por lo tanto IPV6 debe ser desarrollado en etapas; un sitio a la vez. Los pasos de planeación deben ser repetidos para todos los escenarios.

3.4.1 ESQUEMA DE LA METODOLOGÍA DE MIGRACIÓN

El presente esquema muestra el procedimiento requerido para migrar la plataforma IPV6 de la red MPLS de la CNT EP. Este está basado en el análisis de la información

recolectada durante la investigación realizada para el desarrollo del presente proyecto de titulación. Lo primero que se deberá identificar es el alcance, indicando que áreas vamos a cubrir, posterior a esto se indicará un procedimiento para una migración que cumpla con lo mencionado anteriormente. Concluidos estos pasos se podrá seleccionar el método de migración que mejor se ajuste a la red de estudio.

3.4.1.1 Alcance del esquema

Se desea cubrir las siguientes áreas:

- Infraestructura de red.
- QoS.
- Hardware y Software.

3.4.1.2 Flujo de Migración

El esquema establecido para la migración a IPV6 presenta dos fases principales. El primero es la activación de IPV6 y el segundo la configuración de los equipos involucrados. La tabla 3.2 muestra las fases de migración.

Fase 1: Equipos de Borde	**Fase 2:** Equipos de Borde/Core
Tiempo estimado: 1 día	Tiempo estimado: 1 día
• Activar dual-stack en los equipos seleccionados. • Configurar BGP en los routers.	• Configurar IPV6 en equipos de borde para enviar tráfico IPV6 a los usuarios que lo necesiten. • Configurar los routers vecinos para interconectar los clientes.

Tabla 3.2: Fases de migración

Llegado a este punto se debe tomar la decisión de que mecanismo de migración se va a utilizar. Para esto se toma como guía la tabla 3.1 la cual muestra las principales carácterísticas de cada uno de los métodos de migración estudiados.

Se ha decidido la migración de borde mediante el uso de túneles 6VPE, ya que se tendrá el menor impacto en la red, esto es debido a que la red MPLS de CNT EP ya tiene desplegada una configuración en IPV4, al usar IPV6 se necesita realizar túneles VPNs entre clientes IPV6 y así se puede convivir en conjunto IPV4 e IPV6. Con este método no se necesita actualizar ni migrar los routers de core, manteniendo el servicio transparente para los usuarios de los dos protocolos. Además de las siguientes razones:

- Para usar el esquema 6VPE se necesita de una red IPV6 BGP/MPLS VPN construida sobre un core MPLS IPV4, que es el caso de la red de CNT EP.
- La implementación de una VPN IPV6 es similar a una VPN IPV4. Los PEs intercambian información de ruteo VPN-IPV6 usando MP-BGP, y transmite paquetes privados IPV6 a través de túneles para nuestro caso.
- Las VPNs IPV6 son clasificadas en VPN de administración, de servicio individual y líneas arrendadas a empresas, estos para diferenciar los servcios.
- Actualmente la red IP/MPLS de la CNT EP cumple con el esquema necesario para poder realizar la migración.

El propósito de esta migración en los equipos de borde, es proveer soporte IPV6 solo donde sea requerido, tiempos de ejecución y minimizando gastos. IPV6 es estrictamente para usuarios que soporten esta característica. Actualmente, servicios de VPNv4 han sido implementados en la red MPLS de la CNT EP. Como parte de la transición a IPV6, 6VPE será implementado para permitir el paso de tráfico IPV6 sobre la red IP/MPLS.

La infraestructura de capa inferior de la MPLS no necesita ningún cambio, a más de la configuración para que se soporte IPV6 en los PEs correspondientes, este es otro

punto importante ya que el trabajo solo se limita a routers específicos en la red. Todos los servicios que se brindan a través del core IP/MPLS pueden tener activo IPV6. Esto permitirá la implementación gradual de servicios IPV6, sin poner en peligro la infraestructura existente y el desarrollo de la red.

3.4.2 IMPLEMENTACIÓN DE LA METODOLOGÍA

Los PEs involucrados deben ser actualizados de versión para que soporten IPV4/IPV6 dual-stack y 6VPE. La solución tomada para proveer transporte de servicios IPV6 es 6VPE; ésta deberá ser adoptada inmediatamente después de que se tenga clientes que requieran este servicio, y debe ser culminada de acuerdo a los requerimientos del mismo en capacidad.

Los nodos P aún son routers IPV4. Los túneles MPLS establecidos entre PEs y Ps usan los LDP IPV4 o RSVP TE. Los PEs y CEs intercambiarán información de ruteo a través de rutas estáticas IPV6. Por estas razones es muy importante establecer los LDP entre los routers que se realizarán la comunicación para 6VPE.

A diferencia de 6PE, los PEs VPN IPV6 usan RD y ERT (similar a las VPNs IPV4) para el intercambio de rutas. La etiqueta L1 transmitida entre los PEs es una etiqueta de la VPN que identifica a que CE se conecta.

Geográficamente, no existe un orden definido para realizar la migración, ya que la misma se realizará dependiendo de la necesidad de los clientes y la capacidad de soportar IPV6 de los mismos. Después se irán desplegando y configurando los routers PEs para que se soporten tráfico IPV6 sobre la red MPLS/IPV4 de la CNT EP.

En conclusión:

- Se usará RFC4659: BGP-MPLS IP Virtual Private Network (VPN) para IPv6 VPN.
- 6VPE simplemente añade el poder soportar IPV6 a la red actual MPLS/IPV4 ofrecida.
- Para usuarios finales: los servicios v6-VPN son los mismos que v4-VPN (QoS, hub and spoke, acceso a internet, etc.).

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO 3

LIBROS

[1] **Adeel**, Ahmed; **Salman**, Asadullah. *"Deploying IPv6 in Broadband Access Networks".* Septiembre 2011.

[2] **Youngsong**, Mun; Hyewon, **Keren** Lee; *"Understanding IPv6".* Julio. 2005.

PDF, RFC, PAPERS

[3] **ANÓNIMO.** *"Technical_White_Paper_for_IPv6_Dual_Stack_NAT_Solution_V1.0_20111130. pdf"*. Huawei Technologies. 2011.

[4] **ANÓNIMO.** "*Configuration Guide - IP Service(V100R006C00_02).pdf*". Huawei Technologies. 2011.

[5] **ANÓNIMO.** "*IPV6 Migration Planning*". OPNET Technologies Inc. 2009.

CAPÍTULO 4

ANÁLISIS DE REQUERIMIENTOS DE SOFTWARE Y HARDWARE PARA LA MIGRACIÓN Y ANÁLISIS DE COSTOS.

En este capítulo se analizará las versiones de Hardware y Software de los equipos de la red; así como los requerimientos para soportar la tecnología de migración escogida en el capítulo anterior. Al final se analizarán los costos necesarios.

4.1 VERSIONES DE LOS EQUIPOS

Se analizarán las versiones de los equipos dividiendo la red de acuerdo a las áreas de ubicación de los tres routers principales de Pichincha que son:

- IÑAQUITO – INQ.
- MARISCAL – MSC.
- QUITO CENTRO – QCN.

4.1.1 IÑAQUITO

Mediante el comando *show ver* se obtiene la información necesaria para el análisis de cada equipo de la red. La figura 4.1 muestra el resultado obtenido sobre el router UIOINQ01. En la tabla 4.1 se presenta un resumen de las diferentes versiones de los equipos pertenecientes a la zona de IÑAQUITO.

4.1.2 MARISCAL

En la tabla 4.2 se presenta un resumen de las diferentes versiones de los equipos pertenecientes a la zona de MARISCAL.

4.1.3 QUITO CENTRO

En la tabla 4.3 se presenta un resumen las diferentes versiones de los equipos pertenecientes a la zona de QUITO CENTRO.

```
"RP/0/RP1/CPU0:UIOINQP01#sh ver
Wed Mar 28 10:46:21.804 GMT
Cisco IOS XR Software, Version 3.8.2[00]
Copyright (c) 2009 by Cisco Systems, Inc.
ROM: System Bootstrap, Version 1.53(20090311:225342) [CRS-1
ROMMON],
UIOINQP01 uptime is 2 weeks, 3 days, 7 hours, 44 minutes
System image file is "bootflash:disk0/hfr-os-mbi-3.8.2/mbihfr-
rp.vm"
cisco CRS-8/S (7457) processor with 4194304K bytes of memory.
7457 processor at 1197Mhz, Revisión 1.2
2 Management Ethernet
82 GigabitEthernet
20 TenGigE
1019k bytes of non-volatile configuration memory.
57119M bytes of hard disk.
2049888k bytes of disk0: (Sector size 512 bytes).
Boot device on node 0/0/CPU0 is bootflash:
Package active on node 0/0/CPU0:
hfr-fpd, V 3.8.2[00], Cisco Systems, at disk0:hfr-fpd-3.8.2
Built on Wed Oct 28 02:32:12 GMT 2009"
```

Figura 4.1: Comando show ver sobre el router UIOINQP01

EQUIPO	IOS			ROM		HARDWARE	
	Software	***Versión***	***Release***	***Versión***	***Release***	***Chasis***	***Tarjeta de Línea / Procesador***
UIOINQP01	Cisco IOS XR	4.8.2[00]	-	1.53(20090311: 225342)	-	CRS-8/S	SIP-600
UIOCCLE01	c7600rsp72043_rp Software	12.2(33)SRD3	fc3	12.2(33)SRD3	fc3	CISCO7609-S	SIP-400
UIOCNDE01	c7600rsp72043_rp Software	12.2(33)SRD3	fc1	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400
UIOSGQE01	c7600rsp72043_rp Software	12.2(33)SRD3	fc3	12.2(33)SRD3	fc3	CISCO7609-S	SIP-400
UIOTMBE01	c7600s3223_rp Software	12.2(33)SRD3	fc3	12.2(33)SRD3	fc3	CISCO7609-S	SIP-400
UIOCTCE02	ME380x-UNIVERSALK9-M	15.1(2)EY	fc1	-	-	ME-3800X-24FS-M	FOC1549V3VE
UIOCCLE02	ME380x-UNIVERSALK9-M	15.1(2)EY	fc1	-	-	ME-3800X-24FS-M	-
UIOCRPE01	s6523_rp Software	12.2(33)SXI3	fc2	12.2(17r)SX3	fc1	ME-C6524GT-8S	revisión 1.3

Tabla 4.1 Versiones de software y hardware de equipos de zona IÑAQUITO. Pg. 1 de 3

EQUIPO	IOS			ROM		HARDWARE	
	Software	***Versión***	***Release***	***Versión***	***Release***	***Chasis***	***Tarjeta de Línea / Procesador***
UIOLBTE01	c7600s3223_rp Software	12.2(33)SRD3	fc3	12.2(17r)SX3	fc1	CISCO7606-S	SIP-400/ revisión 1.0
UIOCLME01	c7600s3223_rp Software	12.2(33)SRD3	fc3	12.2(17r)SX3	fc1	CISCO7606-S	SIP-400/ revisión 1.0
UIOCLDE01	c7600rsp72043_rp Software	12.2(33)SRD3	fc3	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0
UIOLLZE01	c7600rsp72043_rp Software	12.2(33)SRD3	fc3	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0
UIOMSRE01	c7600s3223_rp Software	12.2(33)SRD3	fc3	12.2(17r)SX3	fc1	CISCO7606-S	SIP-400/ revisión 1.0
UIOLFLE01	c7600s3223_rp Software	12.2(33)SRE3	fc1	12.2(17r)SX3	fc1	CISCO7606-S	SIP-400/ revisión 1.0
UIOINQM01	C3560 Software	12.2(37)SE	fc2	C3560	-	WS-C3560-48TS	revisión E0
UIOCRDE01	c7600s3223_rp Software	12.2(33)SRD3	fc3	12.2(17r)SX3	fc1	CISCO7606-S	SIP-400/ revisión 1.0

Tabla 4.1 Versiones de software y hardware de equipos de zona IÑAQUITO. Pg. 2 de 3

EQUIPO	IOS			ROM		HARDWARE	
	Software	***Versión***	***Release***	***Versión***	***Release***	***Chasis***	***Tarjeta de Línea / Procesador***
UIOLCLE01	c7600s3223_rp Software	12.2(33)SRD3	fc3	12.2(17r)SX3	fc1	CISCO7606-S	SIP-400/ revisión 1.0
UIOLLZE02	ME380x-UNIVERSALK9-M	15.1(2)EY	fc1	-	-	ME-3800X-24FS-M	revisión A0
UIOSNIE01	c7600s3223_rp Software	12.2(33)SRD3	fc3	12.2(17r)SX3	fc1	CISCO7606-S	SIP-400/ revisión 1.0
UIOLNVE01	c7600s3223_rp Software	12.2(33)SRD3	fc3	12.2(17r)SX3	fc1	CISCO7606-S	SIP-400/ revisión 1.0
UIOLNVE01	c7600s3223_rp Software	12.2(33)SRD3	fc3	12.2(17r)SX3	fc1	CISCO7606-S	SIP-400/ revisión 1.0

Tabla 4.1 Versiones de software y hardware de equipos de zona IÑAQUITO. Pg. 3 de 3

EQUIPO	IOS			ROM		HARDWARE	
	Software	***Versión***	***Release***	***Versión***	***Release***	***Chasis***	***Tarjeta de Línea / Procesador***
UIOMSCP01	Cisco IOS XR	4.8.2[00]	-	1.53(20090311: 225342)	-	CRS-8/S	revisión 1.2
UIOVLFE01	c7600rsp72043_rp Software	12.2(33)SRD 5	fc2	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0
UIOETTE01	c7600rsp72043_rp Software	12.2(33)SRC 1	fc1	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0
UIOSGQE01	c7600rsp72043_rp Software	12.2(33)SRD 3	fc3	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0
UIOLCSE01	c7600s3223_rp Software	12.2(33)SRD 3	fc3	12.2(17r)SX3	fc1	CISCO7606-S	SIP-400/ revisión 1.0
UIOLPZE01	c7600s3223_rp Software	12.2(33)SRD 3	fc3	12.2(17r)SX3	fc1	CISCO7606-S	SIP-400/ revisión 1.0
UIOMSCE03	s6523_rp Software	12.2(33)SXI3	fc2	12.2(17r)SX3	fc1	ME-C6524GT-8S	revisión 1.3
UIOCBYE01	c7600rsp72043_rp Software	12.2(33)SRD 3	fc3	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0

Tabla 4.2 Versiones de software y hardware de equipos de zona MARISCAL. Pg. 1 de 2

EQUIPO	IOS			ROM		HARDWARE	
	Software	***Versión***	***Release***	***Versión***	***Release***	***Chasis***	***Tarjeta de Línea / Procesador***
UIOLPZM02	ME340x-METROACCESSK9-M	12.2(55)SE3	fc1	12.2(44r)EY	fc1	ME-3400E-24TS-M	revisión E0
UIOEEPE01	c7600s3223_rp Software	12.2(33)SRD3	fc3	12.2(17r)SX3	fc1	CISCO7606-S	SIP-400/ revisión 1.0
UIOGMNE01	c7600s3223_rp Software	12.2(33)SRD3	fc3	12.2(33r)SRC3	fc1	CISCO7609-S	revisión 1.0

Tabla 4.2 Versiones de software y hardware de equipos de zona MARISCAL. Pg. 2 de 2

EQUIPO	IOS			ROM		HARDWARE	
	Software	***Versión***	***Chasis***	***Versión***	***Release***	***Chasis***	***Tarjeta de Línea / Procesador***
UIOQCNP01	Cisco IOS XR	4.6.1[00]	-	12.0(20060713:113510)	-	12810/PRP	revisión 1.2
UIOETTE01	c7600rsp72043_rp Software	12.2(33)SRC1	fc1	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0
UIOQCNE01	c7600rsp72043_rp Software	12.2(33)SRC1	fc1	12.2(33r)SRC3	fc1	CISCO7613	SIP-400, 200/ revisión 1.0
UIOVLFE01	c7600rsp72043_rp Software	12.2(33)SRD5	fc2	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0
UIOGJLE01	c7600rsp72043_rp Software	12.2(33)SRD3	fc3	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0
UIOPTDE01	c7600rsp72043_rp Software	12.2(33)SRD3	fc3	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0
UIOSGQE01	c7600rsp72043_rp Software	12.2(33)SRD3	fc3	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0
UIOMCHE01	c7600rsp72043_rp Software	12.2(33)SRD3	fc3	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0
UIOMNJE01	c7600rsp72043_rp Software	12.2(33)SRD3	fc3	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0

Tabla 4.3 Versiones de software y hardware de quipos zona QUITO CENTRO. Pg. 1 de 2

EQUIPO	IOS			ROM		HARDWARE	
	Software	***Versión***	***Chasis***	***Versión***	***Release***	***Chasis***	***Tarjeta de Línea / Procesador***
UIOQCHE01	c7600rsp72043_rp Software	12.2(33)SRD 3	fc3	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0
UIOQCNE02	s6523_rp	12.2(33)SXI3	fc2	12.2(17r)SX3	fc1	ME-C6524GT-8S	revisión 1.3
UIOETTE02	Cisco IOS XR	4.1.1[00]	-	20101118:025914	-	ASR9K	Revisión 2.2
UIOQCNM01	C3560	12.2(35)SE1	fc1	C3560	-	WS-C3560-48PS	revisión M0
UIOGMNE01	c7600s3223_rp Software	12.2(33)SRD 3	fc3	12.2(33r)SRC3	fc1	CISCO7609-S	SIP-400/ revisión 1.0

Tabla 4.3 Versiones de software y hardware de quipos zona QUITO CENTRO. Pg. 2 de 2

4.2 ANÁLISIS DE LAS VERSIONES DE SOFTWARE

4.2.1 SOFTWARE C7600

4.2.1.1 12.2(33)SRC [1]

Esta sección describe las principales funciones de software de esta versión. Como todas las versiones de software 12.2 SR o 12.2(33)SRC; este incluye múltiples áreas de tecnología como son: QoS, VPN capa 2, MPLS, VPN capa 3, direccionamiento y servicios IPV4 e IPv6, Ruteo IP, infraestructura y administración.

4.2.1.2 12.2(33)SRD3 [1]

Esta versión es la más actual y soporta las características necesarias para la implementación a realizarse.

Se describirá las principales funciones de Software de esta versión. Como todas las versiones, esta integra varias innovaciones en el IOS, las cuales abarcan varias áreas de tecnología como son: infraestructura flexible en ethernet, administración y QoS, funciones de IPV6.

4.2.1.3 12.2(33)SRD5[1]

No existen nuevas actualizaciones para la versión SRD5, la cual soporta los requerimientos de IPV6.

Las demás funcionalidades del IOS fueron analizadas en los ítems anteriores e incluyen: infraestructura flexible en ethernet, administración y QoS, funciones de capa 3 (IPV4/IPV6) y capa 2; que son las mismas que para SRD3.

Las versiones de software como 12.2(33)SXI3, 12.2(35)SE1, 15.1(2)EY soportan la funcionalidad de 6VPE necesaria para la migración.

4.2.2 SOFTWARE CISCO XR-12810 [2] [3]

No es necesario actualizar esta versión de software ya que la migración y el trabajo se realizan en los equipos de borde; para estos es transparente la comunicación de un cliente IPV6.

Es por este motivo que se escogió 6VPE ya que se tiene el menor impacto en la red. El software IOS de Cisco XR es un sistema operativo distribuido diseñado para la operación continua combinado con la flexibilidad y el alto rendimiento.

4.2.3 ANÁLISIS DEL SOFTWARE INSTALADO

La tabla 4.4 muestra el análisis de las versiones de Software de los equipos instalados en la MPLS de la CNT EP.

4.3 ANÁLISIS DEL HARDWARE DE LOS EQUIPOS

En el siguiente apartado se realizará un análisis del Hardware de los routers que se tiene en la red, chasis de los equipos, en base a las versiones de software que se tiene instalado.

4.3.1 HARDWARE C7600

4.3.1.1 VERSIÓN 12.2(33)SRC [1]

El router cisco de la serie 7600 con procesador 720 con 10 enlaces Gigabit Ethernet, está diseñado específicamente para entregar gran escalabilidad, alto rendimiento, y rápida convergencia; requeridos para los servicios quad-play.

IOS/Software	IPV6	QoS	MPLS/VPN	6VPE
12.2(33)SRC	Mejoras en DHCPv6 Relay IPv6 MIB – RFC 4292[31] y RFC 4293[32]. 	Soporte de Control de Admisión en Túnel para routers Cisco 7600 S. Qos por usuario, para routers Cisco 7600. Qos por Sesión, para routers Cisco 7600. "*Shaping*" y "*Queuing*" por sesión en LNS para routers Cisco 7600 . "*Traffic Shaping Overhead Accounting for ATM for Cisco 7600 Series Routers*".	Mejoras en el IOS Cisco para MPLS TE/RSVP. Mejoras en el IOS Cisco para MPLS LDP. Mejoras en el IOS Cisco para la administración de MPLS. Mejoras en el IOS Cisco para las VPN MPLS de capa 3.	Soporta 6VPE.
12.2(33)SRD3	Soporte para IPV6.	*Dual Rate* en *Service Instances.* IP SLAs Metro-Ethernet 2.0 (EVC) Soporte de ancho de banda restante. Listas de control de Acceso L2 en Instancias de Servicio (EVC).	L2TPv3 - Layer-2 *Tunneling Protocol Version* 3 en Cisco ES+. Administración de MPLS. VPN MPLS de capa 3.	Soporta 6VPE.
12.2(33)SRD5	Mejoras en DHCPv6 Relay IPv6 MIB – RFC 4292 y RFC 4293. Soporte para IPV6.	Dual Rate en Service Instances. IP SLAs Metro-Ethernet 2.0 (EVC) Soporte de ancho de banda restante. Listas de control de Acceso L2 en Instancias de Servicio (EVC).	L2TPv3 - Layer-2 Tunneling Protocol Version 3 en Cisco ES+. Administración de MPLS. VPN MPLS de capa 3.	Soporta 6VPE.

Tabla 4.4 Análisis de las versiones de Software de los equipos instalados en la MPLS de la CNT EP. Pg. 1 de 2

[31] IP MIB
[32] MIB de reenvío IP

IOS/Software	IPV6	QoS	MPLS/VPN	6VPE
XR-12810	Soporta un gran rango de servicios y protocolos de ruteo IPV4 e IPV6 como BGP, RIPv2, RPL (Routing Policy Language), HSRP (Hot Standby Router Protocol) y VRRP (Virtual Router Redundancy Protocol Features).	Soporta mecanismos de QoS incluyendo “policing, marking, queuing, random y hard traffic dropping, y shaping ”, este IOS de Cisco también soporta QoS modular (MQC). Este simplifica la configuración de varias funcionalidades de QoS en varias plataformas Cisco.	Soporta protocolos MPLS, incluyendo TE (Ingeniería de tráfico), RSVP (Resource reservation protocol), LDP (Label Distribution Protocol), VPLS (Virtual Private LAN Service), y L3VPN (Layer 3 VPN). El router cisco CRS-1 soporta también L2VPN.	NA

Tabla 4.4 Análisis de las versiones de Software de los equipos instalados en la MPLS de la CNT EP. Pg. 2 de 2

4.3.1.2 VERSIÓN 12.2(33)SRD [1]

El hardware en esta versión utiliza un diseño extensible priorizado para voz, datos, y servicios inalámbricos móviles. Este está diseñado para interfaces con bajos requerimientos. Éstas pertenecen a las series ES+.

El diseño maximiza las opciones de conectividad y ofrece un servicio superior a través de interfaces programables.

4.3.2 HARDWARE CISCO XR-12810

En este apartado se analizarán los tres routers P[33] de la red.

4.3.2.1 ROUTER UIOQCNP01

Para este equipo se cuenta con las características de hardware mostradas en la figura 4.2 que se obtienen al ejecutar el comando *show versión*.

```
"cisco 12810/PRP (7457) processor with 2097152K bytes of memory.
7457 processor at 1266Mhz, Revisión 1.2
5 Cisco 12000 Series SPA Interface Processor-601/501/401
2 Cisco 12000 Series Performance Route Processors
3 TenGigabitEthernet/IEEE 802.3 interface(s)
20 PLIM QoS controller(s)
6 Ethernet/IEEE 802.3 interface(s)
12 GigabitEthernet/IEEE 802.3 interface(s)
1018k bytes of non-volatile configuration memory.
1998M bytes of compact flash card.
2049920k bytes of ATA PCMCIA card at disk 0 (Sector size 512
bytes).
65536k bytes of Flash internal SIMM (Sector size 256k)."
```

Figura 4.2: Comando show version sobre el router UIOQCNP01

4.3.2.2 ROUTER UIOMSCP01

Este equipo es un P de la red MPLS, perteneciente a MARISCAL y sus características de hardware se observan en la figura 4.3.

[33] Router del core MPLS de la CNT EP de Pichincha.

```
"cisco CRS-8/S (7457) processor with 4194304K bytes of memory.
7457 processor at 1197Mhz, Revisión 1.2
2 Management Ethernet
82 GigabitEthernet
12 TenGigE
1019k bytes of non-volatile configuration memory.
57119M bytes of hard disk.
2049888k bytes of disk0: (Sector size 512 bytes)."
```

Figura 4.3: Comando show ver sobre el router UIOMSCP01

4.3.2.3 UIOINQP01

Este equipo es un P de la red MPLS, perteneciente a IÑAQUITO y sus características de hardware se presentan en la figura 4.4:

```
"cisco CRS-8/S (7457) processor with 4194304K bytes of memory.
7457 processor at 1197Mhz, Revisión 1.2
2 Management Ethernet
82 GigabitEthernet
20 TenGigE
1019k bytes of non-volatile configuration memory.
57119M bytes of hard disk.
2049888k bytes of disk0: (Sector size 512 bytes)."
```

Figura 4.4: Comando show ver sobre el router UIOINQP01

4.3.3 ANÁLISIS DEL HARDWARE INSTALADO

La figura 4.5 muestra un Análisis de las versiones de Hardware de los equipos MPLS instalados en la CNT EP.

EQUIPO	CAPACIDAD	CPU/MEMORIA	PUERTOS
12.2(33)SRC/Cisco 7603-S, 7604, 7606-S, 7609, 7609-S.	720 Gbps de fábrica. Reenvío en capa 2 con una taza de 30 millones de paquetes por segundo. Provee una capacidad de 40 Gbps por slot. Permite expansión por slots para incremento de densidad de puertos.	Tiempos de convergencia rápidos IGMP mejorado Tiempos de boot-up mejorados Mejoras en las tasas de aprendizaje en DHCP, LDP, sesiones IP, e ingeniería de tráfico.	Se ofrece opciones de 2x10Gigabit Ethernet y 3xGigabit Ethernet en RSP. Las interfaces pueden ser configuradas en modo simple o modo mixto.
12.2(33)SRD/ Cisco 7603-S, 7604, 7606, 7606-S, 7609, 7609-S, y 7613	Se ofrece 40 Gbps por slot. Opción de encolado de 256 Kbps.	Tiempos de convergencia rápidos.	4x10GE, 40xGE, 2x10GE, y 20xGE.
XR-12810/ UIOQCNP01	Procesador de 40 Gbps de reenvío.	2097152K bytes / 1266MHz.	3 TenGigabitEthernet/IEEE 802.3. 6 Ethernet/IEEE 802.3. 12 GigabitEthernet/IEEE 802.3.
XR-12810/ UIOMSCP01	Procesador de 40 Gbps de reenvío.	4194304K bytes/1197MHz.	82 GigabitEthernet. 12 TenGigaEthernet.
XR-12810/ UIOINQP01	Procesador de 40G de reenvío.	4194304K/1197MHz.	82 GigabitEthernet. 20 TenGigaEthernet.

Tabla 4.5 Análisis de las versiones de Hardware de los equipos instalados en la MPLS de la CNT EP.

4.4 ANÁLISIS DE REQUERIMIENTOS

4.4.1 SOFTWARE

Después del análisis realizado en la tabla 4.4, se ha determinado que no se requiere hacer ningún cambio en especial para el método de migración que se va a utilizar. Esto ya que soportan IPV6 y 6VPE.

A continuación se muestra a detalle el soporte de CISCO para 6VPE.

IPv6 VPN Router PE (6VPE) [1]

La implementación CISCO de VPN IPV6 en PEs sobre MPLS es referido como 6VPE y permite la conexión de sitios IPV6 a través de una VPN que se comunica sobre un core MPLS IPV4 usando MPLS LSP (Label Switched Paths).

Cisco 6VPE fue inicialmente introducido en la versión 12.2(33)SRB para los routers CISCO 7600.

Esta característica de los routers Cisco 7600 depende de las extensiones BGP en la red IPV4. Además los routers de borde (PEs) deben tener habilitado IPV6 las VPNs tanto de IPV4 como de IPV6 deben poder coexistir simultáneamente con la misma cobertura y políticas. Esta implementación también debe soportar VRF-lite IPV6.

Para los routers de core, no se requiere ningún requisito a más del que actualmente se mantiene.

4.4.2 HARDWARE

Como se muestra en la tabla 4.5 la capacidad actual de las versiones de hardware de los equipos de la CNT EP de Pichincha están lo suficientemente equipadas para soportar 6VPE.

4.5 DIMENSIONAMIENTO DE RED

Se analizaron los routers PE que están conectados directamente a los routers P, estos centralizan el tráfico de varios clientes/empresas. Se tomó estadísticas en la interfaz que conecta al router P. En la figura 4.5 se muestra uno de los puertos donde se tomó estadísticas de tráfico.

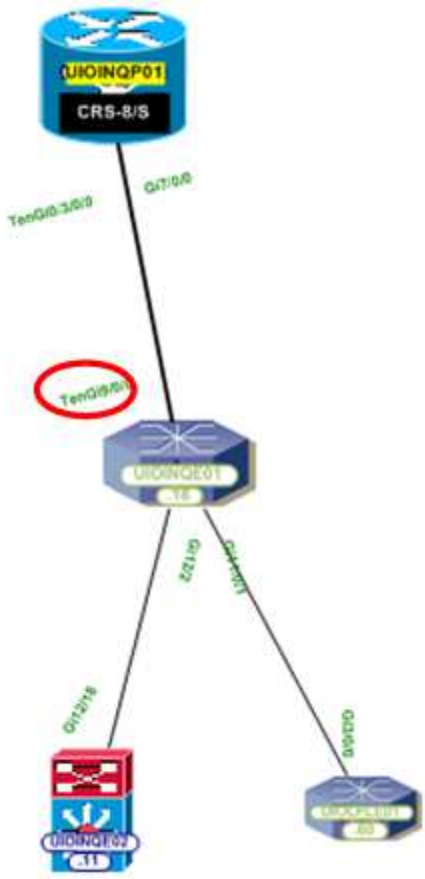


Figura 4.5: Diagrama lógico de los routers PE de IÑAQUITO

Estos routers colectan el tráfico de equipos conectados en clientes o de varios clientes a la vez. La figura 4.6 muestra la estadística de tráfico real para el router UIOVLFE0, este tiene varias conexiones debido a la redundancia, se trabajará sobre la conexión con mayor tráfico.

Sobre este router se configuró un cliente IPV6, por lo que se procederá a realizar el dimensionamiento en el peor de los casos que sería que todos los actuales clientes migren a IPV6.

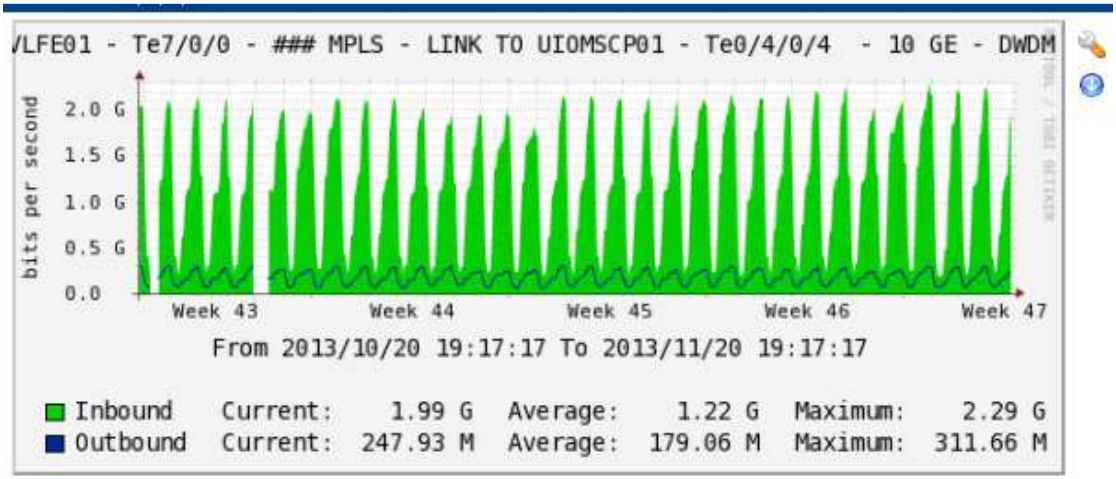


Figura 4.6: Estadística de tráfico entre el PE UIOVLFE01 y el P UIOMSCP01

Actualmente se tiene un tráfico promedio entrante de 1.22 Gbps y tráfico promedio saliente de 179.06 Mbps, estos están sobre una interfaz 10 Giga Ethernet. Se procederá a realizar el cálculo con tráfico IPV6:

Tráfico total en la interfaz = tráfico entrante + tráfico saliente
Tráfico total en la interfaz = 1220 + 179.06 = 1399.06 Mbps

Tramas Ethernet en la interfaz = Tráfico total en la interfaz / 1500 x 8 bits
Tramas Ethernet en la interfaz = 1399060 bits / 12000 bits = 116.6 tramas

Se considerará el mismo número de tramas pero con tráfico IPV6, que es el escenario que se ha planteado. La cabecera de IPV6 se incrementa en 20 bytes, para realizar el cálculo del tráfico extra se tiene:

Tramas generadas por 20 bytes extras = 20 bytes x 116.6 = 2332 bytes
Tráfico total para IPV6 = 2332x8 bits + 1399060 bits = 1417716 bps

Se considera el mismo tipo de tráfico y que todos los clientes migren a IPV6, por ende el mismo número de tramas serán usadas con la diferencia que la cabecera IPV6 agrega 20 bytes adicionales por lo que se procede a multiplicar el número de tramas por los 20 bytes extras en la cabecera. El tráfico que aumenta no afecta a la interfaz de conexión con los routers P ya que la misma es Ten Giga Ethernet.

Ahora se procederá a realizar el mismo análisis para diferentes routers PE conectados a los P de Pichincha, después se resumirá los diferentes valores en una tabla. La figura 4.7 muestra el tráfico entre el PE UIOQCNE01 y el P UIOQCNP01.

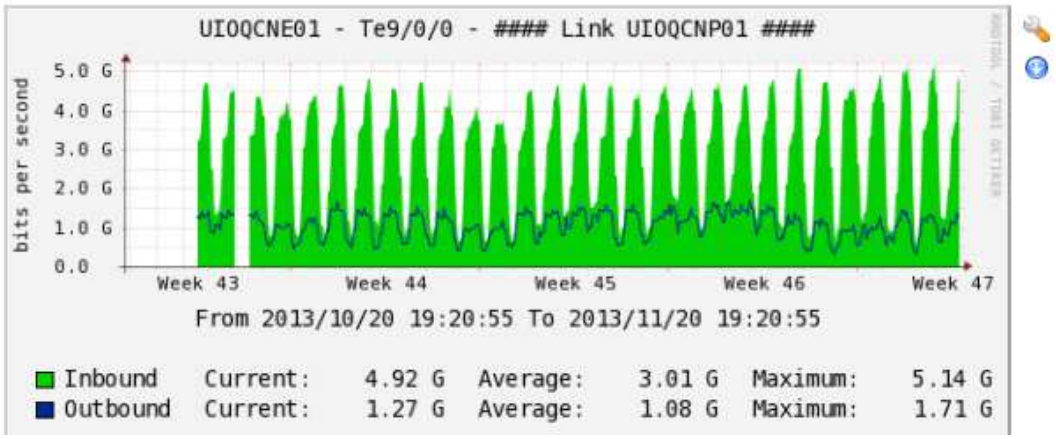


Figura 4.7: Estadística de tráfico entre el PE UIOQCNE01 y el P UIOQCNP01

En este se tiene un tráfico promedio de 3.01 Gbps de entrada y 1.08 Gbps de salida. Lo que nos da un tráfico total de 4.09 Gbps. La figura 4.8 muestra el tráfico entre el PE UIOETTE01 y el P UIOQCNP01.

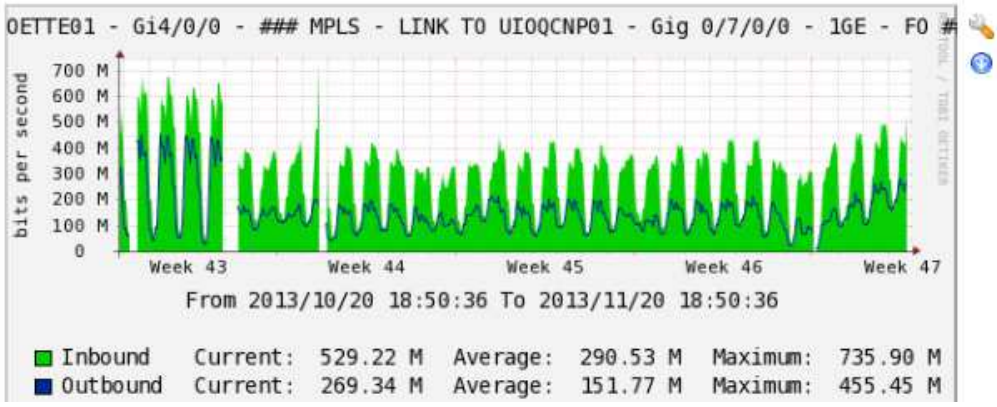


Figura 4.8: Estadística de tráfico entre el PE UIOETTE01 y el P UIOQCNP01

En este se tiene un tráfico promedio de 290.53 Mbps de entrada y 151.77 Mbps de salida. Lo que nos da un tráfico total de 442.30 Mbps. La tabla 4.6 muestra el aumento de tráfico en cada uno de los routers involucrados:

Interfaz	Tráfico total en la interfaz	Tramas Ethernet en la interfaz	Tramas por 20 bytes extras	Tráfico total para IPV6	Porcentaje de tráfico incrementado
UIOVLFE01 - UIOMSCP01(10 Giga)	1399.06 Mbps	116.6	2332 bytes	1417.7 Mbps	1.32%
UIOQCNE01 - UIOQCNP01(10 Giga)	4.09 Gbps	340.8	6817 bytes	4144.53 Mbps	1.32%
UIOETTE01 - UIOQCNP01(Giga)	442.30 Mbps	36.9	737 bytes	448.19 Mbps	1.32%
PROMEDIO	1977.12 Mbps	164.76	3295.2 bytes	2003.48 Mbps	1.32 %

Tabla 4.6 Aumento de tráfico

En conclusión el tráfico incrementado en cada una de las interfaces existentes no se incrementa lo suficiente como para exceder la capacidad de las mismas.

4.6 ANÁLISIS DE COSTOS

El costo es el dinero que se debe desembolsar para adquirir un bien, producto o servicio. Los costos de esta transición valoran elementos como lo son: hardware, software, y costos operacionales (recursos humanos, capacitación, logística, horas extras, etc.).

4.6.1 DETALLE DE COSTOS

Se analizarán los costos que se generarán para poder realizar esta implementación.

4.6.1.1 Costos de Hardware y Software

Como se analizó previamente, para hardware y software no se requiere realizar ningún cambio, ya que el estado actual de los equipos de la red soportan la funcionalidad 6VPE, por ende IPV6.
Por lo tanto los servicios de costos operacionales son los que demandarán gastos. En la tabla 4.7 se muestra los costos necesarios de hardware y software.

ITEM	Descripción	Valor unit.	Cantidad	Valor Total
1	Hardware (Tarjetas adicionales, ampliación de memoria, etc.)	0	0	0
2	Software (Actualización de Software)	0	0	0

Tabla 4.7 Tabla de costos de Hardware y Software

4.6.1.2 Costos Operacionales

"Se llama Costos operacionales al dinero que una empresa o una organización debe desembolsar en concepto del desarrollo de las diferentes actividades que despliega"[34]. Dentro de estos costos se incorpora a los recursos humanos y capacitación, ya que las personas encargadas de esta implementación serán quienes den soporte después de la configuración y quienes capaciten al personal encargado de monitorear la red.

Para el análisis del costo de recursos humanos se toma en cuenta el sueldo de un Ingeniero MPLS de la CNT, que es el encargado de realizar configuraciones sobre la red. Cabe mencionar que el trabajo de este Ingeniero no se limitará a los trabajos sobre IPV6, sino cualquier trabajo que se tenga que realizar sobre la red MPLS de la CNT EP. También hay trabajos que se deberán realizar en ventanas de mantenimiento (periodos de tiempo asignados para trabajos que pueden

[34] http://www.scribd.com/doc/95491769/COSTOS-OPERACIONALES

ocasionar impacto en la red), esto implica gastos en horas extras. En la tabla 4.8 se muestra el desglose de estos Costos.

Se tiene un Costo de $3186 USD por mes. Comparando con la tabla de costos de CNT, este cobra aproximadamente $5040 USD[35] mensuales para un enlace interurbano[36] de 150 Mbps. Por lo tanto se concluye que para enlaces de datos superiores a 100 Mbps el proyecto es viable.

No	Descripción	Cantidad	Sueldo	Total (USD)
1	Ingeniero MPLS de CNT	2	$1980 USD/mes[37]	$3960
2	Horas extras	16	$13 USD/hora	$208
			TOTAL	$3186

Tabla 4.7 Tabla de Costos Operacionales

Como se mencionó antes el trabajo de los Ingenieros no es limitado a IPV6 sino al mantenimiento de toda la MPLS, por lo tanto los costos operacionales no solo se aplican para este proyecto. En la figura 4.9 se muestra la tarifa del enlace de datos interurbanos de CNT, mostrado en la guía comercial de productos de Mayo de 2013.

TARIFAS									
2TXDAT PUNTO INTERURBANO			2TXDAT MEGA ADICIONAL		INTERURBANO PUNTO ADICIONAL			2TXDAT MEGA ADICIONAL	
PLAN TX LOCAL (KBPS)	INSCRIPCIÓN (USD)	TARIFA MENSUAL (USD)	PLAN ACTUAL (Mbps)	TARIFA MENSUAL TECHO (USD)	PLAN TX LOCAL (KBPS)	INSCRIPCIÓN (USD)	TARIFA MENSUAL (USD)	PLAN ACTUAL (Mbps)	TARIFA MENSUAL TECHO (USD)
128	350,00	65,00	< 10 Mbps	115,00	128	350,00	65,00	< 10 Mbps	115,00
256	350,00	90,00	10-34	94,00	256	350,00	90,00	10-34	94,00
512	350,00	130,00	34-45	58,82	512	350,00	130,00	34-45	58,82
1000	350,00	230,00	45-100	67,33	1000	350,00	230,00	45-100	67,33
2000	350,00	332,00	100-150	50,40	2000	350,00	332,00	100-150	50,40
3000	350,00	369,00	>150	50,00	3000	350,00	369,00	>150	50,00
4000	400,00	405,00	Las capacidades no indicadas en los planes deben ser calculadas sumando el valor del plan elegido más el valor que resulte de la cantidad de megas adicionales requeridos dentro del rango de cálculo, por ejemplo: el cálculo de la tarifa de un plan de 15Mbps deberá tomar en cuenta el valor del plan de 10Mbps y sumarle el resultado de 5 por el valor por mega adicional del rango de 10-34Mbps		4000	400,00	405,00	Las capacidades no indicadas en los planes deben ser calculadas sumando el valor del plan elegido más el valor que resulte de la cantidad de megas adicionales requeridos dentro del rango de cálculo, por ejemplo: el cálculo de la tarifa de un plan de 15Mbps deberá tomar en cuenta el valor del plan de 10Mbps y sumarle el resultado de 5 por el valor por mega adicional del rango de 10-34Mbps	
5000	450,00	575,00			5000	450,00	575,00		
10000	500,00	940,00			10000	500,00	940,00		
34000	600,00	2.000,00			34000	600,00	2.000,00		
45000	600,00	3.030,00			45000	600,00	3.030,00		
100000	650,00	5.040,00			100000	650,00	5.040,00		
150000	700,00	9.360,00			150000	700,00	9.360,00		
1000000	1.000,00	48.960,00			1000000	1.000,00	48.960,00		

Figura 4.9: Tarifa de datos interurbanos

[35] Valor consultado a Mayo de 2013.
[36] Transmisión entre dos puntos ubicados fuera de una misma provincia.
[37] Sueldo de un Ingeniero MPLS consultado, con corte al 16 de Abril de 2013.

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO 4

PDF, RFC, PAPERS

[1] **ANÓNIMO**. *"Cisco IOS Software Release 12.2SR New Features and Hardware Support".* Cisco System. 2010.

[2] **ANÓNIMO.** "*Release Notes for Cisco IOS XR Software Release 3.8.2*" Cisco System. 2012.
URL:http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.8.2/general/release/notes/reln_382.pdf
Consultado el 17 de Abril de 2013

[3] **ANÓNIMO.** "*Release Notes for Cisco IOS XR Software Release 3.6.1"*
URL:
http://www.cisco.com/en/US/docs/ios_xr_sw/iosxr_r3.6/general/release/notes/reln_361.html
Consultado el 17 de Abril de 2013

CAPÍTULO 5

ANÁLISIS DE RESULTADOS

En este capítulo se analizarán las opciones de simuladores de red disponibles y que se adapten al desarrollo del presente trabajo, de tal forma que permitan simular con la mayor exactitud la red MPLS de la CNT EP de Pichincha; también se analizará los resultados obtenidos en la simulación de la red MPLS tanto en IPV4 como IPV6, así como las ventajas y desventajas de la migración y su impacto en la Calidad de servicio (QoS).

5.1 INTRODUCCIÓN [1] [2] [3] [4]

Una simulación es [4], una combinación de arte y ciencia. La simulación puede ser imaginada como el flujo de procesos de una entidad de red (nodos, paquetes, etc.), así como estas entidades se mueven a través del sistema, también interactúan con otros sistemas, se unen a actividades, causan cambios de estado del sistema y dejan los procesos.

5.2 SIMULADORES DE RED [1] [3] [4]

Los simuladores[3] emplean la simulación como una técnica que imita el comportamiento de un sistema del mundo real conforme evoluciona en el tiempo. Por lo tanto, permite analizar y observar características, sin la necesidad de acudir al sistema real.

[1]Los simuladores de red intentan modelar las redes del mundo real. La idea es que si un sistema puede ser modelado, sus características pueden ser cambiadas y analizadas. Como el proceso de la modificación de un modelo es relativamente barato, entonces una variedad de escenarios pueden ser analizados a costos bajos.

[3]Actualmente existen varios tipos de simuladores de red disponibles, muchos de libre distribución y otros bajo licencia. A continuación se realizará un análisis de los principales simuladores de red que soporten los protocolos necesarios para la simulación de la red MPLS de la CNT EP Pichincha; y se definirá cual es el que mejor se adapta para el trabajo a realizarse en el presente proyecto.

5.2.1 SIMULADORES DE LIBRE DISTRIBUCIÓN

Hay una gran variedad de estos simuladores entre los que se encuentran:

5.2.1.1 GNS3 (Graphical Network Simulator) [7]

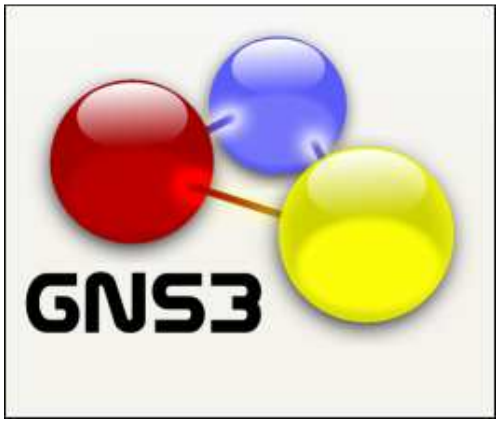


Figura 5.1: GNS3

GNS3 es un simulador gráfico que permite simular redes complejas. Para permitir una simulación completa, GNS3 usa Dynamips, un programa de core que permite la emulación de un IOS de Cisco. GNS3 también usa dynagen que es el generador de las configuraciones de las redes a simular. GNS3 es una herramienta complementaria excelente para simular laboratorios reales[38].

Ventajas:

- Con GNS3 se ejecuta el actual y real IOS de Cisco, y se puede observar exactamente lo que el IOS genera además tiene acceso a todos los

[38] http://www.gns3.net/hardware-emulated/

comandos y parámetros soportados por el IOS en los distintos modelos reales de routers.

- Mediante el GNS3 se pueden hacer todas las pruebas necesarias previas a la implantación real.
- Es de libre distribución.
- Soporta captura de paquetes mediante wireshark.
- No está limitado al desarrollador de software.

Desventajas:

- Depende de la capacidad de memoria RAM del CPU donde está ejecutándose el programa.
- Alto consumo de recursos de CPU y RAM en redes complejas.
- Solo se puede emular hasta la serie Cisco 7200.

5.2.1.2 NS-3[8]

Figura 5.2: NS-3

Este es un simulador de eventos discretos basado en C++ para generar los modelos de simulación. En esta versión las simulaciones de red pueden ser simuladas en C++ puro, y opcionalmente se puede usar phyton para ciertas partes de la simulación.

Ventajas:

- Es software de libre distribución.
- Permite simular una gran variedad de redes IP.

Desventajas:

- Se necesita crear la red desde su programación si se quiere simular algo en específico como la red MPLS de la CNT EP.
- No soporta todos los protocolos requeridos para simular la red MPLS. Si se los desea incluir habría que realizar la programación de cada protocolo necesario.
- No es capaz de emular un router.

5.2.1.3 OMNET++[8]

Este no es un simulador de red por definición, sino un simulador de propósito general basado en eventos discretos. Sin embargo, mediante su paquete INET (Integrated Network Enhanced Telemetry), ofrece una amplia colección de modelos de protocolos de internet. La figura 5.3 muestra la interfaz de usuario de OMNET++.

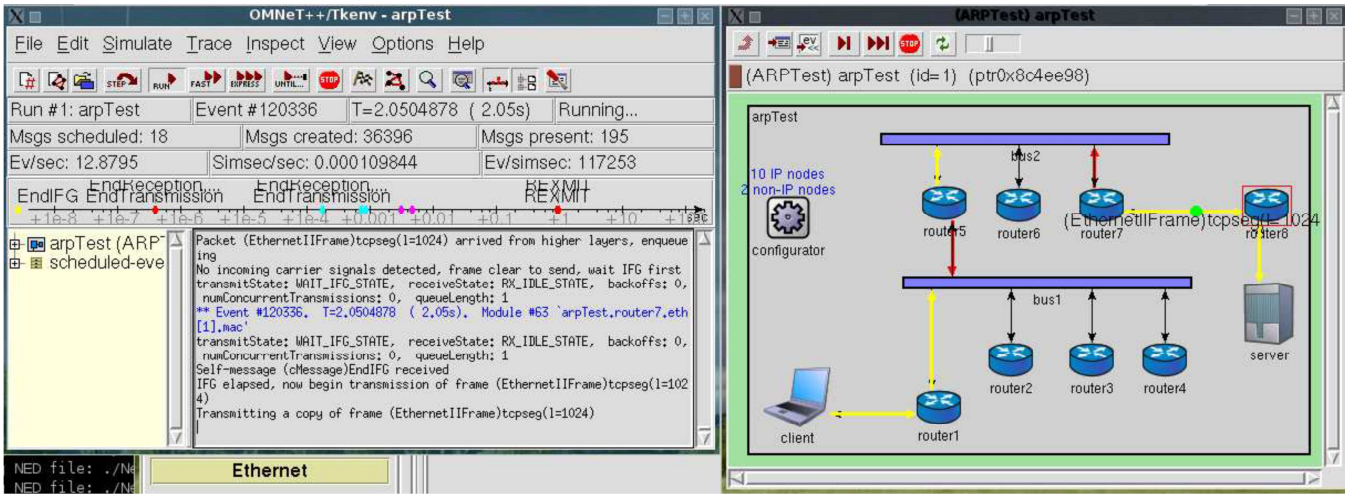


Figura 5.3: Interfaz gráfica OMNET TKenv

Ventajas:

- Mediante el uso de C++ se puede crear módulos que se adapten a nuestra simulación.
- Licencia pública académica.

- Simulaciones más rápidas que OPNET.
- Mayor flexibilidad el momento de crear módulos.

Desventajas:

- Menor grado de realismo que OPNET.
- Pocos modelos de equipos y enlaces.

5.2.2 SIMULADORES COMERCIALES

5.2.1.1 Packet Tracer[4][6]

Packet Tracer es una herramienta de simulación, orientada para alumnos y profesores de Cisco CNNA. Sin embargo Packet Tracer no es un sustituto de un equipo real, pero permite a los estudiantes practicar usando una interfaz en línea de un IOS de Cisco, solucionar problemas de red.

Ventajas

- Soporta todos los protocolos estudiados en el CNNA.
- Interfaz amigable con el usuario
- Permite ver el desarrollo por capaz, del proceso de transmisión.

Desventajas

- Solo permite modelos reales en términos de filtrado y retransmisión de paquetes.
- Su enfoque es meramente pedagógico.
- Solo soporta las tecnologías que el diseñador decida involucrar en el programa.
- No soporta MPLS (Indispensable para el proyecto).

5.2.1.2 OPNET Modeler[3][10]

Figura 5.4: OPNET

Opnet es un lenguaje de simulación orientado a las comunicaciones. Proporciona acceso directo al código fuente, siendo esto una gran ventaja para los nuevos programadores que usen OPNET.

Ventajas:

- Tiene un realismo alto.
- Abarca miles de modelos y enlaces para poder generar nuestra topología.
- Extensa biblioteca de modelos y protocolos.

Desventajas:

- Licencia muy costosa. Se solicitó una cotización a OPNET USA.
- La versión disponible no puede generar nodos con ISIS ni MPLS, es necesario hacer un análisis equipo por equipo para definir estos parámetros.
- Simulación lenta.
- No hace un análisis detallado a nivel de paquetes.

5.3 ELECCIÓN DEL SIMULADOR

Se analizará cada uno de los simuladores indicando las principales características de los mismos y se concluirá cuál es el más óptimo para el proyecto. La tabla 5.1 muestra las principales características de los simuladores analizados.

Después de haber analizado uno por uno los diferentes tipos de simuladores en la tabla 5.1, se tiene dos simuladores que son los más óptimos y que más se ajustan a los requerimientos del proyecto y que se describen a continuación.

SIMULADOR	LICENCIA	EQUIPOS SOPORTADOS	PROTOCOLOS SOPORTADOS	OBSERVACIONES
GNS3	Gratis	1710, 1720, 1721, 1750 1751, 1760 2610, 2611, 2610XM, 2620, 2620XM, 2650XM, 2611XM, 2621, 2621XM, 2651XM 3620, 3640, 3660 2691, 3725, 3745 7206	Todos los soportados por el IOS cargado.	Soporta Wireshark, más adecuado para la simulación.
NS-3	Gratis	Modelos para los elementos que conforman una red de computadoras, por ejemplo, dispositivos de red que representan los dispositivos físicos que conectan un nodo con el canal de comunicación.	TCP y UDP, FTP, Telnet, Web, CBR y VBR.	Trabaja sobre C++, no soporta IPV6.
OMNET++	Gratis	NA	Trabaja a nivel de módulos.	Mediante el uso de C++ se puede crear módulos que se adapten a nuestra simulación.

Tabla 5.1: Principales características de los simuladores analizados Pg. 1 de 2

SIMULADOR	LICENCIA	EQUIPOS SOPORTADOS	PROTOCOLOS SOPORTADOS	OBSERVACIONES
Packet Tracer	Pagado	Routers y switches con un limitado número de comandos.	HTTP, Telnet, SSH, TFTP, DHCP, DNS; TCP y UDP; IPv4, IPv6, ICMPv4, ICMPv6; RIP, EIGRP, multi-area OSPF, ruteo estático, y redistribución de rutas; Ethernet/802.3, 802.11, HDLC, Frame Relay, y PPP; ARP, CDP, STP, RSTP, 802.1q, VTP, DTP, y PAgP.	No soporta MPLS.
OPNET	Pagado	Soporte de casi todos los Routers y Switches CISCO.	VoIP, TCP, OSPFv3, MPLS, IPV6, Otros.	Licencia demasiado costosa, sin ésta no soporta ISIS y MPLS, necesarios para el proyecto.

Tabla 5.1: Principales características de los simuladores analizados Pg. 2 de 2

5.3.1 OPNET

Permite recrear cada uno de los nodos de la red MPLS de la CNT EP. Mediante el uso de la herramienta *"Device configuration Imports (DCI)",* esta permite generar modelos de red importando datos de configuración de los diferentes modelos de red. DCI usa los datos de los archivos de configuración de los equipos, para configurar los atributos de OPNET que controlarán las diferentes tecnologías y protocolos; los archivos de configuración que se necesitan son las salidas de los comandos mostrados en la tabla 5.2 y colocados en un archivo .txt, de cada uno de los nodos a simular.

	COMANDO	Observación
1	show running-config	Requerido para routers Cisco
	show config all	Requerido para Cisco Catalyst Switches
2	show versión	Recomendado
3	show cdp neighbors detail	Requerido para switches Cisco; Opcional para routers Cisco
4	show interfaces	Opcional, pero recomendado para routers y Switches
5	show vlan	Requerido para switches Cisco
	show vtp status	Requerido para switches Cisco
	show standby	Opcional
6	show mpls traffic-eng tunnels	Opcional pero recomendado si se usa la opción auto-bandwidth
7	show ip route	Requerido para crear las tablas de ruteo
	show ip route vrf	Requerido para crear las tablas VRF de reenvío

Tabla 5.2: Comandos para DCI

OPNET generará un nodo por cada archivo de configuración donde se tenga toda la información de los comandos listados en la Tabla 5.2. El principal problema que se genera es que se necesita licencias adicionales para poder simular MPLS e ISIS. En la figura 5.5 se observa el error que se genera al no tener las licencias necesarias.

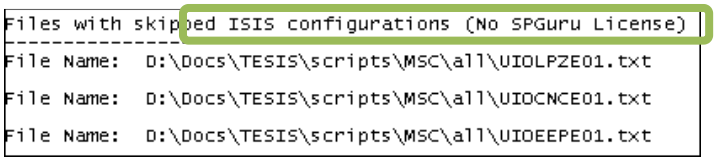


Figura 5.5: Error generado por falta de licencia para ISIS

En este caso se requiere instalar licencia de SPGuru Edition y constituye el principal inconveniente para usar este simulador en el proyecto. En la figura 5.6 se muestra la red que generó OPNET después de leer los archivos .txt requeridos pero con las limitaciones de licencias.

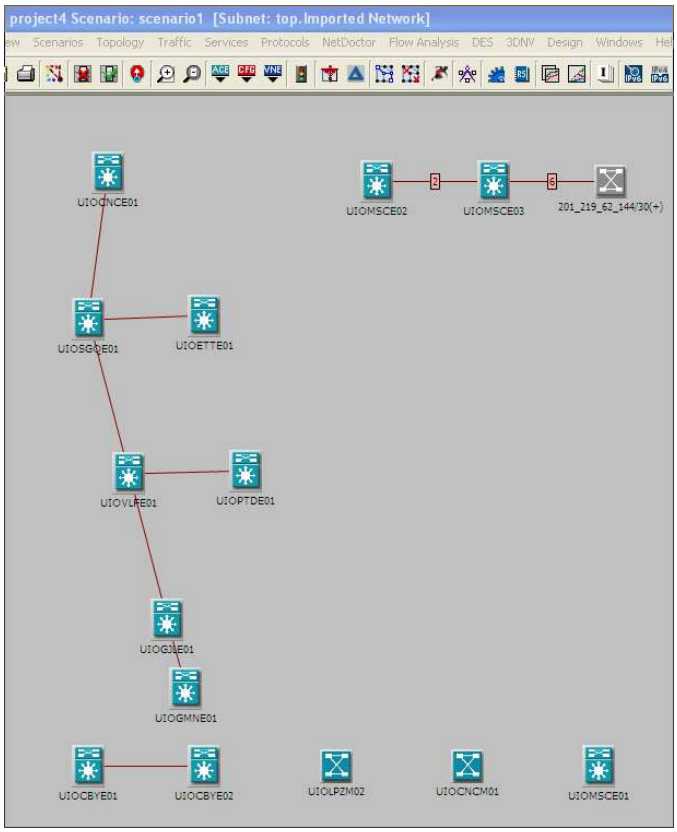


Figura 5.6: Ejemplo de la red que generada OPNET

Después de revisar todos los parámetros de este simulador, se concluye que **NO** es conveniente usar este software para realizar la simulación de la red MPLS de la CNT EP de Pichincha, por las siguientes razones:

- Las licencias son muy costosas.
- Para un proyecto de simulación el costo a pagar es demasiado elevado.

5.3.2 GNS3

El simulador que permite emular los IOS de Cisco y se instaló sin problemas. La primera limitante que se tuvo, es que GNS3 solo soporta hasta el modelo Cisco C7200, y en la red de la CNT en su mayoría son routers C7600, además de los routers de core que son XR y CRS-8/S.

Para solucionar este inconveniente se adecuaron los scripts de los otros equipos[39] a los C7200 y se incluyeron todas las características requeridas en este proyecto como son: MPLS, QoS, IPV6, ISIS, ACLs, etc. Los scripts originales se encuentran en el ANEXO 1 y CD adjunto.

La segunda limitante fue el elevado uso del CPU, ya que GNS3 usa muchos recursos de la PC y la capacidad de simulación se limita al procesamiento de la PC sobre la que corre GNS3; para esto se decidió usar tres computadoras y que cada una simule un router P con sus respectivos PEs y CEs. En la figura 5.7 se muestra el ambiente de trabajo para el P de Mariscal en donde la nube representa la conexión con otra computadora a través del puerto Ethernet.

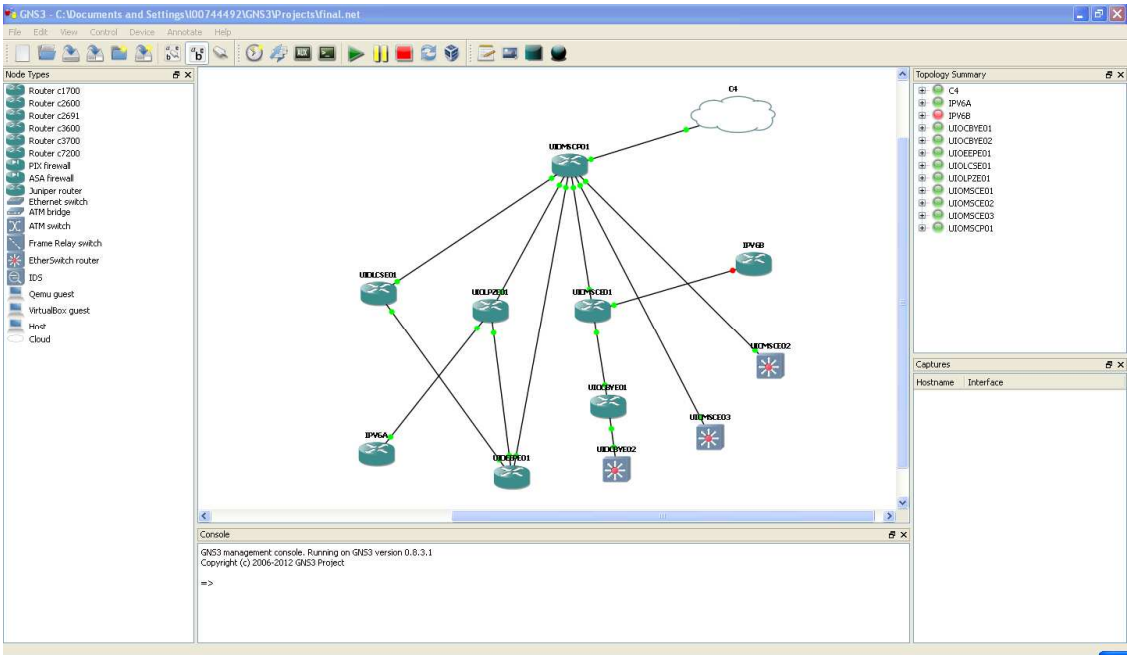


Figura 5.7: Simulación de los nodos conectados al P de Mariscal

[39] Estos scripts se encuentran detallados en el ANEXO 1.

El problema con este tipo de configuración es que al conectar las tres computadoras los routers P no aprenden las rutas mediante ISIS, las tarjetas Ethernet de las computadoras no permitían el paso de tráfico multicast y se requiere configurar rutas estáticas en los equipos P para que estos se puedan comunicar. Para solventar este inconveniente se realizó las pruebas en un servidor prototipo de laboratorio. Este servidor tiene la capacidad suficiente para simular toda la red en un solo ambiente de trabajo. En la figura 5.8 se muestra las características de este servidor.

Figura 5.8: Características del servidor usado

Ya superados estos dos inconvenientes, se procedió con la simulación de la red MPLS de la CNT EP de Pichincha en su estado actual sobre el simulador escogido que fue GNS3.

En la figura 5.9 se muestra una captura de pantalla de la red entera con todos sus routers encendidos y funcionales.

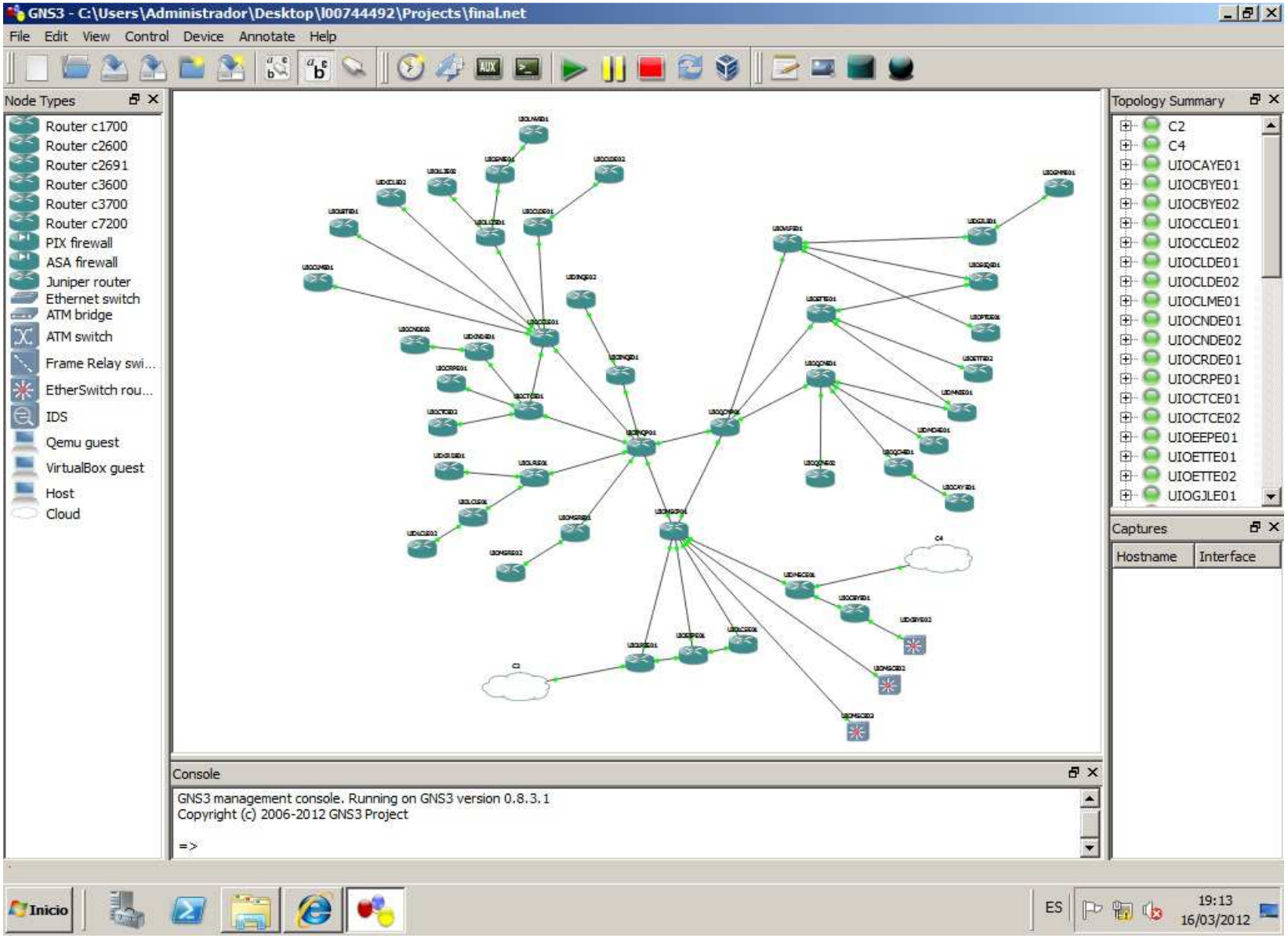


Figura 5.9: Red CNT MPLS PICHINCHA Simulada

5.4 SIMULACIÓN DE LA RED MPLS ZONA PICHINCHA EN SU SITUACION ACTUAL

En la figura 5.9 se muestra la red MPLS zona Pichincha de la CNT simulada por el software GNS3 en donde se observan todos los nodos funcionando correctamente lo que indica una comunicación eficiente.

5.4.1 COMPROBACIÓN DE FUNCIONAMIENTO DE MPLS

Para poder comprobar un correcto funcionamiento de MPLS se necesita validar:

- Funcionamiento del CEF.
- Propagación del protocolo IS-IS por los nodos sin fallas.
- Adecuada habilitación de LDP y comprobación del reenvío de paquetes con etiquetas MPLS.

5.4.1.1 Comprobación de CEF

Con el objeto de verificar la funcionalidad de CEF y mostrar el contenido de la tabla FIB, se utiliza el comando show ip cef. En la figura 5.10 se muestra el resultado al aplicar este comando en el router UIOQCNE01.

Si se desea comprobar que CEF se encuentre habilitado en un router y que contenido se encuentra en la tabla FIB (entradas y prefijos IP aprendidos), se debe ejecutar el comando **show ip cef summary** tal y como se muestra en la figura 5.11.

En la figura 5.12 se muestra la salida del comando **show ip cef detail** observando en detalle cada una de las entradas de la tabla FIB.

```
UIOQCNE01#sh ip cef
Prefix              Next Hop            Interface
0.0.0.0/0           drop                Null0 (default route handler entry)
0.0.0.0/32          receive
10.8.0.3/32         10.80.3.1           GigabitEthernet1/0
10.8.0.14/32        receive
10.8.0.26/32        10.80.3.1           GigabitEthernet1/0
10.8.0.28/32        10.80.3.1           GigabitEthernet1/0
10.11.0.14/32       receive
10.11.0.28/32       10.80.3.1           GigabitEthernet1/0
10.12.0.14/32       receive
10.12.0.28/32       10.80.3.1           GigabitEthernet1/0
10.13.0.14/32       receive
10.13.0.28/32       10.80.3.1           GigabitEthernet1/0
10.14.0.14/32       receive
10.30.0.3/32        10.80.3.1           GigabitEthernet1/0
10.30.0.14/32       receive
10.30.0.26/32       10.80.3.1           GigabitEthernet1/0
10.30.0.28/32       10.80.3.1           GigabitEthernet1/0
10.40.0.3/32        10.80.3.1           GigabitEthernet1/0
10.40.0.14/32       receive
10.40.0.26/32       10.80.3.1           GigabitEthernet1/0
10.40.0.28/32       10.80.3.1           GigabitEthernet1/0
10.41.0.14/32       receive
Prefix              Next Hop            Interface
10.41.0.28/32       10.80.3.1           GigabitEthernet1/0
10.50.0.3/32        10.80.3.1           GigabitEthernet1/0
10.50.0.14/32       receive
10.50.0.26/32       10.80.3.1           GigabitEthernet1/0
10.50.0.28/32       10.80.3.1           GigabitEthernet1/0
10.51.0.14/32       receive
10.51.0.28/32       10.80.3.1           GigabitEthernet1/0
10.80.0.12/30       10.80.3.1           GigabitEthernet1/0
10.80.2.120/30      10.80.3.1           GigabitEthernet1/0
10.80.3.0/30        attached            GigabitEthernet1/0
10.80.3.0/32        receive
10.80.3.1/32        10.80.3.1           GigabitEthernet1/0
10.80.3.2/32        receive
10.80.3.3/32        receive
```

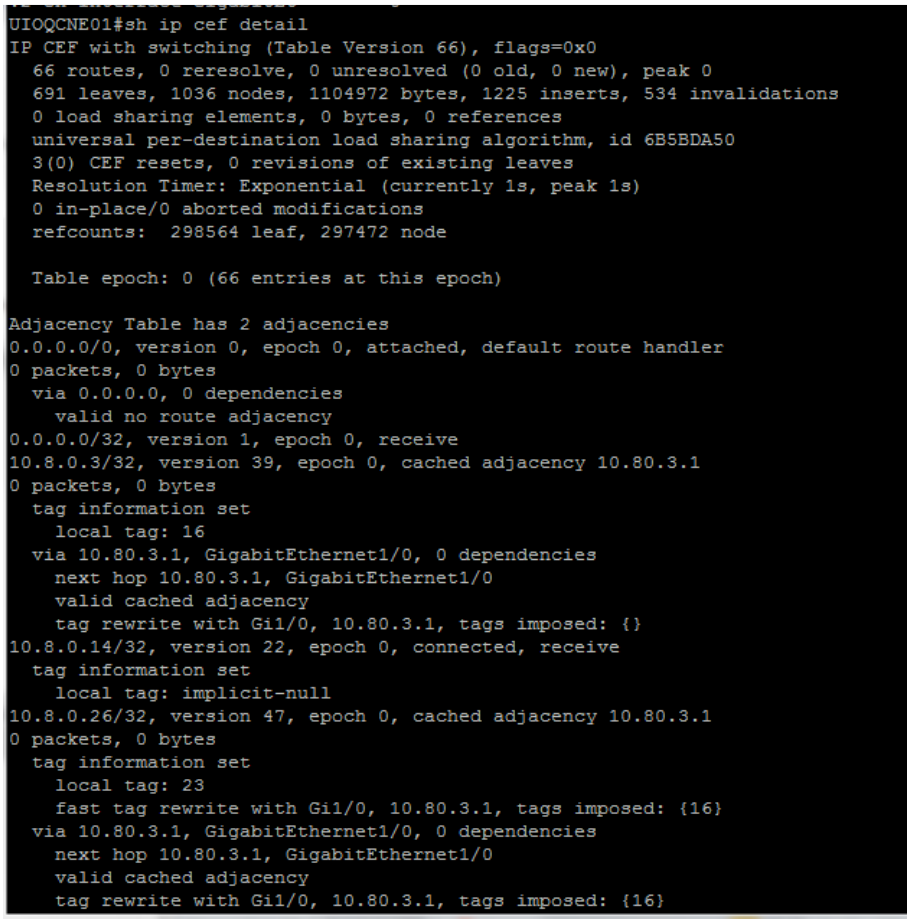
Figura 5.10: show ip cef en UIOQCNE01

```
UIOQCNE01#sh ip cef summary
IP CEF with switching (Table Version 66), flags=0x0
  66 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 0
  691 leaves, 1036 nodes, 1104972 bytes, 1225 inserts, 534 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id 6B5BDA50
  3(0) CEF resets, 0 revisions of existing leaves
  Resolution Timer: Exponential (currently 1s, peak 1s)
  0 in-place/0 aborted modifications
  refcounts:  298564 leaf, 297472 node

  Table epoch: 0 (66 entries at this epoch)

Adjacency Table has 2 adjacencies
UIOQCNE01#
```

Figura 5.11: show ip cef summary en UIOQCNE01



```
UIOQCNE01#sh ip cef detail
IP CEF with switching (Table Version 66), flags=0x0
  66 routes, 0 reresolve, 0 unresolved (0 old, 0 new), peak 0
  691 leaves, 1036 nodes, 1104972 bytes, 1225 inserts, 534 invalidations
  0 load sharing elements, 0 bytes, 0 references
  universal per-destination load sharing algorithm, id 6B5BDA50
  3(0) CEF resets, 0 revisions of existing leaves
  Resolution Timer: Exponential (currently 1s, peak 1s)
  0 in-place/0 aborted modifications
  refcounts:  298564 leaf, 297472 node

  Table epoch: 0 (66 entries at this epoch)

Adjacency Table has 2 adjacencies
0.0.0.0/0, version 0, epoch 0, attached, default route handler
0 packets, 0 bytes
  via 0.0.0.0, 0 dependencies
    valid no route adjacency
0.0.0.0/32, version 1, epoch 0, receive
10.8.0.3/32, version 39, epoch 0, cached adjacency 10.80.3.1
0 packets, 0 bytes
  tag information set
    local tag: 16
  via 10.80.3.1, GigabitEthernet1/0, 0 dependencies
    next hop 10.80.3.1, GigabitEthernet1/0
    valid cached adjacency
    tag rewrite with Gi1/0, 10.80.3.1, tags imposed: {}
10.8.0.14/32, version 22, epoch 0, connected, receive
  tag information set
    local tag: implicit-null
10.8.0.26/32, version 47, epoch 0, cached adjacency 10.80.3.1
0 packets, 0 bytes
  tag information set
    local tag: 23
    fast tag rewrite with Gi1/0, 10.80.3.1, tags imposed: {16}
  via 10.80.3.1, GigabitEthernet1/0, 0 dependencies
    next hop 10.80.3.1, GigabitEthernet1/0
    valid cached adjacency
    tag rewrite with Gi1/0, 10.80.3.1, tags imposed: {16}
```

Figura 5.12: show ip cef detail en UIOQCNE01

5.4.1.2 Comprobación del Protocolo IS-IS

En la figura 5.13 se observa la salida del comando **show ip protocols** que muestra los protocolos de enrutamiento que se encuentran activos en uno de los routers de core; uno de ellos el protocolo IS-IS.

Ahora que ya se tiene el protocolo levantado, se necesita validar que exista adyacencia entre los vecinos con el comando **show isis neighbors**. En la figura 5.14 se muestra la salida de este comando para el router UIOQCNE01.

En este caso los vecinos adyacentes para UIOQCNE01 están determinados por el “System Id” (UIOQCNE02, UIOQCNP01) junto con la interfaz por donde se aprende la ruta (Gi2/0, Gi1/0), la dirección IP de cada vecino, el estado (UP/DOWN) y el Holdtime (22/26 segundos).

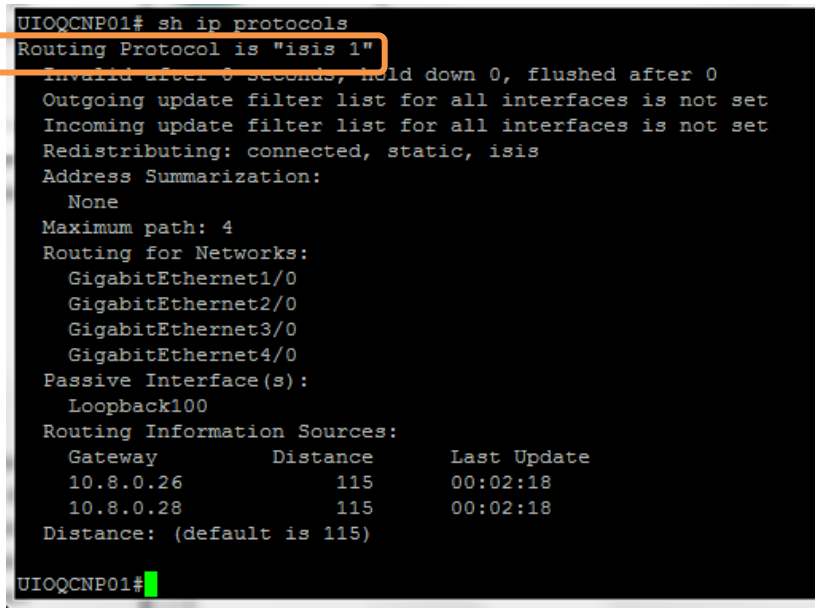


Figura 5.13: show ip protocols en UIOQCNP01

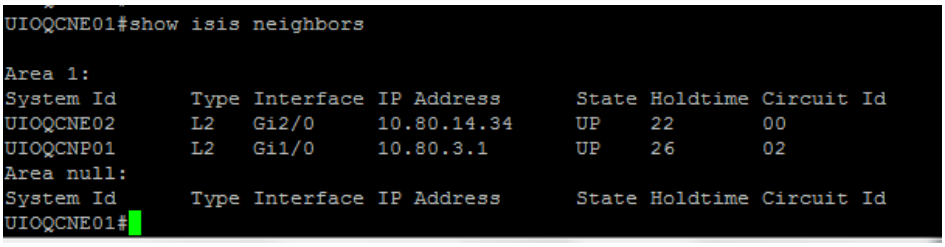


Figura 5.14: show isis neighbors en UIOQCNE01

Finalmente, para verificar que los routers se encuentran conectados en todas las áreas, se utiliza el comando **show isis topology,** éste despliega una lista de la localización de todos los equipos conocidos. En la figura 5.15 se verifica la salida de este comando para el equipo UIOQNCE01:

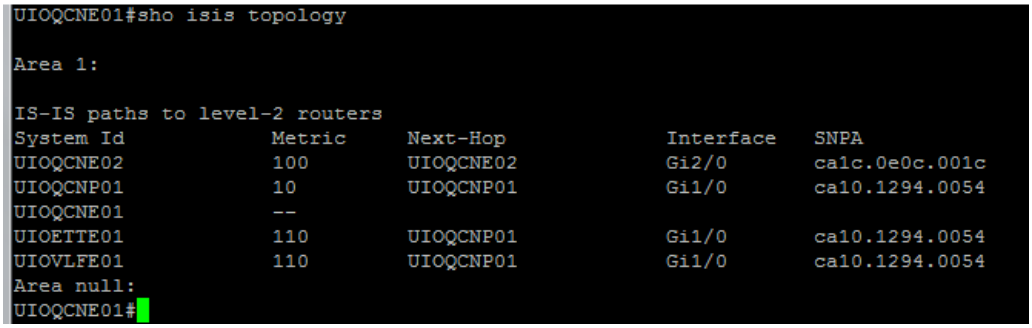


Figura 5.15: show isis topology en UIOQCNE01

5.4.1.3 Comprobación de LDP y funcionamiento de MPLS

A fin de verificar que MPLS se encuentre habilitado en el router y cuáles de sus interfaces se encuentran configuradas para la conmutación de etiquetas, se utiliza comando **show mpls interfaces**. Para el caso del equipo UIOQCNE01 la salida se muestra en la figura 5.16:

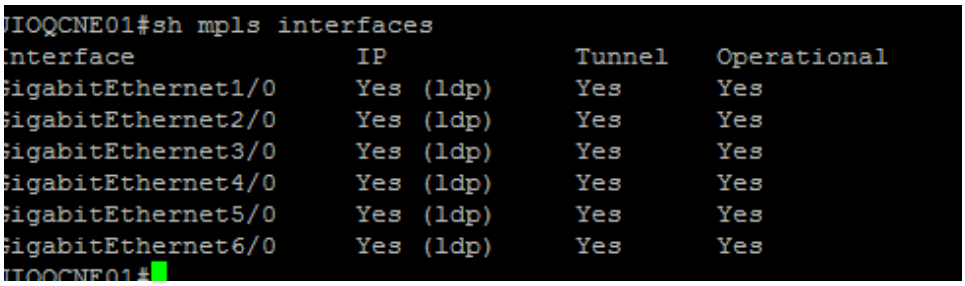


Figura 5.16: show mpls interfaces en UIOQCNE01

Aquí se pueden observar las interfaces del router activas y con LDP funcionando.

Una vez comprobado que MPLS se encuentra activo en las interfaces, lo siguiente será verificar que el protocolo LDP se encuentre correctamente configurado; para esto se puede observar la figura 5.17 en donde se tiene la salida del comando **show mpls ldp discovery**:

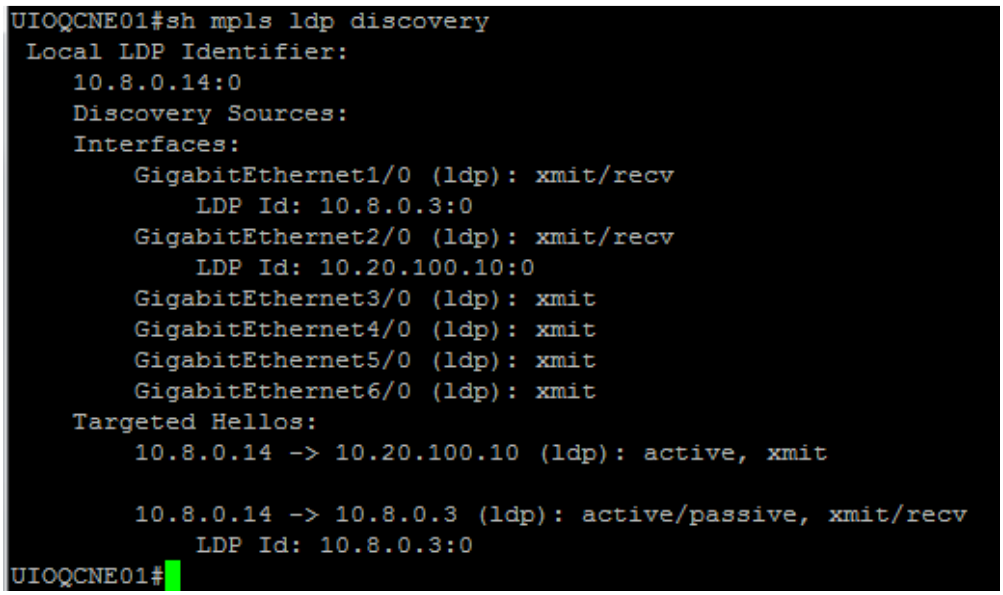


Figura 5.17: show mpls ldp discovery en UIOQCNE01

Se despliega el estado del proceso LDP, además de generar una lista de interfaces sobre las cuales LDP se encuentra corriendo.

Ahora, para mostrar el contenido de la LIB, se utiliza el comando **show mls ldp bindings** en el cual se puede verificar la tabla de etiquetas a ser procesadas por el router para propagar a sus vecinos. En el caso de la figura 5.18, si los routers vecinos desean comunicarse con la IP 10.8.0.26 (UIOETTE01) a través del equipo UIQCNE01, estos deben etiquetar el paquete con el valor “20”, y en el caso de que se envíe tráfico desde UIOQCNE01 hacia UIOETTE01 a través de la IP 10.8.0.30 (UIOQCNP01) éste debe etiquetar el paquete con un valor de “16”:

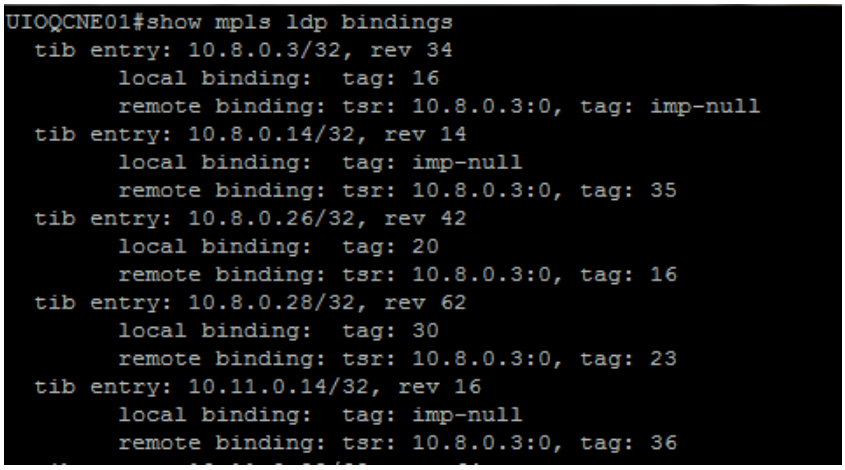


Figura 5.18: show mpls ldp bindings en UIOQCNE01

En la figura 5.19 se muestra la captura de tráfico icmp hacia la IP 10.8.0.26 donde se observa la etiqueta mpls asignada con valor “16”:

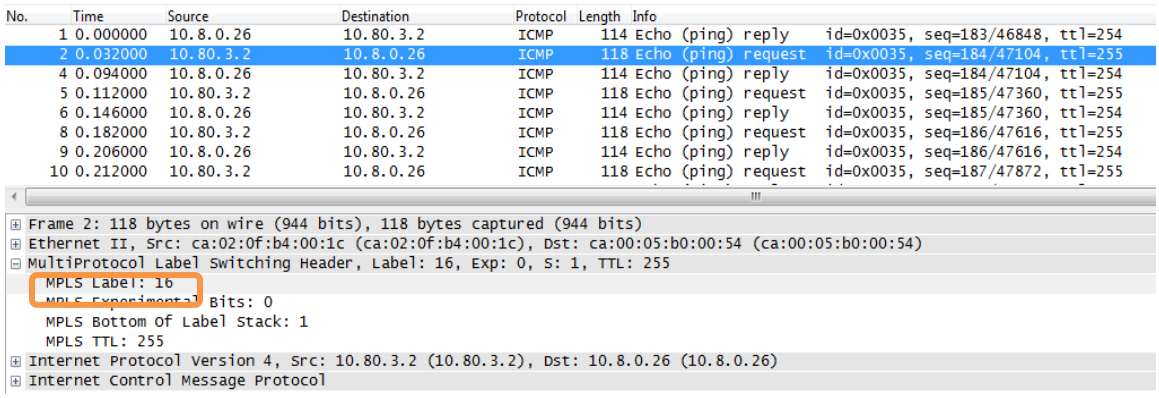
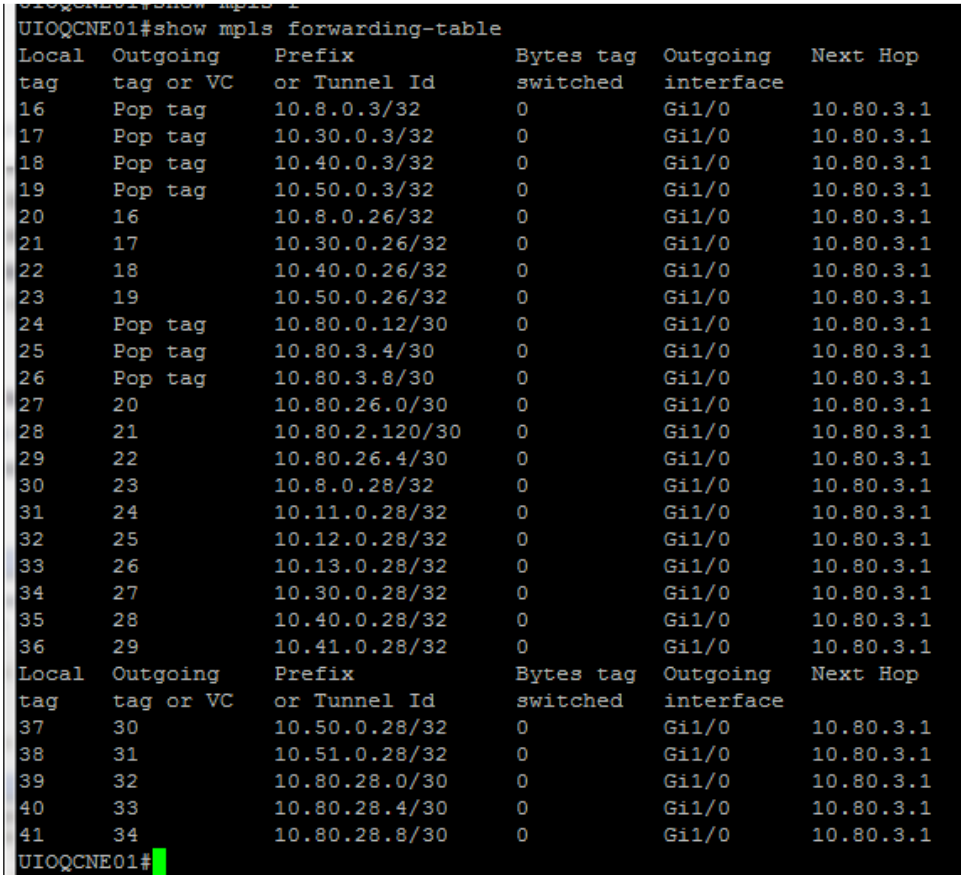


Figura 5.19: captura wireshark de tráfico ICMP

Finalmente se muestra en la figura 5.20 la tabla de envío y etiquetado mpls para alcanzar cada una de las redes o prefijos de red; esto se lo logra con el comando **show mpls forwarding-table**:



```
UIOQCNE01#show mpls forwarding-table
Local  Outgoing    Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
16     Pop tag     10.8.0.3/32      0          Gi1/0      10.80.3.1
17     Pop tag     10.30.0.3/32     0          Gi1/0      10.80.3.1
18     Pop tag     10.40.0.3/32     0          Gi1/0      10.80.3.1
19     Pop tag     10.50.0.3/32     0          Gi1/0      10.80.3.1
20     16          10.8.0.26/32     0          Gi1/0      10.80.3.1
21     17          10.30.0.26/32    0          Gi1/0      10.80.3.1
22     18          10.40.0.26/32    0          Gi1/0      10.80.3.1
23     19          10.50.0.26/32    0          Gi1/0      10.80.3.1
24     Pop tag     10.80.0.12/30    0          Gi1/0      10.80.3.1
25     Pop tag     10.80.3.4/30     0          Gi1/0      10.80.3.1
26     Pop tag     10.80.3.8/30     0          Gi1/0      10.80.3.1
27     20          10.80.26.0/30    0          Gi1/0      10.80.3.1
28     21          10.80.2.120/30   0          Gi1/0      10.80.3.1
29     22          10.80.26.4/30    0          Gi1/0      10.80.3.1
30     23          10.8.0.28/32     0          Gi1/0      10.80.3.1
31     24          10.11.0.28/32    0          Gi1/0      10.80.3.1
32     25          10.12.0.28/32    0          Gi1/0      10.80.3.1
33     26          10.13.0.28/32    0          Gi1/0      10.80.3.1
34     27          10.30.0.28/32    0          Gi1/0      10.80.3.1
35     28          10.40.0.28/32    0          Gi1/0      10.80.3.1
36     29          10.41.0.28/32    0          Gi1/0      10.80.3.1
Local  Outgoing    Prefix           Bytes tag  Outgoing   Next Hop
tag    tag or VC   or Tunnel Id     switched   interface
37     30          10.50.0.28/32    0          Gi1/0      10.80.3.1
38     31          10.51.0.28/32    0          Gi1/0      10.80.3.1
39     32          10.80.28.0/30    0          Gi1/0      10.80.3.1
40     33          10.80.28.4/30    0          Gi1/0      10.80.3.1
41     34          10.80.28.8/30    0          Gi1/0      10.80.3.1
UIOQCNE01#
```

Figura 5.20: show mpls forwarding-table en UIOQCNE01

5.4.2 COMPROBACIÓN DE FUNCIONAMIENTO DE BGP ENTRE CLIENTES

En la simulación realizada se crearon 3 clientes en tres diferentes nodos (UIOETTE01, UIOVLFE01 y UIOQCNE02) todos estos pertenecientes a la vrf “prueba” la cual fue relacionada con el sistema autónomo del BGP 28006 para el enrutamiento; a continuación se podrá comprobar el funcionamiento de BGP con VPNV4 para la conectividad entre los clientes finales. En la figura 5.21 se muestra la configuración de la vrf prueba, mientras que en la 5.22, 5.23 y 5.24 se puede observar la configuración de los clientes para IPV4.

```
Current configuration : 396 bytes
ip vrf pruipv4
 description vrf ipv4
 rd 12:1
 route-target export 12:1
 route-target import 12:1
!
```

Figura 5.21: Configuración de vrf

```
UIOQCNE02#sh running-config interface gi6/0
Building configuration...

Current configuration : 210 bytes
!
interface GigabitEthernet6/0
 description 809451 - COOPAD - MATRIZ
 ip vrf forwarding prueba
 ip address 10.0.0.1 255.255.255.252
 negotiation auto
 service-policy input QoSv
 service-policy output QoSv
end

UIOQCNE02#
```

Figura 5.22: Configuración de un cliente en la interfaz GI6/0

```
UIOVLFE01#sh running-config int FastEthernet0/1
Building configuration...

Current configuration : 246 bytes
!
interface FastEthernet0/1
 description By VPNSC: Job Id# = 6151 (809192 - COOPAD - VILLAFLORA)
 ip vrf forwarding prueba
 ip address 10.0.0.29 255.255.255.252
 duplex auto
 speed auto
 service-policy input QoSv
 service-policy output QoSv
end
```

Figura 5.23: Cliente IPV4 en la interfaz FE0/1

```
UIOETTE01#show running-config interface FastEthernet0/0
Building configuration...

Current configuration : 201 bytes
!
interface FastEthernet0/0
 description COOPAD-TRES
 ip vrf forwarding prueba
 ip address 10.0.0.6 255.255.255.252
 duplex auto
 speed auto
 service-policy input QoSv
 service-policy output QoSv
end

UIOETTE01#
```

Figura 5.24: Cliente IPV4 en la interfaz FE0/0

Una vez configurados los clientes se debe lograr la comunicación entre ellos; para esto se configuran los vecinos en BGP, address-family para ipv4 y vpn4, así como para la vrf recién creada.

En la figura 5.25 se puede ver la configuración de BGP del equipo UIOQCNE01 en donde:

- Los vecinos configurados pertenecen a los routers UIOVLFE01 y UIOETTE01 con las IP´s respectivas (10.8.0.28, 10.8.0.26).
- El address-family tanto ipv4 como en la vrf tienen una redistribución estática.
- El address-family vpnv4 se encuentra asociado a los vecinos creados anteriormente.

```
router bgp 28006
 bgp router-id 10.20.100.10
 no bgp default ipv4-unicast
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 neighbor 10.8.0.26 remote-as 28006
 neighbor 10.8.0.26 description ### iBGP To UIOVLFE01 ###
 neighbor 10.8.0.26 password 7 0214294B5A531F711D1950
 neighbor 10.8.0.26 update-source Loopback100
 neighbor 10.8.0.28 remote-as 28006
 neighbor 10.8.0.28 description ### iBGP To UIOVFLE01 ###
 neighbor 10.8.0.28 password 7 0214294B5A531F711D1950
 neighbor 10.8.0.28 update-source Loopback100
 !
 address-family ipv4
 redistribute connected
 redistribute static route-map REDISTRIBUCION_STATIC
 no auto-summary
 no synchronization
 exit-address-family
 !
 address-family vpnv4
 neighbor 10.8.0.26 activate
 neighbor 10.8.0.26 send-community both
 neighbor 10.8.0.28 activate
 neighbor 10.8.0.28 send-community both
 exit-address-family
 !
 address-family ipv4 vrf prueba
 redistribute connected
 redistribute static
 no synchronization
 exit-address-family
 !
```

Figura 5.25: Configuración BGP necesaria

Para verificar el protocolo a nivel de usuarios finales; el comando **show ip bgp vpnv4 vrf prueba** nos muestra la base de datos de topología BGP en el túnel vpnv4 tal como se muestra en la figura 5.26.

```
UIOETTE01#sh ip bgp vpnv4 Vrf prueba
BGP table version is 25, local router ID is 10.8.0.26
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: 28006:1 (default for vrf prueba)
*>i10.0.0.0/30      10.20.100.10             0    100      0 ?
*> 10.0.0.4/30      0.0.0.0                  0         32768 ?
*>i10.0.0.28/30     10.8.0.28                0    100      0 ?
UIOETTE01#
```

Figura 5.26: Usuarios de la vrf configurada para IPV4

En donde el asterisco (*) indica que a dirección del next hop o próximo salto es válida, el símbolo “>” indica el mejor camino por una ruta seleccionada por BGP, la letra “i” presente quiere decir que un vecino IBGP ha advertido la ruta al router, y si no está presente y en su lugar se encuentra un espacio en blanco, significa que BGP aprendió dicha ruta desde un par externo.

Una vez configurado BGP y los clientes finales; se puede probar la conectividad entre estos tres; en las figuras 5.27, 5.28 y 5.29 se muestran las pruebas de icmp extremo a extremo para los tres clientes realizados en la simulación.

```
UIOQCNE02#ping vrf prueba 10.0.0.29

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.29, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/128/168 ms
UIOQCNE02#ping vrf prueba 10.0.0.6

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.0.0.6, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/103/160 ms
```

Figura 5.27: Conectividad entre clientes pertenecientes a la vrf configurada en UIOQCNE02

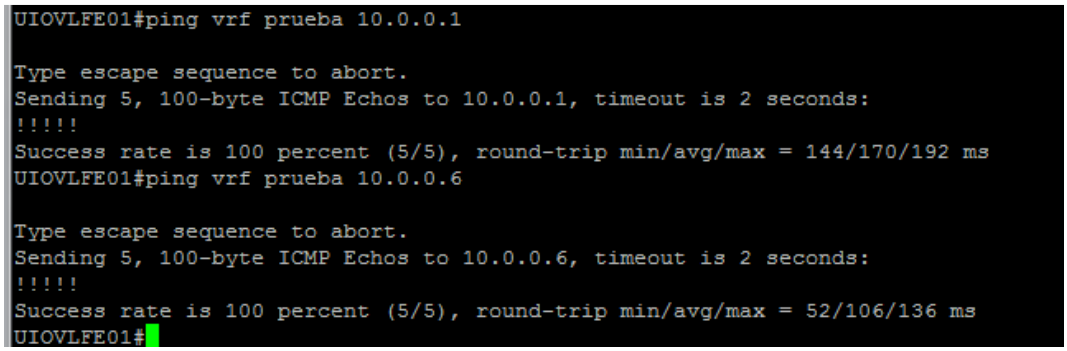


Figura 5.28: Conectividad entre clientes pertenecientes a la vrf configurada en UIOVLFE01

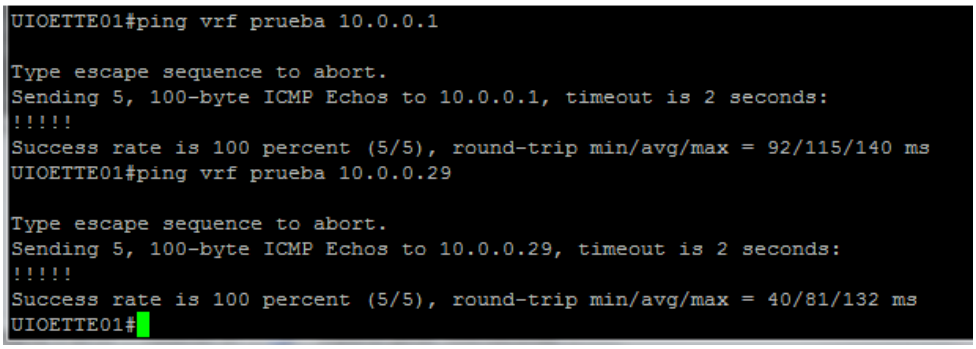


Figura 5.29: Conectividad entre clientes pertenecientes a la vrf configurada en UIOETTE01

5.4.3 COMPROBACIÓN DE FUNCIONAMIENTO DE QoS

El objetivo principal de la calidad de servicio utilizado en la simulación es poder diferenciar y dar prioridad a los servicios de voz por sobre los de datos frente a una saturación del canal; esto se logra otorgando un valor de precedencia alto de acuerdo a la tabla 5.3.

La tabla 5.4 muestra los valores de precedencia desde el menos al más importante de acuerdo al RFC 791.

De tal manera que se crea la política de servicio (policy-map) **rtp**, la cual asigna precedencia 5 al tráfico que coincida con la clase de servicio **rtp**; la figura 5.30 muestra la configuración del policy-map rtp.

DSCP Name	DS Field Value		IP Precedence
	Binary	Decimal	
CS0	000 000	0	0
CS1	001 000	8	1
AF11	001 010	10	1
AF12	001 100	12	1
AF13	001 110	14	1
CS2	010 000	16	2
AF21	010 010	18	2
AF22	010 100	20	2
AF23	010 110	22	2
CS3	011 000	24	3
AF31	011 010	26	3
AF32	011 100	28	3
AF33	011 110	30	3
CS4	100 000	32	4
AF41	100 010	34	4
AF42	100 100	36	4
AF43	100 110	38	4
CS5	101 000	40	5
EF	101 110	46	5
CS6	110 000	48	6
CS7	111 000	56	7

Tabla 5.3: Tabla comparativa para QoS[40]

[40] http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_0_4_s_v_1_3/qos/configuration/guide/n1000v_qos_6dscpval.html

Valor	Descripción
000 (0)	Rutina o mejor esfuerzo
001 (1)	Prioridad
010 (2)	Inmediato
011 (3)	Flash (principalmente utilizado para señalización de voz y video)
100 (4)	Señal Continua
101 (5)	Crítica (utilizada principalmente para voz)
110 (6)	Internet
111 (7)	Red

Tabla 5.4: Tabla con valores de precedencia

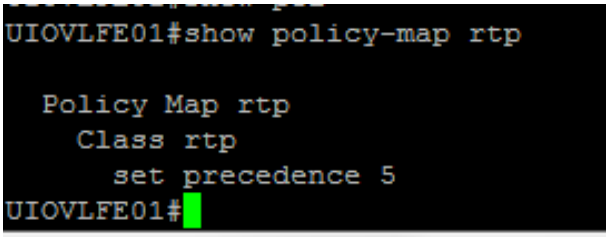


Figura 5.30: Configuración del policy-map

En la figura 5.31 se puede observar la configuración de la clase de servicio **rtp** la cual en la línea **"match protocol rtp"** permite el tráfico que coincida con el protocolo rtp (voz).

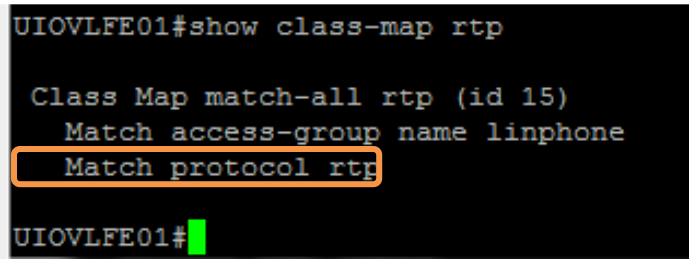


Figura 5.31: Configuración del class-map para voz

Para aplicar QoS a la interfaz deseada basta con añadir con comando **service-policy** ya sea de entrada (input) o salida (output); para el caso de la simulación se configura en ambas vías ya que el tráfico de voz a comprobar es de extremo a

extremo. En la figura 5.32 se puede observar la configuración en la interfaz para QoS.

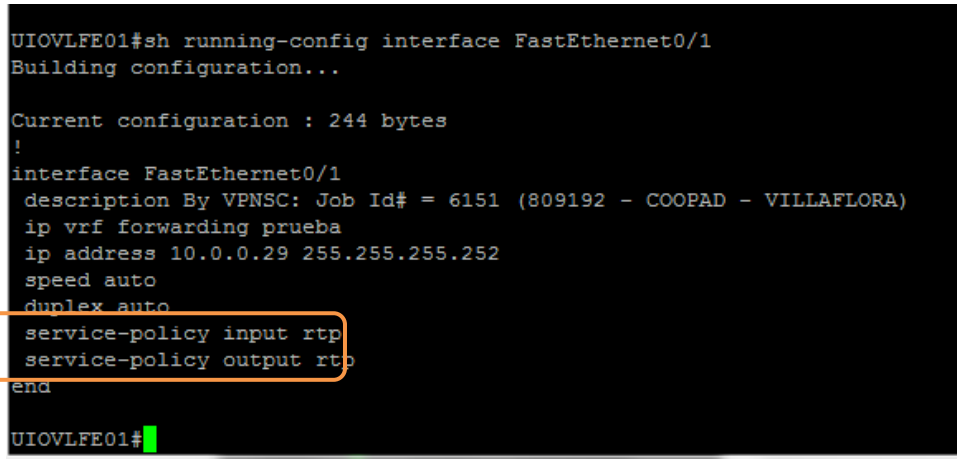


Figura 5.32: Configuración de Qos en la interfaz hacia el cliente

5.5 SIMULACIÓN DE LA RED MPLS ZONA PICHINCHA IMPLEMENTANDO IPV6

Para esta simulación se tomó en cuenta el uso de 6VPE para que IPV4 e IPV6 puedan coexistir libremente además de presentar un mínimo impacto en la red, como se demostró en capítulos anteriores.

5.5.1 COMPROBACIÓN DE LA CONECTIVIDAD, CONFIGURACIÓN Y OPERACIÓN DE IPV6 [5]

Se validará la configuración de IPV6 en la MPLS con los siguientes pasos:

- Funcionamiento de IPV6 CEF
- Interfaces configuradas correctamente
- Revisión de tráfico IPV6

5.5.1.1 Comprobación de CEF

Con el objeto de verificar la funcionalidad de CEF y mostrar el contenido de la tabla FIB para IPV6, se utiliza el comando **show ipv6 cef detail** mostrado en la figura 5.33.

```
UIOVLFE01#show ipv6 cef det
IPv6 CEF is enabled and running centrally.
VRF Default
 4 prefixes (4/0 fwd/non-fwd)
 Table id 0x1E000000
 Database epoch:        0 (4 entries at this epoch)

::/0, epoch 0, flags default route handler
  no route
::/127, epoch 0, flags attached, discard
  discard
FE80::/10, epoch 0, flags attached, receive, local
  receive for Null0
FF00::/8, epoch 0, flags attached, receive, local
  receive for Null0
UIOVLFE01#
```

Figura 5.33: Tabla FIB para IPV6.

5.5.1.2 Comprobación de Interfaces IPV6

El comando **show ipv6 interfaz** mostrado en la figura 5.34 es usado para verificar que las direcciones IPV6 estén configuradas correctamente.

```
UIOLPZEO1#sh ipv6 interface
GigabitEthernet1/0 is up, line protocol is up
  IPv6 is enabled, link-local address is FE80::C808:15FF:FE18:1C
  No Virtual link-local address(es):
  Description: ### IPV6 a UIOMSCEO1 GI4/0###
  Global unicast address(es):
    FEC0::1, subnet is FEC0::/64
  Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF18:1C
  VPN Routing/Forwarding "pruipv6"
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  Input features: QoS classify, QoS actions
  Service-policy input: qos-voice
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
UIOLPZEO1#
```

Figura 5.34: Configuración para una interfaz conectada a un cliente IPV6.

5.5.1.3 Comprobación de tráfico IPV6

El comando **show ipv6 traffic** muestra las estadísticas ICMP, en la figura 5.35 se muestra el resultado para el router UIOLPZE01.

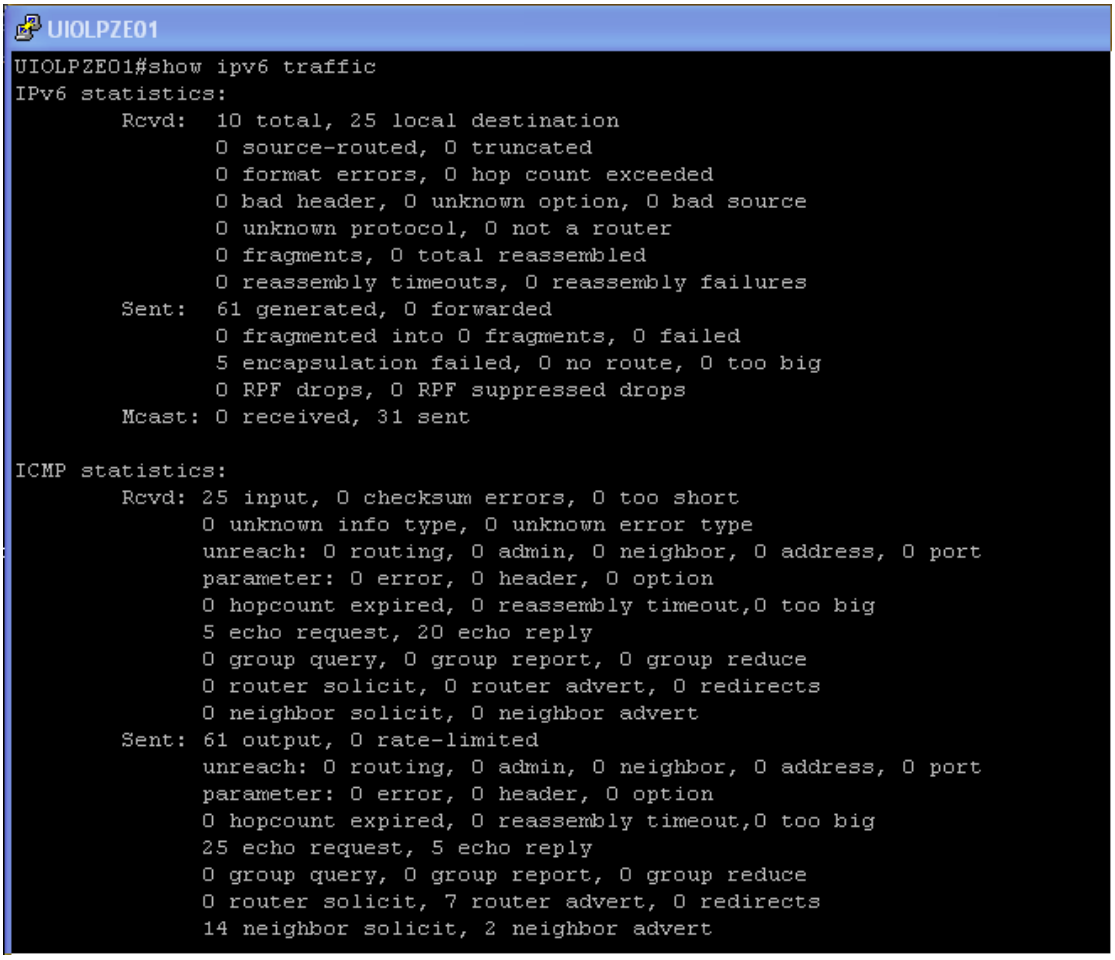


Figura 5.35: Estadísticas de tráfico IPV6

5.5.2 COMPROBACIÓN DE FUNCIONAMIENTO DE BGP ENTRE CLIENTES IPV6

Se creó un cliente el cual pertenece a la vrf “pruipv6”, esta vrf está relacionada con AS 28006. A continuación se muestra las configuraciones realizadas para la creación de la VPNV6 que permite la comunicación entre clientes IPV6. En la figura 5.36 se muestra la creación de la vrf “pruipv6”, y en la figura 5.36 la asignación a la interfaz respectiva.

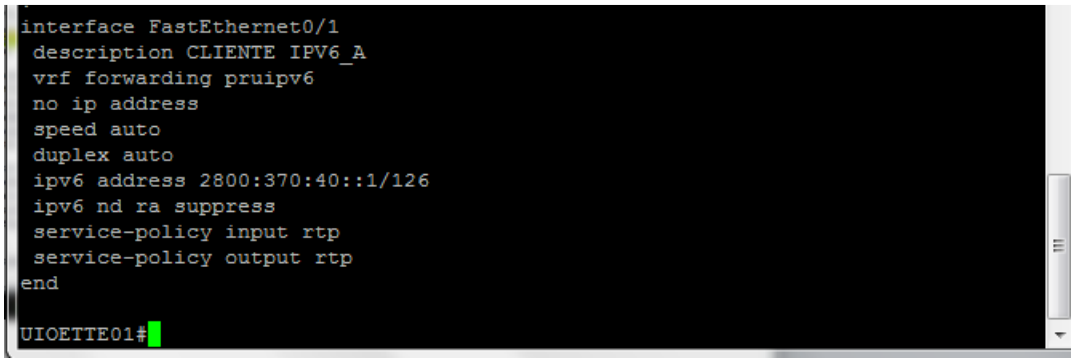


Figura 5.36: Reenvío de tráfico IPV6 por la interfaz fe0/1

Al igual que en IPV4 se procede con la creación de los routers vecinos; se debe configurar las vecinas con las que tendremos conexión, en la figura 5.37 se puede observar que en el router UIOVLFE01 de IP 10.8.0.28 se configura el router vecino UIOETTE01 con la IP 10.8.0.26.

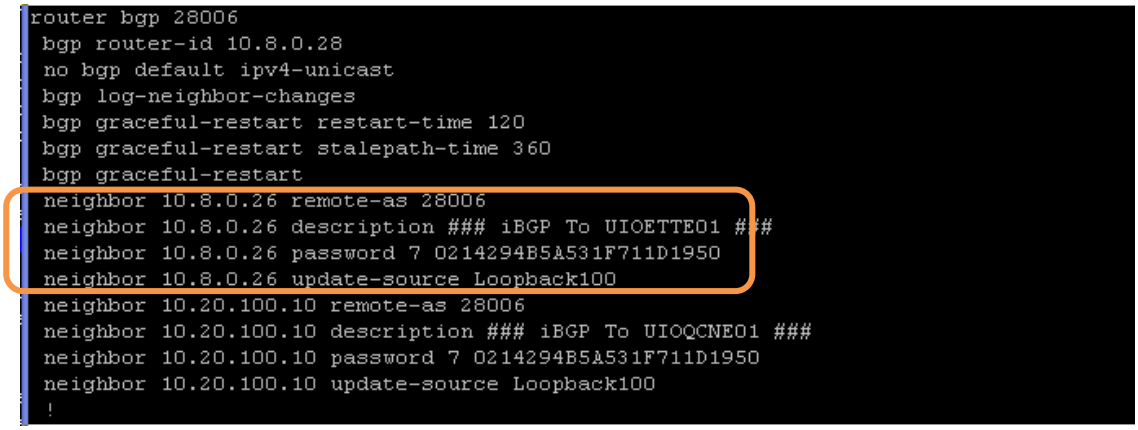


Figura 5.37: Vecinas BGP del router UIOVLFE01

También se tiene dos **address-family,** el vpnv6 asociado a las vecinas (PEs) creadas anteriormente el cual nos permitirá intercambiar rutas con el/los routers par PE, es mostrado en la figura 5.38; y el ipv6 vrf pruipv6, mostrado en la figura 5.39, es usado para la redistribución de rutas a través de la vrf especificada, para este caso se tiene rutas estáticas entre los PEs y CEs del cliente IPV6.

A continuación se realiza la revisión de sesiones establecidas entre vecinos, para esto se usa el comando **show bgp vpnv6 unicast all,** el resultado se muestra en la figura 5.40.

```
address-family vpnv6
 neighbor 10.8.0.26 activate
 neighbor 10.8.0.26 send-community both
 neighbor 10.20.100.10 activate
 neighbor 10.20.100.10 send-community both
exit-address-family
!
```

Figura 5.38: VPNV6 para el cliente IPV6

```
!
address-family ipv6 vrf pruipv6
 redistribute connected
 redistribute static route-map REDISTRIBUCION_STATIC
 no synchronization
exit-address-family
!
```

Figura 5.39: “ipv6 vrf pruipv6” para el cliente IPV6

```
UIOETTE01#show bgp vpnv6 un
UIOETTE01#show bgp vpnv6 unicast
% Incomplete command.

UIOETTE01#show bgp vpnv6 unicast ?
  all  Display information about all VPN NLRIs
  rd   Display information for a route distinguisher
  vrf  Display information for a VPN Routing/Forwarding instance

UIOETTE01#show bgp vpnv6 unicast all
BGP table version is 7, local router ID is 10.8.0.26
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: 28006:2 (default for vrf pruipv6)
*>i2800:370:36:1::/64
                    ::FFFF:10.8.0.28
                                         0    100      0 ?
*> 2800:370:40::/126
                    ::                   0         32768 ?
```

Figura 5.40: Sesiones BGP para VPNV6 establecidas en la simulación

Ya que está establecida la comunicación, se puede proceder a probar conectividad; en la figura 5.41 se observa las pruebas de ping entre los routers PE del cliente IPV6, demostrando la conectividad de los mismos.

5.5.3 COMPROBACIÓN DE FUNCIONAMIENTO DE QoS EN IPV6

El objetivo principal es mantener la calidad de servicio QoS que se tenía para los clientes en IPV4 en los nuevos clientes IPV6. En IPV6 no se puede especificar el

comando “**match protocol rtp**” ya que este sirve solo para IPV4. Para poder demostrar Qos para VoIP en nuestra simulación se procedió a crear una lista de acceso (access list), al igual que las demás QoS de la red. En la figura 5.42 se muestra la lista de acceso creada, esta hace referencia al puerto UDP 7078 que es el puerto usado por el software linphone para llamadas VoIP.

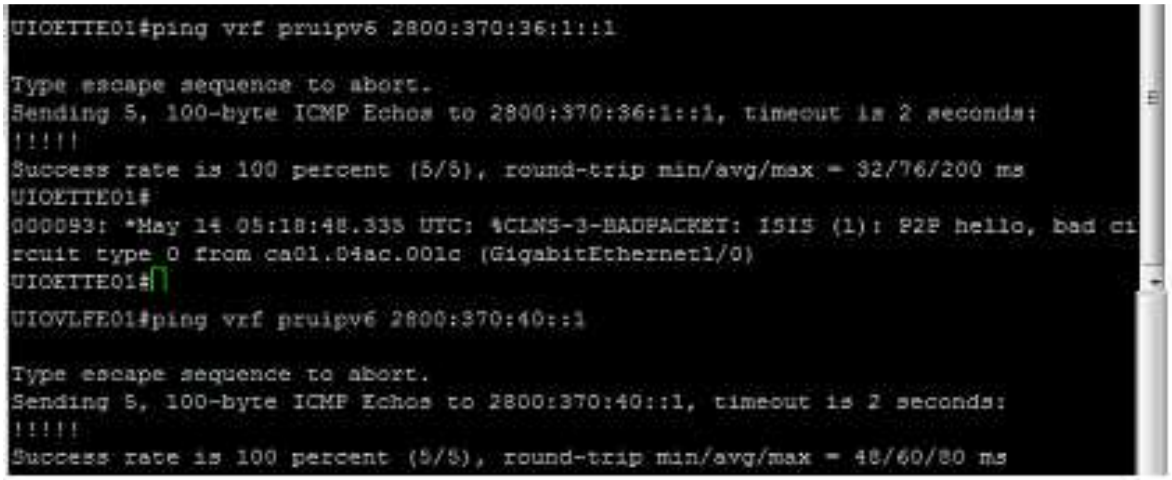


Figura 5.41: Conectividad entre dos puntos para el cliente IPV6

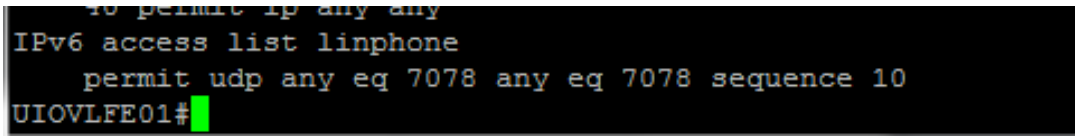


Figura 5.42: Lista de acceso creada para VoIP

Después, dentro de la clase de servicio (class-map) **“rtp”** se añadió la lista de acceso “linphone” creada previamente con el comando **match access-group name linphone,** este tomará todo el tráfico que cumpla con lo especificado en la lista de acceso; en la figura 5.43 se muestra la configuración.

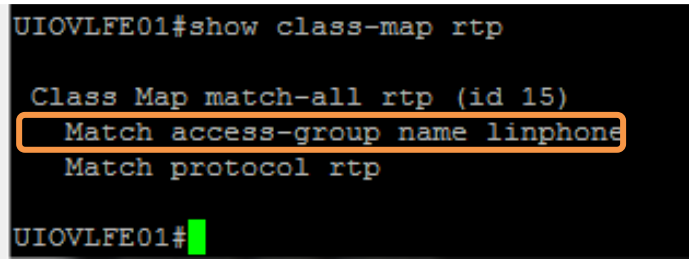


Figura 5.43: Lista de acceso añadida a la clase de servicio rtp

Esta clase de servicio ya está añadida a la política de servicio **rtp.** Al igual que en IPV4, mediante el comando **service-policy** se añade la política de servicio a la interfaz del cliente IPV6, para nuestro caso se añadió tanto para la entrada como la salida de datos de las interfaces hacia los clientes IPV6, como se muestra en la figura 5.44.

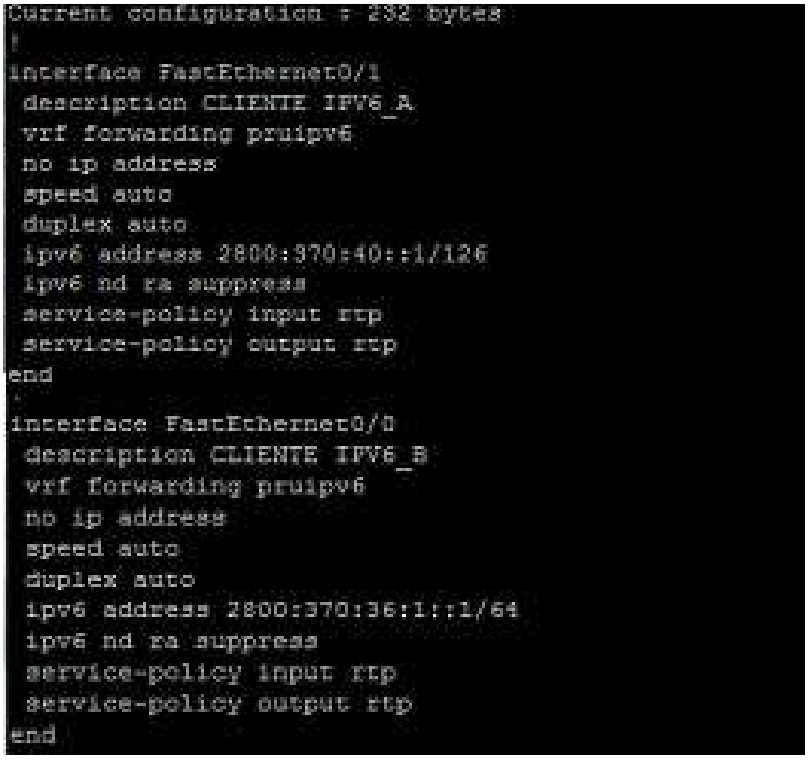


Figura 5.44: Configuración de Qos en la interfaz hacia el cliente IPV6

Así como para el caso de IPV4 se probará en IPV6 tres tipos de servicio: voz, datos icmp y datos ftp. En el apartado siguiente se muestra el detalle de los mismos.

La tabla 5.5 se muestra una comparativa para los comandos tanto IPV4 como IPV6, desarrollados en el presente proyecto.

5.6 PRUEBAS DE CALIDAD DE SERVICIO EN IPV4 E IPV6 (QoS)

Las pruebas de QoS en la simulación se las realizaron utilizando 3 tipos de servicio: voz, datos icmp y datos ftp; y para el análisis de tráfico se utilizó wireshark. A continuación se detallan los tres casos de QoS a comprobar.

		IPV4	IPV6
CEF		Router(config)# ip cef distributed	Router(config)# ipv6 cef distributed
MPLS FRAME MODE	**INTERFAZ DE LOOPBACK**	Router(config)# interface Loopback 100	Router(config)# interface Loopback 100
	MPLS	Router(config)# mpls ip	Router(config)# mpls ip
	LDP	Router(config)# mpls ldp neighbor 11.56.4.48 password 7 044926165E745C1E5F4D53	Router(config)# mpls ldp neighbor 11.56.4.48 password 7 044926165E745C1E5F4D53
		Router(config)# mpls ldp graceful-restart	Router(config)# mpls ldp graceful-restart
		Router(config)# mpls ldp router-id Loopback100 force	Router(config)# mpls ldp router-id Loopback100 force
IS-IS		Router(config)# router isis 1	Router(config)# router isis 1
BGP		Router(config)# router bgp 28006	Router(config)# router bgp 28006
	ADDRESS FAMILY	Router(config)# address-family vpnv4	Router(config)# address-family vpnv6
		Router(config)# address-family vpnv4 vrf prueba	Router(config)# address-family ipv6 vrf pruipv6
VRF		Router(config)# ip vrf prueba rd 12:1 route-target export 12:1 route-target import 12:1	Router(config)# vrf definition pruipv6 rd 12:1 route-target export 12:1 route-target import 12:1
INTERFAZ		Router(config)# interface fa0/1 ip vrf forwarding prueba ip address x.x.x.x x.x.x.x	Router(config)# interface fa0/1 vrf forwarding pruipv6 ipv6 address x:x:x::/x ipv6 nd ra suppress

Tabla 5.5: Tabla comparativa de comandos IPV4 e IPV6. Pg. 1 de 2

		IPV4	IPV6
QoS	**Policy Map**	Router(config)# Policy Map rtp Class rtp set precedence 5	Router(config)# Policy Map rtp Class rtp set precedence 5
	Class Map	Router(config)# Class Map match-all rtp Match protocol rtp	Router(config)# Class Map match-all rtp Match access-group name linphone

Tabla 5.5: Tabla comparativa de comandos IPV4 e IPV6. Pg. 2 de 2

Cabe mencionar que CNT utiliza Access-list (lista de acceso) para diferenciar el tráfico de voz y el de datos; a una sola interfaz se le asigna todo el tráfico de voz. Para propósito de esta tesis se ha asignado diferentes tipos de tráfico a una sola interfaz y después se analiza su resultado de acuerdo a las capturas obtenidas con wireshark.

5.6.1 PRUEBAS DE CALIDAD DE SERVICIO (QoS) CON TRÁFICO ICMP

El tráfico ICMP (ping) es el más común y utilizado para realizar pruebas de primer nivel y conectividad entre dos puntos; bajo este tipo de tráfico se puede evidenciar perdida de servicio, tiempos altos o intermitencias en un circuito.

5.6.1.1 Objetivo

Para la comprobación de la calidad de servicio (QoS) utilizando este tipo de paquetes se presentan dos escenarios, el primero sin aplicar la calidad de servicio y el segundo en donde se utilizan comandos extendidos para poder emular tráfico de voz y garantizar un 100% de paquetes entregados a su destino.

- **Primer escenario:** se realizará una prueba de ping extremo – extremo sin la aplicación de políticas de QoS en la interfaz.

- **Segundo escenario:** aplicando la política de QoS llamada QoSv nuevamente se ejecutara un ping extendido entre los dos extremos.

5.6.1.2 Análisis de resultados

En la figura 5.45 se puede verificar un ping extendido entre dos de los clientes configurados. Debido a que la simulación de la red depende de la capacidad y memoria del computador, existirá una pérdida considerable de paquetes (7%) tomando en cuenta que el servicio a contratar por el cliente es de datos.

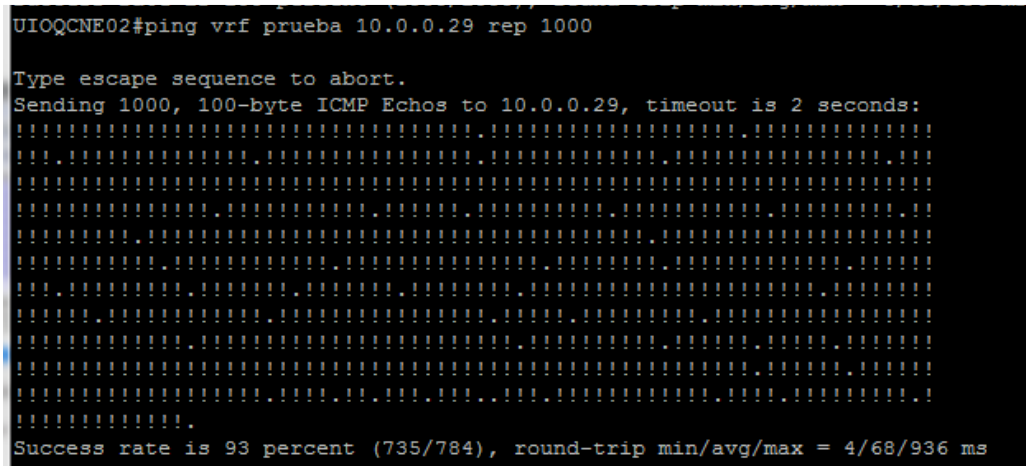


Figura 5.45: Ping extendido sin Tipo de Servicio

Aplicando QoS en la interfaz y utilizando comandos extendidos ofrecidos por cisco, se puede garantizar un 100% de efectividad de entrega de paquetes icmp; esto debido a que el tipo de servicio especificado (160) hace que se le entregue la precedencia critica (5); la figura 5.46 muestra los comandos extendidos utilizados y una efectividad del 100%, mientras que en la figura 5.47 se puede observar la captura de wireshark que muestra la precedencia otorgada.

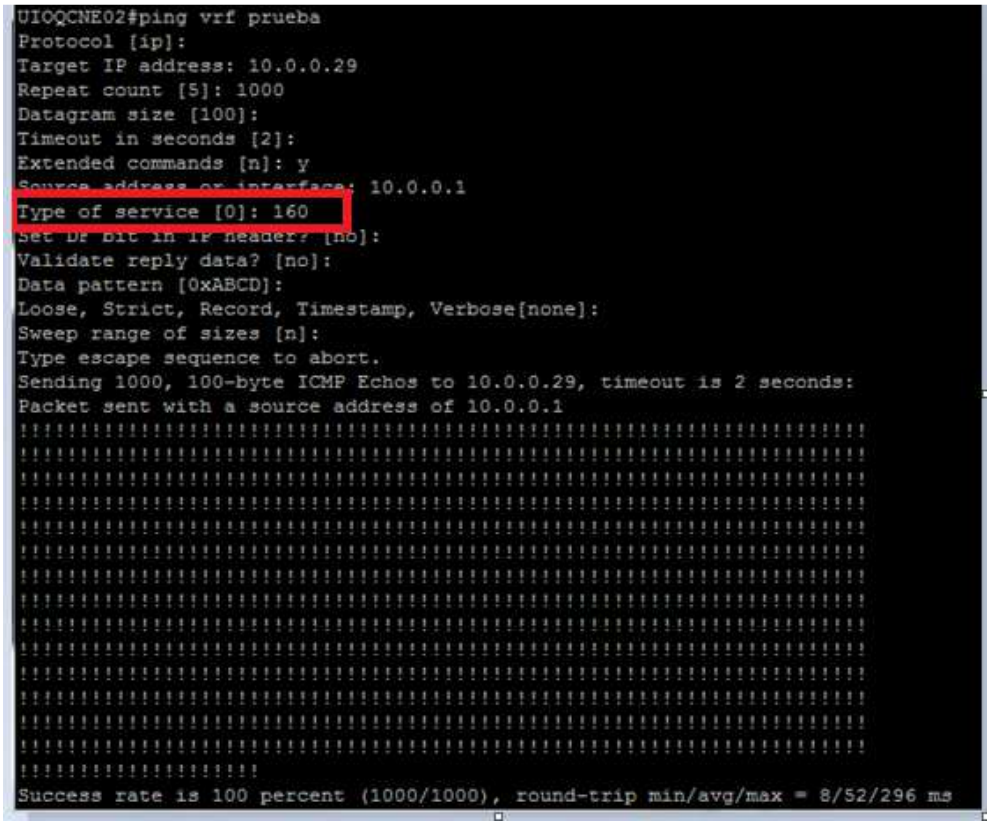


Figura 5.46: Ping extendido con ToS de 160 y efectividad del 100%

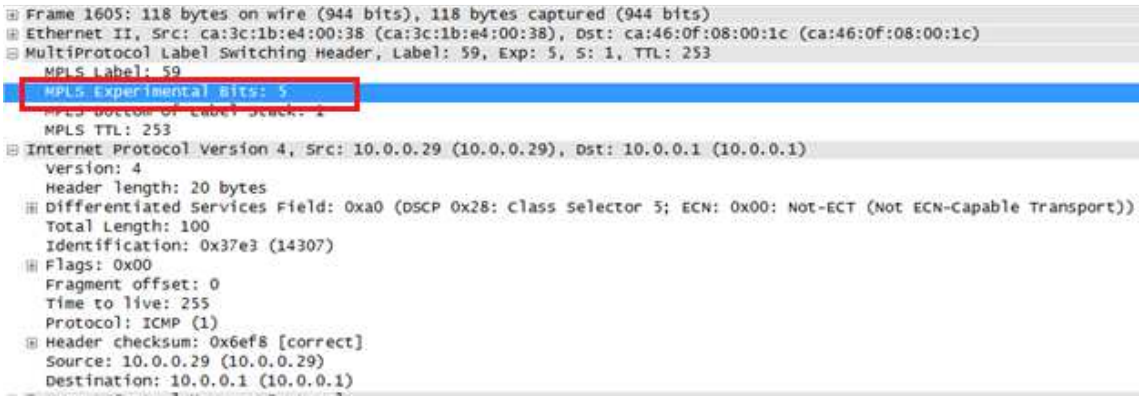


Figura 5.47: Captura en Wireshark que muestra el bit EXP en 5.

5.6.2 PRUEBAS DE CALIDAD DE SERVICIO (QoS) CON TRÁFICO DE VOZ Y TRANSFERENCIA DE ARCHIVOS (FTP)

El tráfico de voz se diferencia del de datos por la importancia del mismo ya que el usuario desea siempre ser escuchado y que le escuchen todo el tiempo, por lo que una falla en la red o saturación en el canal sin una QoS adecuada puede causar interrupciones o retardo en la comunicación.

Intermitencias y/o tiempos en el canal, pueden ser muchas de las veces imperceptibles en lo que a tráfico ftp se refiere, ya que con la política del mejor esfuerzo un paquete puede ser reenviado y al final el usuario recibirá la información completa.

5.6.2.1 Análisis de resultados

Para comprobar el funcionamiento correcto de la QoS aplicada en la interfaz que para este caso fue la política de servicio denominada "**rtp"** se utilizó una aplicación de SIP VoIP llamada linphone, la cual fue instalada en cada equipo terminal (PC) y estos conectados a la red MPLS.

Se realizó entonces una llamada desde un computador hacia el otro y se pudo evidenciar una comunicación eficaz, clara y sin cortes. Por la parte del análisis de tráfico se puede verificar en la figura 5.48 la precedencia y/o experimental bits que recibe el trafico rtp (5) para lograr una comunicación eficiente.

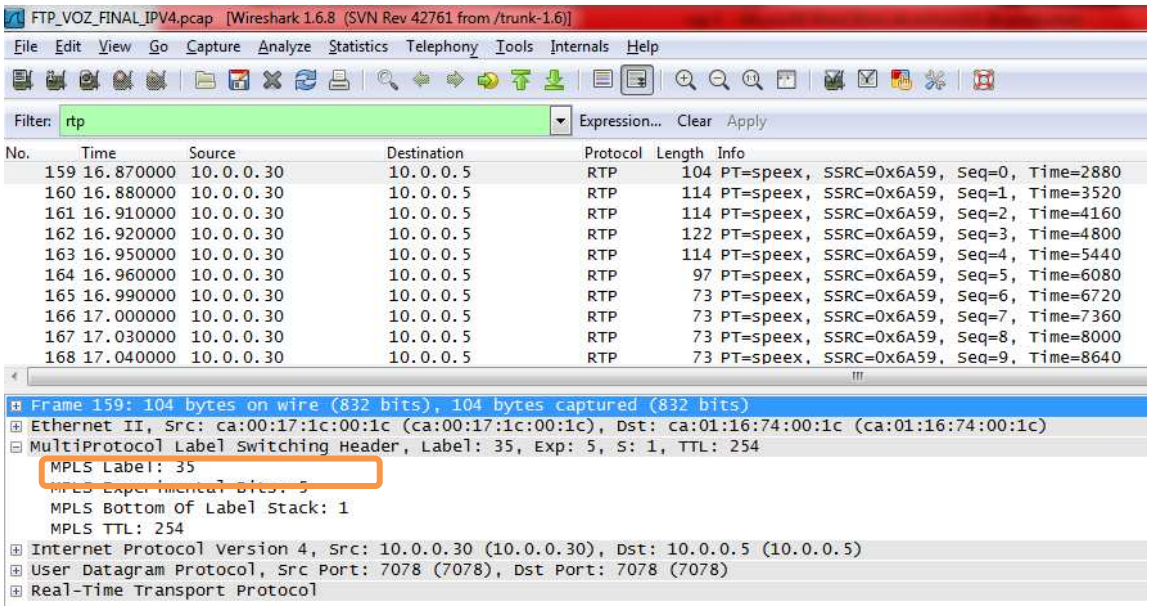


Figura 5.48: MPLS Exp Bit para tráfico de voz

Para generar tráfico ftp se utilizó un servidor ftp en un computador y en el otro se configuro el cliente; cabe indicar que tanto la llamada como una trasferencia de un archivo se la realizaron simultáneamente; de esta manera el trafico ftp obtuvo la prioridad más baja y se dio preferencia a la voz, pero esto no quiere decir que el archivo no se transfirió; el mismo llego a su destino exitosamente. En la figura 5.49 se muestra la captura de tráfico ftp en donde se evidencia el bit experimental en cero.

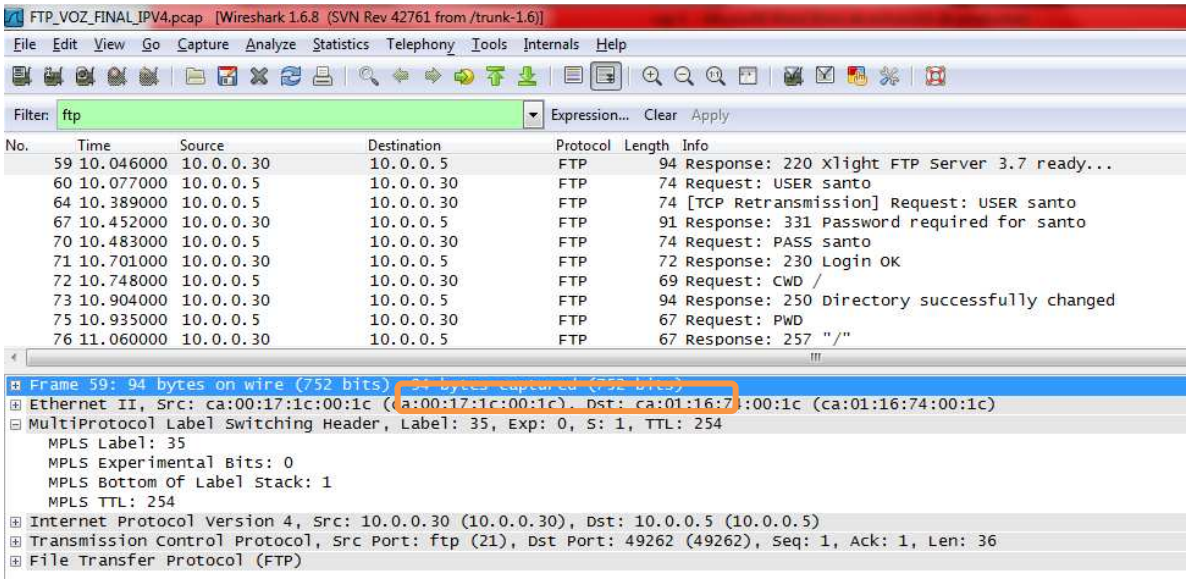


Figura 5.49: MPLS Exp Bit para tráfico ftp.

5.6.3 PRUEBAS DE CALIDAD DE SERVICIO (QoS) CON TRÁFICO ICMPv6

Se realizará las mismas pruebas que para IPV4 para poder analizar los resultados.

5.6.3.1 Objetivo

Para la comprobación de la QoS bajo este tipo de paquetes se presentan dos escenarios, el primero sin aplicar la calidad de servicio y el segundo en donde se crea una regla para poder emular tráfico de voz y garantizar un 100% de paquetes entregados a su destino.

- **Primer escenario:** se realizara una prueba de ping extremo – extremo sin la aplicación de políticas de QoS en la interfaz.

- **Segundo escenario:** aplicando la política de QoS llamada rtp nuevamente se ejecutara un ping extendido entre los dos extremos.

5.6.3.2 Análisis de resultados

Para el primer escenario se tiene un ping extendido entre dos puntos del cliente IPV6, a este tráfico no se le ha asignado ninguna calidad de servicio QoS y se tiene una eficiencia del 95%, en la figura 5.50 se observa el resultado del comando ping.

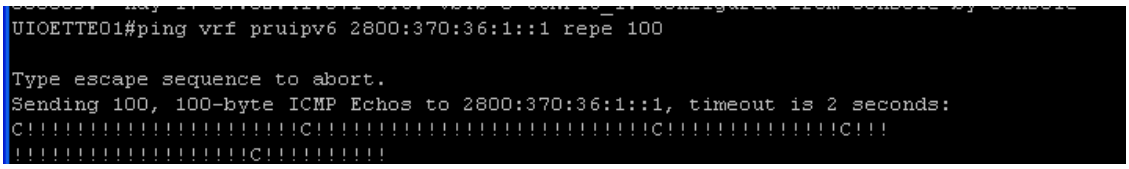


Figura 5.50: Ping con 95% de efectividad, sin QoS

Para efectos de prueba se creó una nueva regla en la clase de servicio, ésta se muestra en la figura 5.51; esta regla dará una precedencia de 5 a los paquetes

IPV6 por ende a nuestro ping, en la figura 5.52 se puede observar que se tiene una efectividad del 100%.

```
class-map match-any CM-Datosnocriticos
  match mpls experimental topmost 1  2
  match ip precedence 1  2
class-map match-all rtp
  match access-group name linphone
  match protocol ipv6
class-map match-all copp-class-filemanagement
  match access-group name copp-filemanagement
!
```

Figura 5.51: Nueva regla para la clase de servicio *rtp*

```
UIOETTE01#ping vrf pruipv6 2800:370:36:1::1 repe 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 2800:370:36:1::1, timeout is 2 seconds:
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 52/103/200 ms
UIOETTE01#
```

Figura 5.52: Ping con 100% de efectividad, con QoS

5.6.4 PRUEBAS DE CALIDAD DE SERVICIO (QoS) CON TRÁFICO DE VOZ Y TRANSFERENCIA DE ARCHIVOS (FTP) EN IPv6

5.6.4.1 Análisis de resultados

Para el tráfico de voz se usó el programa linphone, como se mencionó anteriormente; la política de servicio rtp asigna la precedencia de 5 a este tráfico, como se puede observar en la figura 5.53 al capturar los paquetes usando wireshark.

Para el tráfico ftp se siguió el mismo procedimiento que en IPV4, se hizo una captura mientras se realizaba una llamada y se puede observar la prioridad de tráfico que se asigna a cada tipo de paquete en la figura 5.54; 5 para VoIP y 0 para ftp.

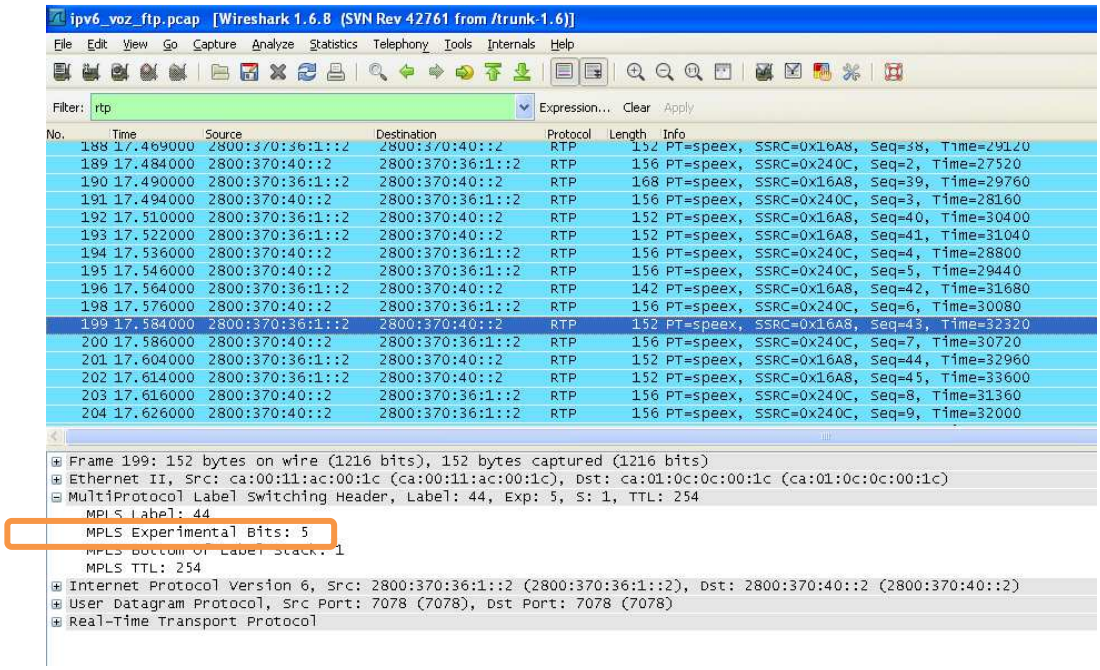


Figura 5.53: Tráfico de voz con prioridad 5

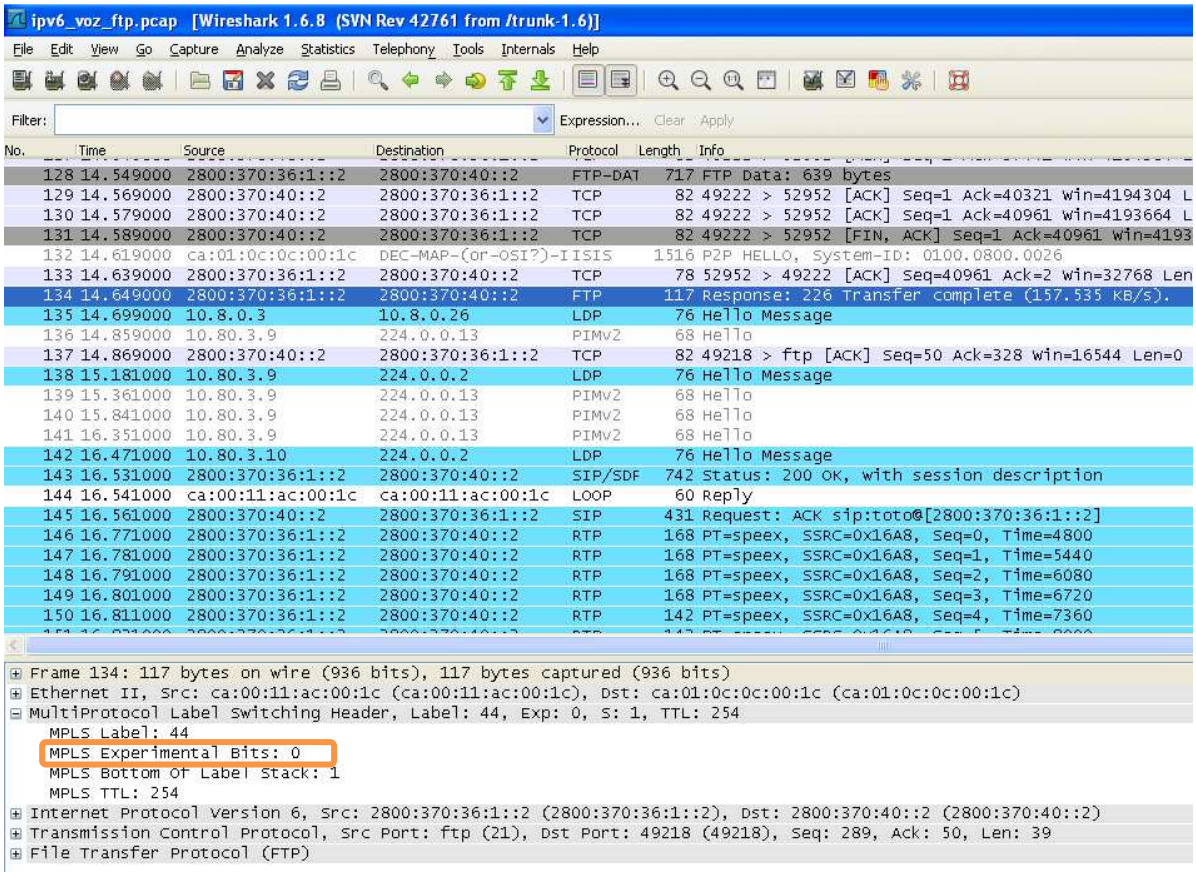


Figura 5.54: Tráfico de voz y ftp por un mismo canal, con su respectiva precedencia. Pg. 1 de 2

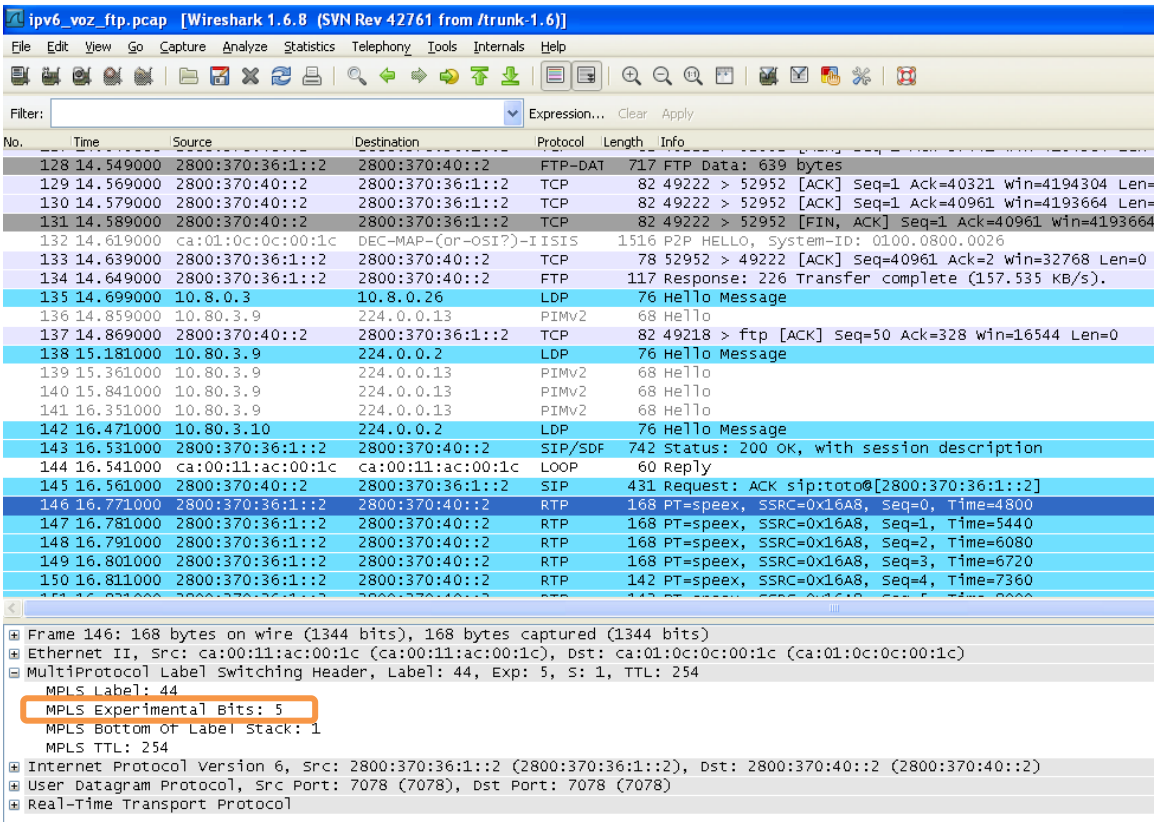


Figura 5.54: Tráfico de voz y ftp por un mismo canal, con su respectiva precedencia. Pg. 2 de 2.

5.8 VENTAJAS Y DESVENTAJAS DE LA MIGRACIÓN

5.8.1 VENTAJAS DE LA MIGRACIÓN

- La principal ventaja es el aumento de direcciones disponibles, también gracias al nuevo sistema de empaquetamiento hay una mejora en el direccionamiento permitiendo crear redes mucho más eficientes.
- Convivencia con IPV4, que hará posible un mínimo impacto e inversión.
- Disponibilidad de direcciones del tipo unicast multicast y anycast.
- Gran movilidad, nos permitirá cambiar de red sin perder conectividad.
- No se necesita ninguna actualización ni de hardware ni de software.

5.8.2 DESVENTAJAS DE LA MIGRACIÓN

- Se necesita extender un soporte continuo para IPV6.
- Se necesitan routers que realicen un tipo de NAT entre IPV6 e IPV4 cuando nuestro cliente IPV6 quiera comunicarse con la red IPV4.

- Para ciertas configuraciones de QoS es necesario rediseñar el método de aplicación de la misma.

5.9 IMPACTO SOBRE LA CALIDAD DE SERVICIO QoS

La QoS en IPV6 es muy similar a IPV4 a excepción de ciertos parámetros:

- IPV6 no soporta NBAR (Network-Based Application recognition), ciertamente porque es una aplicación basada en IPV4.
- No hay manera de coincidir directamente con paquetes **rtp**, es decir no existe la posibilidad de **match protocol rtp** para IPV6.
- IPV6 solo soporta listas de acceso que tengan nombre.
- IPV6 tiene un campo llamado Flow Label de 20 bits que identifica flujos específicos que necesitan un tratamiento especial de QoS.
- El campo Traffic Class de 8 bits indica que clases de paquetes específicos necesitan algún tratamiento especial de QoS, tiene el mismo significado que el ToS en IPV4. Esto quiere decir que se tiene un tratamiento de QoS en IPV6 y es compatible con IPV4.

5.9.1 QoS para IPV6 [5]

En la tabla 5.6 se hace una comparación de QoS para IPV4 e IPV6.

CARACTERÍSTICA	IPV4	IPV6
Differentiated Services (DiffServ)	SI	SI
Clasificación de paquetes	SI	SI
Conformado de tráfico	SI	SI
Políticas en tráfico	SI	SI
Marcado de paquetes	SI	SI
Encolado	SI	SI
(WRED)-based drop	SI	SI
Compressed Real-Time Protocol	SI	NO
NBAR	SI	NO
Committed access rate	SI	NO
Priority queueing	SI	NO
Custom queueing (CQ)	SI	NO

Tabla 5.6: Comparativa de QoS para CISCO

REFERENCIAS BIBLIOGRÁFICAS CAPÍTULO 5

LIBROS

[1] **Shannon**. *“Introduction to the art and science of simulation”.* 1989.

[2] Teerawat, **Issariyakul**; Ekram, **Hossain**. *“Introduction to Network Simulator NS2”.* 2009.

PDF, RFC, PAPERS

[3] **ANÓNIMO**. *”OPNET: Manual de Usuario”*. Universitat Politécnica de Catalunya. 2004.

[4] **ANÓNIMO**. *”Packet Tracer 5.0”* Cisco. 2009.

[5] **ANÓNIMO**. *”Configuring IPV6”*. Cisco. 2010.
URL:http://www.cisco.com/en/US/docs/storage/san_switches/mds9000/sw/rel_3_x/configuration/guides/cli_3_4_x/ipv6.html

INTERNET

[6] Jack **Hughes**. *“Network Simulation”* el Viernes 20/09/2009 – 14:15 **URL:** http://www.openxtra.co.uk/articles/networksimulation Consultado el 14 de Octubre de 2013

[7] **ANÓNIMO**. *“Introduction to GNS3”*
URL: http://www.gns3.net/gns3-introduction/
Consultado el 14 de Octubre de 2013

[8] **ANÓNIMO**. *“Packet Tracer, features”*
URL: http://www.packettracer.info/ packet-tracer-5-3-features.html
Consultado el 17 de Octubre de 2013

CAPÍTULO 6

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- La posibilidad del uso de simuladores de red nos permite optimizar nuestras redes y realizar pruebas prácticas antes de poner en funcionamiento un esquema final.
- La versión actual del protocolo de internet (IPV4), es ampliamente usado. Es fácil de implementar, robusto y soporta un gran número de aplicaciones. Sin embargo, el gran crecimiento de internet y la necesidad del uso de más y más direcciones IP en servicios de internet y las aplicaciones, han creado deficiencias como la falta de direcciones IPV4, esto quiere decir que cada vez se tiene más dispositivos que necesitan direcciones IP, lo que conlleva a un agotamiento de las mismas.
- IPV6 es la siguiente generación de protocolo de internet, que ofrece más direcciones IP y solucionará el problema de agotamiento de direcciones IPV4 en una forma paulatina.
- Los proveedores de servicios y empresas que han estado usando MPLS, deben ver a la integración de servicios IPV6 sobre la MPLS como una evolución normal. El backbone de la MPLS puede ser usado para conectar islas IPV6.
- Un ambiente de simulación correcto, nos permite analizar el comportamiento de una red, pero no nos permite desarrollarlo a su máxima capacidad ya que depende del computador sobre el que se corra la simulación.
- Actualmente el mayor problema es la incompatibilidad entre IPV4 e IPV6. Muchas de las aplicaciones existentes no pueden ejecutarse en equipos que sean solo IPV6. Esto debido a que las aplicaciones necesitan invocar a la función de socket durante la inicialización del programa, este parámetro difiere en IPV6 e IPV4 y debe ser considerado por el programador.

- La situación actual de la CNT EP permite usar 6VPE como método óptimo de migración, obteniendo un mínimo impacto en la red y con el costo mínimo, esto debido a que todos los equipos sobre los que se realizó el estudio soportan IPV6 y las configuraciones necesarias para 6VPE.
- 6VPE ofrece un mayor nivel de seguridad que 6PE. Esto debido a que 6VPE crea túneles seguros entre clientes, mientras que 6PE no lo hace.
- La Qos no se afecta después de la migración, la forma de implementación cambia, se debe manejar con diferentes ACLs. De acuerdo con la red de CNT EP se debe crear nuevas listas de acceso indicando las IPs y puertos a los cuales se les debe brindar QoS.

6.2 RECOMENDACIONES

- Al conectar una PC a GNS3 a través de una MS Loopback, se debe ingresar el comando **ipv6 nd ra suppress,** esto desactivará el modo de asignación dinámica de dirección IP y nos permitirá realizar las pruebas necesarias.
- Se recomienda usar esta simulación para cualquier prueba de QoS sobre la MPLS de la CNT EP, sea ésta sobre IPV6 o IPV4.
- Para pruebas futuras, si no se dispone de un servidor de alta capacidad, se recomienda simular solo cierta parte de la red con todos sus routers, por ejemplo Mariscal; con esto se pueden verificar los servicios a una escala menor.
- Para una simulación a una escala mayor, se recomienda usar un servidor con las características mínimas que son: procesador de 4 núcleos, 8 GB de RAM y 2 tarjetas Ethernet. Esto debido a que GNS3 usa muchos recursos en donde esté instalado.
- Se recomienda manejar de igual manera el tráfico de servicios tanto en IPV4 como en IPV6; actualmente CNT separa en VRFs el tráfico de voz, IPTV, datos, etc. Esto ayudará a la gestión de la red.
- Al usar GNS3 se recomienda asignar un IDLE PC cuando se tengan encendidos los routers con los cuales se va a trabajar, así se asignará un

valor adecuado de acuerdo al trabajo que se esté realizando y no se sobrecargará la PC donde se esté trabajando.

- Antes de ejecutar la simulación se recomienda modificar el archivo **topology.net** de acuerdo a la máquina donde se simule, especificando los paths de donde se tomará los archivos de configuración.
- Para usar IPV6 se recomienda usar el IOS de cisco c7200-adventerprisek9-mz.122-33.SRC1.bin, ya que éste da soporte para IPV6 y todos los recursos usados en este proyecto.
- Si CNT realiza una migración a mayor escala se recomienda tener un plan de direccionamiento para cada cliente y crear un sistema autónomo para la parte referente a IPV6.
- Para la implementación real a clientes finales, se recomienda usar VLANs para cada servicio al igual que en IPV4.

ANEXOS

ANEXO 1, Scripts Utilizados

ANEXO 2, Red MPLS Pichincha en A3

ANEXO 3, Manual de configuración de IPV6

ANEXO 4, Manual de Linphone

ANEXO 5, Datasheet equipos CISCO