ANÁLISIS DEL RENDIMIENTO DE UNA RED MPLS CON CALIDAD DE SERVICIO MEDIANTE SIMULADOR GNS3

Autor:
José Escalona

Urb. Yuma II, calle No 3. Municipio San Diego

Teléfono: (0241) 8714240 (máster) – Fax: (0241) 8712394

REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSÉ ANTONIO PÁEZ

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA EN TELECOMUNICACIONES

ANÁLISIS DEL RENDIMIENTO DE UNA RED MPLS CON CALIDAD DE SERVICIO MEDIANTE SIMULADOR GNS3

Trabajo de grado presentado como requisito para optar al título de

INGENIERO EN TELECOMUNICACIONES

Autor:
José Escalona
C.I: V-24.662.745
Tutor:
Ing. Rainier Blanco
C.I: V-11.556.607

San Diego, Enero de 2019

FI-T-008-2019-ICR

Valencia, 21 de Marzo de 2019

Ciudadano:
José Escalona
C.I: 24.662.725
Presente-

Cumplo con informarle que la Comisión de Trabajo de Grado y Pasantías de la Facultad de Ingeniería en su reunión **N° 01-2019** de fecha **21-03-2019** aprobó el proyecto de trabajo de grado titulado **ANÁLISIS DEL RENDIMIENTO DE UNA RED MPLS CON CALIDAD DE SERVICIO MEDIANTE SIMULADOR GNS3** Presentado por usted como requisito para optar al título de Ingeniero en Telecomunicaciones.

Se ratifica la designación del Ing. Rainier Blanco, C.I: 11.556.607 y la Ing. Alicia De Pizzella, C.I: 4.598.880 como Tutores Académicos que lo asesorarán en el desarrollo de este proyecto.

Atentamente,

Facultad de Ingeniería UJAP DECANATO

Prof. Luís [illegible]
Decano de la Facultad de Ingeniería

c.c. Coordinación de Pasantías y Trabajo de Grado (1).
LI/lc.

REPÚBLICA BOLIVARIANA DE VENEZUELA

UNIVERSIDAD JOSÉ ANTONIO PÁEZ

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA EN TELECOMUNICACIONES

ACEPTACIÓN DEL TUTOR

Quien suscribe, Ingeniero **Rainier Blanco** portador de la cédula de identidad N° **11.556.607**, en mi carácter de tutor del trabajo de grado presentado por el(los) ciudadano(s) **José Escalona**, portador(es) de la cédula de identidad N° **24.662.745**, (respectivamente), titulado **ANÁLISIS DEL RENDIMIENTO DE UNA RED MPLS CON CALIDAD DE SERVICIO MEDIANTE SIMULADOR GNS3.** Presentado como requisito parcial para optar al título de Ingeniero de Telecomunicaciones, considero que dicho trabajo reúne los requisitos y méritos suficientes para ser sometido a la representación pública y evaluación por parte del jurado examinador que se designe.

En San Diego, a los 27 días del mes de mayo del año dos mil diecinueve.

Ing. Rainier Blanco

C.I.: V- 11.556.607

AGRADECIMIENTOS

José Ramón Escalona San Blas

Inicialmente agradezco a Dios por permitirme lograr todo lo que hoy en día he logrado, a mi familia por apoyarme en cada etapa de mi carrera. A mi madre y padre por siempre estar allí conmigo dándome ánimos para seguir adelante. A mi abuela Maria Teresa por ser mi guía durante toda mi vida.

A mí mismo por lograr este trabajo, y a mi tutor Rainier Blanco por guiarme y orientarme a lo largo de este proyecto.

ÍNDICE GENERAL

INDICE DE FIGURAS

ÍNDICE DE TABLAS

REPÚBLICA BOLIVARIANA DE VENEZUELA
UNIVERSIDAD JOSÉ ANTONIO PÁEZ
FACULTAD DE INGENIERÍA
ESCUELA DE INGENIERÍA EN TELECOMUNICACIONES

RENDIMIENTO DE UNA RED MPLS CON CALIDAD DE SERVICIO MEDIANTE SIMULADOR GNS3

Autor: José Escalona
Tutor: Ing. Rainier Blanco
Fecha: 2019

RESUMEN

Con referencia a la informática y la telecomunicación, un protocolo de comunicaciones es el conjunto de reglas y estándares que tienen como fin controlar las secuencias de los mensajes que suceden en una comunicación entre las entidades que forman parte de una misma red. Desde el punto de vista tecnológico, todo el mundo está conectado mediante la infraestructura de redes basadas en el Protocolo de Internet (Protocolo IP por sus siglas en inglés), surge un nuevo protocolo para el transporte e enrutamiento de datos que se puede aplicar independiente del medio por donde se van a enviar los datos, es decir, se implementa entre la capa 3 (capa de red) y capa 2 (capa de enlace de datos) del modelo OSI y recibe el nombre de Multiprotocolo de Conmutación de Etiquetas (MPLS por sus siglas en inglés). Por lo que es necesario estudiar a fondo este protocolo ya que actualmente los programas de estudio orientados a la enseñanza de protocolos en redes de comunicaciones no contemplan las redes basadas en MPLS. En tal sentido la investigación tiene como objetivo Analizar el rendimiento de una red MPLS con calidad de servicio mediante simulador GNS3. La metodología q se pretende usar se encuentra enmarcada en el paradigma cuantitativo con un diseño experimental de tipo descriptivo, con nivel de campo. Utilizando la técnica de observación directa para recoger los datos, utilizando como instrumento la lista de cotejo.

Descriptores: Red MPLS, Multiprotocolo, simulador GNS3, infraestructura de redes

INTRODUCCIÓN

A nivel mundial, la popularidad de internet desde su nacimiento se ha incrementado a tal punto que en la actualidad, las nuevas generaciones no conciben el mundo sin su uso constante. Esto ha traído como resultado un acelerado ritmo en el crecimiento de las redes de datos.

La demanda establecida, genera cambios constantes para satisfacer las necesidades de los consumidores. De allí el desarrollo de la tecnología MPLS (**Multiprotocol Label Switching** o Protocolo de conmutación de etiquetas), creada para redes de nuevas aplicaciones que interactúa con otros protocolos como el de la calidad de servicios para generar entornos de mayor fiabilidad, acortando distancias geográficas mientras se incrementa el rendimiento y la calidad de las redes.

Desde el punto de vista tecnológico, todo el mundo está conectado mediante la infraestructura de redes basadas en el Protocolo de Internet (Protocolo IP por sus siglas en inglés), surge un nuevo protocolo para el transporte e enrutamiento de datos que se puede aplicar independiente del medio por donde se van a enviar los datos, es decir, se implementa entre la capa 3 (capa de red) y capa 2 (capa de enlace de datos) del modelo OSI y recibe el nombre de Multiprotocolo de Conmutación de Etiquetas (MPLS por sus siglas en inglés). Por lo que es necesario estudiar a fondo este protocolo ya que actualmente los programas de estudio orientados a la enseñanza de protocolos en redes de comunicaciones no contemplan las redes basadas en MPLS

En este orden de ideas, se presenta la siguiente investigación, que busca analizar el rendimiento de una red MPLS con calidad de servicio mediante el simulador GNS3 para entender el comportamiento de las redes que usan el protocolo y la capacidad de las redes para proveer diferentes niveles de servicio. El actual trabajo está estructurado de la siguiente manera:

En el Capítulo I, se muestra el planteamiento y formulación del problema que explica la situación actual observada por el investigador y bajo la cual se estructuran

los objetivos que guiaron el trabajo. Así mismo se presenta la justificación y alcance del proyecto

En el Capítulo II, se presenta el marco teórico que fundamenta la investigación, mostrando trabajos previos que anteceden y dan luces al proyecto, seguido por el marco teórico que explica los protocolos y terminologías propias del problema planteado.

Seguidamente, el Capítulo III, muestra el accionar metodológico que oriento la investigación para el cumplimiento de los objetivos planteados a través del desarrollo del tipo de investigación, diseño y nivel, así como las técnicas e instrumentos de recolección de información que brindaran los datos necesarios para dar respuesta a los objetivos.

El capítulo IV, se refiere y muestra los resultados obtenidos una vez que se aplicó la herramienta de simulación GNS3 y se estudió la red

Finalmente, se presentan las conclusiones y recomendaciones.

CAPÍTULO I
EL PROBLEMA

1.1 Planteamiento del Problema

Con referencia a la informática y la telecomunicación, un protocolo de comunicaciones es el conjunto de reglas y estándares que tienen como fin controlar las secuencias de los mensajes que suceden en una comunicación entre las entidades que forman parte de una misma red. Los teléfonos o los ordenadores son algunos ejemplos de estas comunicaciones.

Ahora bien, con el crecimiento tecnológico y con el desarrollo de las telecomunicaciones se depende de plataformas digitales, que permiten hacer más eficientes los procesos, obtener mayor cantidad de información de los clientes y disponer de la flexibilidad y agilidad que se requiere en un entorno cada vez más competitivo. El mismo se logra a través de la implementación de técnicas y protocolos, lo cual permite adaptarse a las crecientes tecnologías en el área de telecomunicaciones.

Cabe destacar que , “Desde el punto de vista tecnológico, todo el mundo está conectado mediante la infraestructura de redes basadas en el Protocolo de Internet (Protocolo IP por sus siglas en inglés), el nuevo lenguaje universal de las comunicaciones convergentes digitales que revolucionó la informática y su capacidad de transferir datos”(Palma,2014, pág. 172).

Antes lo anterior descrito, la tecnología IP se usaba de forma educativa en las universidades y no era implementada como un medio de transmisión de datos, pero existían redes de comunicación basadas en Modo de Transferencia Asíncrona (ATM por sus siglas en inglés) y Frame Relay para el envío masivo de datos en una red, las cuales se usan en la actualidad. Muchas empresas hoy en día tienen implementados estos tipos de redes, por lo cual se ha convertido en un reto emigrar a nuevas

tecnologías como es IP la cual sustituye estas dos tecnologías de transporte de datos, ya sea por el alto costo del cambio de los equipos, la logística a implementar o no querer emigrar a otra tecnología por la fiabilidad que le ofrece ATM o Frame Relay a una empresa.

Debido a los factores antes descritos, surge un nuevo protocolo para el transporte e enrutamiento de datos que se puede aplicar independiente del medio por donde se van a enviar los datos, es decir, se implementa entre la capa 3 (cada de red) y capa 2 (capa de enlace de datos) del modelo OSI y recibe el nombre de Multiprotocolo de Conmutación de Etiquetas (MPLS por sus siglas en inglés). Por lo que es necesario estudiar a fondo este protocolo ya que actualmente los programas de estudio orientados a la enseñanza de protocolos en redes de comunicaciones no contemplan las redes basadas en MPLS, tecnología usada hoy en día para el transporte de datos de redes de alta velocidad, siendo una desventaja en la formación académica del futuro egresado en ingeniería de telecomunicaciones.

Sobre la base de las ideas expuestas, surge la necesitada de desarrollar un simulador con MPLS para entender el comportamiento de las redes que usan el protocolo. Además las redes MPLS usan parámetros de Calidad de Servicio (QoS por sus siglas en ingles), la cual se define como capacidad que tiene una red de proveer diferentes niveles de servicio para asegurar distintos perfiles de tráfico para mejorar el rendimiento de una red de transporte de datos.

Partiendo de todo lo anterior expuesto, es necesario comprender el desempeño de una red que usa MPLS más QoS a través de la simulación.

1.2 Formulación del Problema.

Con el objetivo de dar cumplimiento a las expectativas planteadas en el párrafo anterior el investigador se preguntan:

¿Cuál es el rendimiento y comportamiento de una red MPLS con calidad de servicio según el simulador GNS3?

1.3 Objetivos de la Investigación

1.3.1 Objetivo General

Analizar el rendimiento de una red MPLS con calidad de servicio mediante simulador GNS3

1.3.2 Objetivos Específicos

- Estudiar los fundamentos de MPLS en cuanto a estructura y diseño de red.
- Determinar los parámetros de calidad de servicio aplicables a una red basada en MPLS.
- Aplicar el simulador GNS3 a las redes basadas en MPLS con calidad de servicio.
- Determinar los parámetros de desempeño y el rendimiento de una red MPLS con calidad de servicio.

1.4 Justificación

Si bien es cierto, estamos en un mundo con un crecimiento tecnológico cada vez más rápido por tanto las redes de comunicaciones deben adaptarse a esos cambios, es así que surge MPLS, el cual ofrece flexibilidad para entregar y enrutar tráfico en caso de fallas de enlace, congestión, cuello de botella y mejorar la calidad de servicio.

Sin embargo para entender dicha tecnología se requiere de personal capacitado que maneje la gestión de redes no solo dentro de las empresas de telecomunicaciones, sino también en las universidades.

Es por esta razón que el presente trabajo se enfoca en estudiar y explicar la tecnología MPLS con factores de calidad de servicio, sus conceptos, sus aplicaciones, sus ventajas y sus beneficios a través de una adecuada herramienta de simulación, demostrando de esta manera que el conocimiento se afianza con la práctica.

1.5 Alcance

Con esa finalidad, este trabajo de investigación se simulará una red MPLS con calidad de servicio por medio de un simulador con parámetros reales, con la finalidad

de lograr emular las características de la misma y entender y comprender el desempeño y/o comportamiento de una red real.

CAPÍTULO II
MARCO TEÓRICO

2.1 Antecedentes de la Investigación

La investigación **Análisis y mejora de la red de datos de la UNSAAC sobre la plataforma IP-MPLS en un banco de pruebas,** realizada por Moreno y Quispe (2017) en Universidad Nacional de San Antonio Abad del Cusco, Facultad de Ingeniería Eléctrica, Electrónica, Informática y Mecánica, Escuela Profesional de Ingeniería Electrónica propone el diseño e integración de una red IP-MPLS para la Universidad Nacional San Antonio Abad del Cusco, que atenderá las necesidades requeridas y mejoras en el servicio a los usuarios, el autor se propone como objetivo principal Analizar y proponer la red IP-MPLS para mejorar la red de datos en la UNSAAC, que permita ofrecer diferentes niveles de servicio en un entorno de mayor fiabilidad y el transporte de un tráfico óptimo.

Durante el desarrollo de esta tesis se realiza la simulación global de toda la arquitectura de red propuesta en el software GNS3 y una pequeña muestra de simulación con equipos reales; se definen escenarios de redes IP; a los cuales serán sometidos a diversos tráficos; se evaluaran los comportamientos resultantes de la interacción con estos tráficos y se comprobará el funcionamiento de esta alternativa tecnológica para proporcionar QoS, Ingeniería de Tráfico, transmisión óptima de información, uso de recursos de red, entre otras características que son de interés. Finalmente se realizó el análisis de costo beneficio que permitió determinar el precio de implementar la red propuesta de dicha investigación.

El autor, llega a una serie de conclusiones parciales, destacando su conclusión general donde afirma que una vez analizados e interpretados los resultados arrojadas por los instrumentos de recolección de datos aplicados, se obtuvo como resultados la fiabilidad en acceso a la red de nuestros usuarios, la red garantiza un crecimiento a futuro a nivel físico y lógico, seguridad en la red y fácil administración. Así mismo el método de balancear la carga del tráfico mediante el protocolo BGP y políticas de

servicio creados, escogiendo la mejor ruta para su destino; adecuar la comunicación y petición a mayor intensidad en la INTRANET aprovechando la abundante información académica de la UNSAAC.

Por otro lado, Crow Sanchez (2016) en su investigación titulada **Análisis de calidad de servicio en transferencia de voz y video en una red de tecnología MPLS (MULTI-PROTOCOL LABEL SWITCHING)** presentada ante la Escuela Superior Politécnica de Chimborazo, Faculta de Informática y Electrónica; Ingeniería En Electrónica, Telecomunicaciones y Redes en Ecuador, el autor diseñó e implemento una *red Multiprotocol Label Switching* (MPLS) para realizar el análisis de calidad de servicio al transferir audio y video, realizado con equipos CISCO en los laboratorios de la academia CISCO. Estableciendo como objetivo general Analizar la calidad de servicio en la transferencia de voz y video en una red de tecnología MPLS (Multi-Protocol label switching).

Este autor llega a la conclusión que las pruebas realizadas en los laboratorios cisco de la Escuela Superior Politécnica de Chimborazo demostró un 66,66% en el trafico tanto para voz y video a consideración del 50% de los valores máximos recomendados por la UIT-T G.1010, Y.1541, IEEE 802.1p, concluyendo que se obtuvo una mejora del 16,66% con la arquitectura de red MPLS utilizando VRF para aislar el tráfico de tiempo real con el trafico externo que este caso fue TCP lo cual demostró un nivel eficiente en la evaluación comparando con los valores máximos recomendados UIT-T G.1010, Y.1541, IEEE 802.1p.

Seguidamente explica que la tecnología de las telecomunicaciones evolucionan constantemente es por eso que cada vez existen nuevas y mejores maneras de asegurar la calidad de servicio y más aún en aplicaciones de audio y video. Lo cual se propone investigar sobre IGMPLS que son redes de fibra óptica. Redes con servicios diferenciados que den prioridad a los paquetes más críticos como los de en tiempo real.

Finalmente Castro (2015) realizó la investigación llamada **Diseño y simulación de una Red MPLS para interconectar estaciones remotas utilizando el Emulador GNS3**, presentada en la Universidad Politécnica Salesiana de Guayaquil, donde establece como objetivo entender la tecnología MPLS, mediante un diseño que

simule la implementación de una red que interconecte estaciones remotas de una empresa X, describiendo claramente las ventajas y beneficios.

La autora explica que la simulación en GNS3 ayudará a interactuar con los diferentes equipos, protocolos, topología y configuraciones que se utilizan en tiempo real, los cuales podrían ser aplicaciones en componentes reales, sin obtener ningún inconveniente al momento de conectarlos, instalarlos y programarlos tal cual se realizó en la simulación.

Esta autora concluye que después de implementar el diseño en el simulador, el protocolo MPLS este presenta varios beneficios para empresas puesto que su servicio de calidad y su ingeniería de tráfico disminuye notablemente el tráfico de una red. Además, dicho protocolo soporta nuevos servicios que las redes IP convencionales no hacen, in mencionar que funciona en cualquier tecnología de transporte.

2.2 Bases Teóricas

2.2.1 Redes de comunicaciones

Una red de comunicaciones es un conjunto de medios técnicos que permiten la comunicación a distancia entre equipos autónomos (no jerárquica -master/slave-). Normalmente se trata de transmitir datos, audio y vídeo por ondas electromagnéticas a través de diversos medios (aire, vacío, cable de cobre, fibra óptica, entre otros.). La información se puede transmitir de forma analógica, digital o mixta, pero en cualquier caso las conversiones, si las hay, siempre se realizan de forma transparente al usuario, el cual maneja la información de forma analógica exclusivamente. Las redes más habituales son las de ordenadores, las de teléfono, las de transmisión de audio (sistemas de megafonía o radio ambiental) y las de transmisión de vídeo (televisión o vídeo vigilancia).

- **Componentes básicos de las redes**

Para formar una red se requieren elementos:

1. Hardware (equipos físicos electrónicos).
2. Software (programas) y protocolos de red.

Los elementos físicos se clasifican en dos grandes grupos: dispositivos de usuario final (hosts) y dispositivos de red. Los dispositivos de usuario final incluyen los computadores, impresoras, escáneres, y demás elementos que brindan servicios directamente al usuario y los segundos son todos aquellos que conectan entre sí a los dispositivos de usuario final, posibilitando su intercomunicación.

El fin de una red es la de interconectar los componentes hardware de una red, y por tanto, principalmente, las computadoras individuales, también denominados hosts, a los equipos que ponen los servicios en la red, los servidores, utilizando el cableado o tecnología inalámbrica soportada por la electrónica de red y unidos por cableado o radiofrecuencia. En todos los casos la tarjeta de red se puede considerar el elemento primordial, sea ésta parte de un ordenador, de un conmutador, de una impresora, u otro dispositivo, sea de la tecnología que sea (Ethernet, wifi, entre otros.).

2.2.2 Modelos de Referencia.

- **Modelo OSI**

Interconexión de Sistemas Abiertos (OSI por sus siglas en inglés) es el modelo de referencia para la descripción de las arquitecturas de redes (conjunto de capas y protocolos de red), aunque raramente se ha implementado por completo. Su objetivo es conseguir que un conjunto heterogéneo de equipos autónomos (no jerárquico -master/slave-) comunicados por medios de baja calidad también heterogéneos, aparezca ante el usuario como un medio homogéneo y fiable. (Ver figura 1)

- **Modelo TCP/IP**

Protocolo de Control de Transmisión Y Protocolo de internet (TCP/IP por sus siglas en inglés), este modelo no está orientado a la conexión entre equipos, sino a la interconexión de redes que ya están implementadas en origen, por tanto no pretende competir con el modelo OSI, sino implementar una parte de sus niveles. (Ver figura 1)

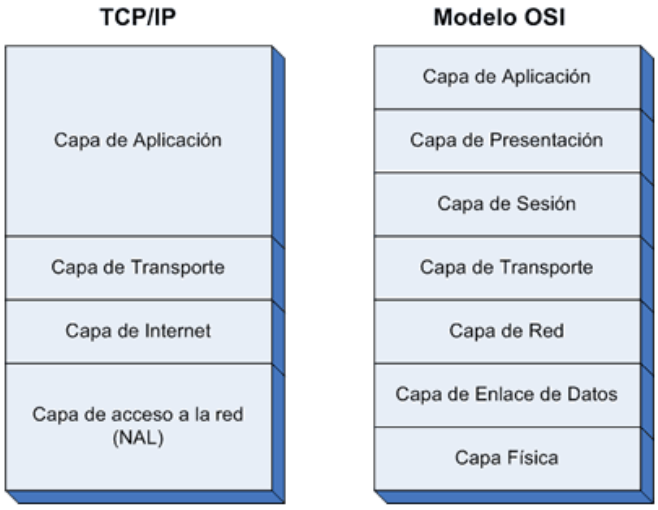


Figura 1. Diagrama de bloques de modelo TCP/IP y modelo OSI.

Fuente: "Redes de comunicaciones",
RedIRIS (2009).

Así el conjunto TCP/IP no hace ninguna referencia al nivel de usuario ni al nivel físico, sino únicamente al nivel de **enrutamiento** entre redes (protocolo IP) y al de transporte (por medio de los protocolos TCP y UDP). Sin embargo en la práctica la gran mayoría de redes, y en concreto Internet, se basan en IP para generar redes, es decir para conectar equipos, complementando TCP-UDP/IP con protocolos a nivel de usuario "por arriba" y a nivel físico "por debajo", generando una pila de protocolos conocida como familia de protocolos de Internet o modelo Internet.

2.2.3 Enrutamiento

Cada nodo intermedio de una comunicación debe conocer dónde ha de enviar el paquete que ha recibido. En el caso de los circuitos (conmutados o virtuales) solo se toma la decisión en el inicio de la conexión. En el caso de paquetes conmutados (datagramas) se toma la decisión con cada paquete. Este proceso de decisión se denomina enrutamiento.

La solución más sencilla pero ineficaz es enviar el paquete por todos los interfaces menos por el que llegó (inundación). Es el funcionamiento de los concentradores. Este sistema no se considera un protocolo de **enrutamiento**. Para

enrutadores (routers) sencillos se puede utilizar configuraciones estáticas de **enrutamiento**. Los encaminadores más modernos permiten utilizar auténticos protocolos de **enrutamiento** dinámico que sirven para intercambiar información entre encaminadores y adaptarse a situaciones cambiantes de tráfico basándose en:

- Capacidad del enlace.
- Tráfico medio.
- Retardo.
- Fiabilidad.

Las técnicas básicas son:

- Vector de distancia: cada encaminador mantiene una tabla con las distancias mínimas hacia cada posible destino y el interfaz de salida. Le pasa esta información a todos sus vecinos. Tiene el problema de la cuenta a infinito.
- Estado de enlace: identifica a sus vecinos y su coste y manda esa información a todos los encaminadores de la red. Con esa información se calcula el mapa de la red. Debido a que los protocolos de **enrutamiento** no son escalables se utiliza **enrutamiento** jerárquico. Esto simplifica el intercambio de información aunque puede no aprovechar todos los caminos mínimos.

Cada nodo intermedio de una comunicación puede utilizar variantes de dos técnicas de reenvío:

- Store-and-forward: almacena completamente el paquete y luego, si es correcto, lo reenvía.
- Cut-througth: conforme recibe el paquete, y una vez que sabe porque puerto lo tiene que reenviar, empieza su retransmisión. Si después el paquete resulta erróneo se propaga el error al siguiente nodo. Esta técnica es más rápida y sencilla para redes fiables.

Ø **Tipo de enrutamientos.**

Las redes requieren que la posibilidad de conexión entre sitios sea óptima. La posibilidad de conexión de una red remota es proporcionada por los routers y los

switches de capa 3 que operan en las capas de distribución y de núcleo, como se muestra en la Imagen 2. Los routers y los switches de capa 3 descubren las redes remotas de una de las dos maneras siguientes:

- **Manualmente:** Las redes remotas se introducen manualmente en la tabla de rutas por medio de rutas estáticas.
- **Dinámicamente:** Las rutas remotas se descubren automáticamente por medio de un protocolo de enrutamiento dinámico, como el Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado (EIGRP por sus siglas en inglés) o el Protocolo Primer Camino Más Corto (OSPF por sus siglas en ingles).

2.2.4 Métrica.

Cada protocolo de enrutamiento computa o calcula una métrica, que es un valor que representa la "dificultad" o el "costo" para llegar a una ruta de destino. Si un router tiene dos caminos hacia la misma red, sólo pondrá en la tabla de enrutamiento a aquella que tenga mejor métrica (menor costo). La única excepción es cuando los dos caminos tienen exactamente la misma métrica, en ese caso se agregarán ambos caminos a la tabla de enrutamiento.

2.2.5 Distancia Administrativa.

La distancia administrativa es el primer criterio que un router utiliza para determinar qué protocolo de ruteo utilizar si dos protocolos proporcionan información de ruta para el mismo destino, la cual mide la fiabilidad de la fuente de la información de ruteo. La distancia administrativa tiene importancia local solamente y no se publica en actualizaciones de ruteo.

Cuanto más bajo sea el valor de la distancia administrativa, más confiable será el protocolo. Por ejemplo, si un router recibe una ruta a cierta red de Primer Camino Más Corto (OSPF por sus siglas en inglés) con distancia administrativa predeterminada: 110 y de Protocolo de enrutamiento de puerta de enlace interior (IGRP por sus siglas en inglés) con una distancia administrativa predeterminada: 100,

el router optará por IGRP porque es más confiable. Esto significa que el router agrega la versión de la ruta de IGRP a la tabla de enrutamiento.

2.2.6 Protocolos de enrutamiento y sistemas autónomos.

Un sistema autónomo (AS por sus siglas en inglés) se trata de un conjunto de redes IP y routers que se encuentran bajo el control de una misma entidad (en ocasiones varias) y que poseen una política de **enrutamiento** similar a Internet. Dependiendo de la relación de un router con un AS, encontramos diferentes clasificaciones de protocolos como lo son Protocolo de Pasarela Interior (IGP por sus siglas en ingles) y Protocolo de Pasarela Exterior (EGP por sus siglas en inglés).

- **Tipos de AS**

Los sistemas autónomos pueden agruparse en tres categorías, dependiendo de sus conexiones y modo de operación.

- AS stub: se conecta únicamente con un AS.
- AS de tránsito: se conecta con varios AS y además permite que se comuniquen entre ellos.
- AS multihomed: Se conecta con varios AS, pero no soporta el tráfico de tránsito entre ellos

2.2.7 IGPs

IGPs intercambian información de **enrutamiento** dentro de un único sistema autónomo. (Ver figura 2). Los ejemplos más comunes son:

- IGRP: la diferencia con la RIP es la métrica de enrutamiento.
- EIGRP: es un protocolo de enrutamiento vector-distancia y estado de enlace.
- OSPF: enrutamiento jerárquico de pasarela interior.
- Protocolo de Información de enrutamiento (RIPv2 por sus siglas en inglés): no soporta conceptos de sistemas autónomos.
- Sistema de Intermedio a Sistema de Intermedio (IS-IS por sus siglas en inglés).

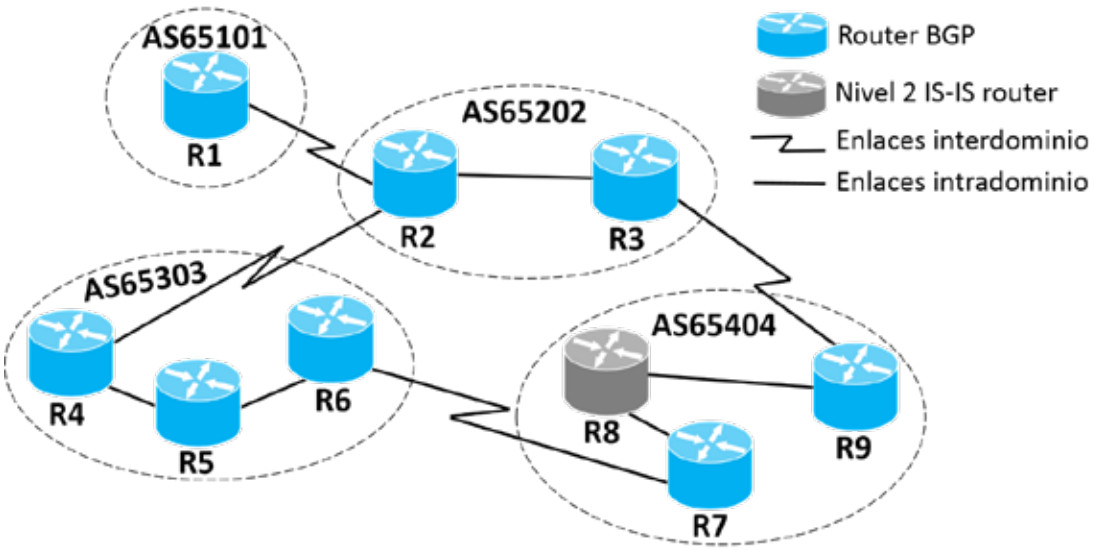


Figura 2. Tipos de sistemas autónomos.

Fuente: "Redes de comunicaciones", RedIRIS (2009).

2.2.8 EGPs

EGPs intercambian rutas entre diferentes sistemas autónomos. Donde encontramos:

- EGP. Utilizado para conectar la red de backbones de la Antigua Internet.
- Protocolo de Puerta de Enlace de Frontera (BGP por sus siglas en inglés). La actual versión, BGPv4 data de 1995.

2.2.9 MPLS

Es un mecanismo de transporte de datos estándar creado por el Grupo de Trabajo de Ingeniería de Internet (IETF por sus siglas en inglés) y definido en el RFC 3031. Siendo una tecnología de reenvío de paquetes de alto rendimiento que integra las capacidades de gestión de tráfico y rendimiento de la conmutación de capa de enlace de datos (Capa 2) con la escalabilidad, flexibilidad y rendimiento del enrutamiento de capa de red (Capa 3). Permite a los proveedores de servicios enfrentar los desafíos generados por el crecimiento explosivo y brinda la oportunidad de servicios diferenciados sin necesidad de sacrificar la infraestructura existente. (Ver figura 3)

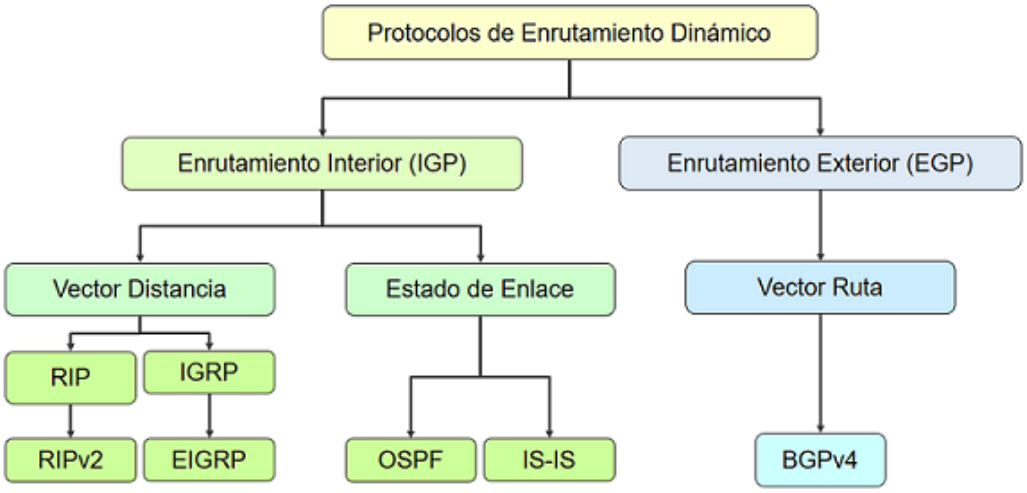


Figura 3. Clasificación de los protocolos de enrutamiento dinámico.

Fuente: "Análisis y mejora de la red de datos de la unsaac sobre la plataforma ip-mpls en un banco de pruebas", Tesis, Cusco (2017).

La arquitectura MPLS es notable por su flexibilidad:

- Los datos pueden transferirse a través de cualquier combinación de tecnologías de Capa 2.
- Se ofrece soporte para todos los protocolos de Capa 3.
- El escalado es posible más allá de lo que se ofrece en las redes de hoy.

Específicamente, MPLS puede habilitar de manera eficiente la entrega de servicios IP a través de una red conmutada por ATM y Frame Relay. Admite la creación de diferentes rutas entre una fuente y un destino en una red troncal de Internet basada únicamente en el enrutador.

Ø **Fundamentos.**

MPLS es una tecnología relativamente nueva que se desarrolló para solucionar la mayoría de los problemas que existen en la técnica actual de reenvío de paquetes. La IETF cuenta con un grupo de trabajo MPLS que ha unido esfuerzos para estandarizar esta tecnología.

La mayoría de los protocolos de enrutamiento desarrollados en la actualidad están basados en algoritmos diseñados para obtener el camino más corto para el recorrido del paquete por la red y no toman en cuenta parámetros adicionales como son retardo, jitter, y congestión de tráfico, los cuales pueden afectar el desempeño de la red, por lo que la ingeniería de tráfico es un reto para los administradores de redes.

MPLS actúa como nexo entre los protocolos de red y el correspondiente protocolo de nivel de enlace. Para ello, en la estructura de una trama, se sitúa la cabecera MPLS después de la cabecera de nivel de red y antes de la cabecera de nivel de enlace. De hecho, el reenvío de paquetes MPLS está basado en etiquetas y no en el análisis de los datos encapsulados desde niveles superiores.

Es una tecnología multiprotocolo que admite cualquier protocolo de red, pero al mismo tiempo permite cualquier tecnología en capas inferiores.

De esta forma, “Se ha proporcionado un atractivo mecanismo para aprovechar la infraestructura actualmente desplegada en ámbitos troncales, facilitando así la migración de tecnologías; sin embargo, los esfuerzos realizados desde hace años para desarrollar mecanismos innovadores que den soporte a IP sobre ATM no se han perdido, ya que la mayoría de las técnicas desarrolladas son válidas para disponer de IP sobre MPLS y MPLS sobre ATM” (Damon, 2002, pp. 8-9).

“La adición del envío de paquetes basado en etiquetas complementa el enrutamiento convencional pero no lo reemplaza. MPLS es un trabajo realizado y especificado por el IETF que da los parámetros para la eficiente designación de ruteo, envío y conmutación de tráfico que fluye por la red” (Gallear, 2002, p. 10).

2.2.10 Arquitectura MPLS.

Antes de explicar cómo trabajo una red MPLS, deben ser aclarados varios conceptos básicos que aplican para cualquier tecnología de conmutación.

- **Elementos**

1. Conmutación de etiqueta: describe la tecnología genérica que combina las tecnologías de capa 2 (capa de enlace de datos) y capa 3 (capa de red). La

solución de conmutación de etiquetas puede caracterizarse por el uso de envío de paquetes con etiquetas intercambiadas combinada con los protocolos de control de IP y un mecanismo de distribución de etiqueta.

2. Etiqueta (Label): es un identificador corto (de longitud fija) y con significado local, empleado para identificar un Clase de Equivalencia de Reenvió **(**FEC por sus siglas en ingles). Un paquete puede tener una o más etiquetas apiladas (jerarquía). Cuando un paquete atraviesa dominios interiores a otros dominios, es cuando se produce el apilamiento de etiquetas. El **LSR** al recibir un paquete siempre consultará la etiqueta de nivel superior.
3. Clase de Equivalencia de Reenvío FEC: agrupación de paquetes que comparten los mismos atributos (dirección destino, Redes Virtuales Privadas (VPN por sus siglas en inglés), entre otras y/o requieren el mismo servicio (multicast, QoS, entre otros). Se asigna en el momento en que el paquete entra a la red. Todos los paquetes que forman parte de la clase, siguen un mismo **LSP.**
4. Camino de Etiqueta Conmutada (LSP por sus siglas en inglés): es una ruta a través de uno o más **LSRs** en un nivel de jerarquía que sigue un paquete de un **FEC** en particular. Este camino puede establecerse tanto mediante protocolos de enrutamiento como manualmente. Los **LSPs** son unidireccionales (simplex) por naturaleza.
5. Protocolo de Distribución de Etiquetas (LDP por sus siglas en inglés): es un protocolo para el intercambio y distribución de etiquetas entre los LSR de una red MPLS.
6. Dominio MPLS: es una porción de una red que contiene dispositivos que entienden MPLS. Un dominio MPLS está constituido por los siguientes dispositivos:
    a. Enrutador de Conmutación de Etiquetas (LSR por sus siglas en inglés): es un dispositivo de alta velocidad que posee el componente de control

IP y un componente de envío de etiquetas intercambiadas y que típicamente reside en el medio de una red.

b. Enrutador Frontera de Etiquetado (LER por sus siglas en inglés): cualquier dispositivo que se encuentre entre una red MPLS y una red no MPLS, procesa paquetes etiquetados y no etiquetados, se identifican con las letras PE (Provider Edge)

7. Enrutador Perimetral del Cliente (CE Router por sus siglas en inglés): es un componente frecuente de una arquitectura MPLS que se conecta a un enrutador perimetral del proveedor (enrutador PE) para llevar las comunicaciones del lado del cliente al lado del proveedor. (Ver figura 4)

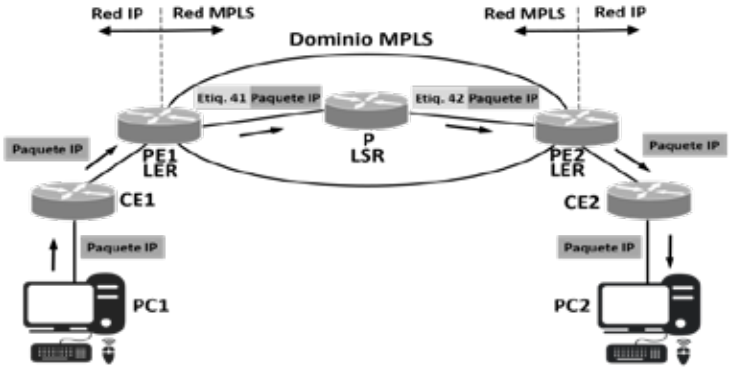


Figura 4. Arquitectura MPLS

Fuente: "Redes de comunicaciones", RedIRIS (2009).

· **Procesos MPLS**

1. Push (Empujar): es el acto de aplicar una etiqueta adicional a un paquete. Es posible que el paquete ya tenga una etiqueta, ya que MPLS puede admitir varias etiquetas apiladas. Este empuje se realiza normalmente en el ingreso LER, en el borde de la red. El LER requiere una asignación para que sepa qué datos colocar en un LSP. También

se puede realizar en el núcleo de una red donde se agrupan o encapsulan múltiples LSP dentro de otro LSP.

2. Swap (Intercambiar): es el acto de reemplazar una etiqueta. El interior del paquete etiquetado nunca se inspecciona. El intercambio se realiza por LSRs.
3. Pop (Quitar): es el acto de quitar la etiqueta más externa del paquete. Una o más etiquetas aún podrían estar dentro. El popping se realiza normalmente en la salida LER. Los LER deben realizar una búsqueda adicional para decidir cómo reenviar el paquete encapsulado. Los Penúltimos enrutadores sacarán la etiqueta pero solo reenviarán el paquete no encapsulado de acuerdo con la tabla de búsqueda para el LSP. (Ver figura 5)

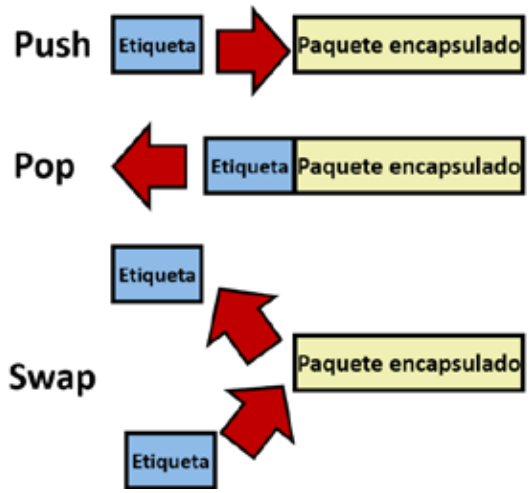


Figura 5. Procesos de etiquetado MPLS.

Fuente: https://suryaokhrabo.blogspot.com/2016/07/blog-post.html (2018).

2.2.11 Etiqueta MPLS.

Las etiquetas se insertan en cabeceras **MPLS**, entre los niveles 2 y 3. Según las especificaciones del **IETF**, **MPLS** debía funcionar sobre cualquier tipo de transporte: **PPP**, **LAN**, **ATM**, **Frame Relay**, entre otros. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas (**ATM**, **Frame Relay**, entre otros.), se pueden utilizar esos campos nativos para las etiquetas. Sin embargo, si la

tecnología de nivel 2 empleada no soporta un campo para etiquetas (enlaces **PPP** o **LAN**), entonces se emplea una cabecera genérica **MPLS** de 4 octetos, que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del nivel 3.

- **Cabecera MPLS.**

MPLS funciona anexando un encabezado a cada paquete. Dicho encabezado contiene una o más "etiquetas", y al conjunto de etiquetas se le llama pila o "stack". Cada etiqueta consiste en cuatro campos. (Ver figura 6)

Figura 6. Cabecera MPLS.

Fuente: https://es.wikipedia.org/wiki/Multiprotocol_Label_Switching (2018).

- Etiqueta: con tamaño de 20 bits permite más de 1 millón de etiquetas únicas por espacio de etiqueta. El espacio de la etiqueta podría definirse por interfaz o por plataforma. La multidifusión utiliza un espacio de etiqueta separado de unidifusión sobre MPLS. La etiqueta es el identificador de circuito que utiliza el LSR para reenviar el paquete.
- Experimental (EXP por su siglas en inglés): con un tamaño 3 bits, originalmente este campo de 3 bits no estaba en uso. Sin embargo, las implementaciones actuales lo utilizan para definir la cola en la que se coloca un paquete en una interfaz saliente, lo cual se denomina QoS.
- S (1 bit): Parte inferior de la pila. esta entrada se usa para indicar si esta es la última etiqueta antes de los datos encapsulados (S = 1) o si hay otra etiqueta dentro (S = 0). Esto permite colocar una pila de etiquetas teóricamente infinitas frente a un paquete y una gran flexibilidad en términos de poder escalar una red y habilitar nuevos servicios.

- Tiempo de vida (TTL por sus siglas en inglés): con un tamaño de 8 bit, cualquier red debe garantizar una topología sin bucles o limitar de alguna manera el efecto de los bucles cuando se producen. Los protocolos de enrutamiento IP no garantizan una topología libre de bucles, por lo que debemos limitar el efecto de los bucles de enrutamiento con un TTL. Al igual que IP TTL, en MPLS, el TTL decrementa cada LSR. Si el TTL llega a cero, el paquete se descarta.

Ø **Pilas de etiquetas**

Uno de los aspectos más poderosos de MPLS es la pila o acumulamiento de etiquetas. Un paquete etiquetado puede llevar muchas etiquetas, organizado como una pila LIFO de etiquetas (último en entrar primero en salir). El procesamiento está siempre basado en la etiqueta de la cima. En cualquier LSR, la etiqueta puede ser añadida a la pila (operación push) o removida de la pila (operación pop). El apilamiento de etiquetas permite la agregación de LSPs en un solo LSP para una porción de la ruta a través de una red, creando un túnel.

"Al principio del túnel, un LSR asigna la misma etiqueta a los paquetes de un número de LSPs colocando la etiqueta sobre la pila de cada paquete. Al final del túnel, otro LSR extrae el elemento de la cima de la pila de la etiqueta, mostrando la etiqueta interna. Esto es similar a ATM que tiene un nivel de pila (canales virtuales dentro de caminos virtuales), pero MPLS soporta una pila ilimitada. La pila de etiquetas proporciona una considerable flexibilidad en la transmisión de la información. Este proceso está basado en la etiqueta de más alta numeración, sin contemplar la posibilidad de que algún número de otra etiqueta haya sido anteriormente la más alta o que otro número de alguna etiqueta haya estado por debajo de esa" (Gallear, 2003, pp.19-20).

En un modelo más general, "MPLS soporta la colocación de múltiples etiquetas a un solo paquete; en este caso, se soporta un diseño de ruteo jerárquico. Estas etiquetas se organizan en una pila o "stack" 20 con una forma last-in, first-out

(LIFO), y forma la llamada pila de etiquetas o label stack. El principal empleo de la pila de etiquetas se tiene cuando se emplea una operación MPLS llamada Tunneling" (Gallear, 2003, pp.19-20).

2.2.12 Funcionamiento de MPLS

El funcionamiento del protocolo MPLS debe seguir los siguientes pasos:

1. Creación y distribución de etiquetas.
2. Creación de tablas en cada enrutador.
3. Creación de LSPs.
4. Agregar etiquetas a los paquetes con la información de la tabla.
5. Envío del paquete.

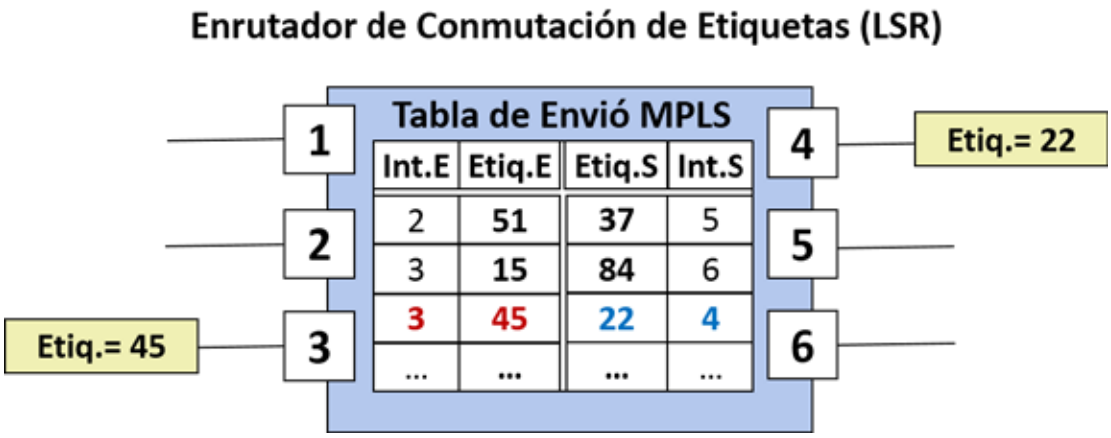
Por lo cual el funcionamiento de una red MPLS lo podemos dividir en dos partes fundamentales, las cuales son envió de paquetes y control de información.

- **Envió de Paquetes.**

La base del MPLS está en la asignación e intercambio de etiquetas, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son unidireccionales (simplex) por naturaleza; el tráfico bidireccional (dúplex) requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un conmutador de etiquetas (LSR) a otro, a través del dominio MPLS.

El envío se implementa mediante el intercambio de etiquetas en los LSPs. Sin embargo, MPLS utiliza los protocolos de señalización de enrutamiento como Protocolo de Reserva de Recursos (RSVP por su siglas en inglés) o bien un nuevo estándar de señalización LDP.

Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera. Por ejemplo, si éste fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM, lo que se haría transformando las direcciones y las tablas de enrutamiento IP en las direcciones y el



enrutamiento ATM. Este problema lo resuelve el procedimiento de intercambio de etiquetas MPLS. (ver figura 7)

Figura 7. Tabla de envió MPLS.

Fuente:https://ldc.usb.ve/~poc/RedesII/Grupos/G5/funcionamiento_envio.htm (2018).

Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada/salida correspondientemente, que se utilizan para acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta (en los **LSR** exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola), en la **figura 7** se ilustra un ejemplo del funcionamiento de un **LSR** del núcleo **MPLS.**

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura 8 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de **enrutamiento** y asigna el paquete a la clase FEC definida por el grupo 212.95/16. Así mismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP**.**

Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el algoritmo de intercambio

de etiquetas. Al llegar un paquete al LSR de cola (salida), este determina que el siguiente salto va fuera de la red MPLS, por lo que al consultar la tabla de conmutación de etiquetas, remueve la etiqueta y envía dicho paquete por enrutamiento convencional. Como se ve, la identidad del paquete IP original queda enmascarada durante el transporte por la red MPLS. (Ver figura 8)

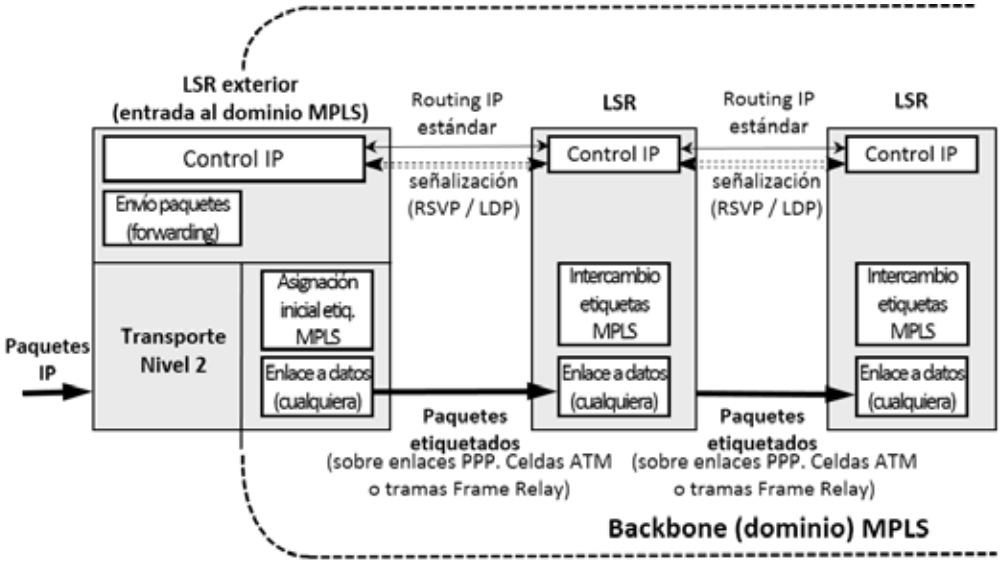


Figura 8. Tabla de envió MPLS.

Fuente:https://ldc.usb.ve/~poc/RedesII/Grupos/G5/funcionamiento_envio.htm (2018).

· **Control de Información.**

Después de ver el mecanismo básico de envío de paquetes en MPLS. Queda por definir dos aspectos fundamentales:

1. Cómo se generan las tablas de envío que establecen los LSPs.
2. Cómo se distribuye la información sobre las etiquetas a los LSRs.

· **Tablas de Envío.**

Las tablas de envió se generan con la información que se tiene sobre la red, tales como topología, patrón de tráfico y características de los enlaces, entre otros. Esta información es la que manejan los protocolos internos IGP (OSPF, IS-IS, RIP, IGRP y EIGRP) para construir sus tablas de enrutamiento. MPLS utiliza esta información de estos protocolos para establecer los caminos virtuales o LSPs.

Para cada "ruta IP" en la red se crea un camino de etiquetas, concatenando las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

- **Información de las etiquetas.**

El segundo aspecto se refiere a la información de "señalización", necesaria siempre que se quiera establecer un circuito virtual. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas. De hecho, se están estandarizando diferentes protocolos para tal fin. Entre los protocolos existentes que se extienden para soportar MPLS, se encuentra el Protocolo RSVP y BGP en las formas conocidas como MPLS-BGP, MPLS-RSVP-TUNNELS. También se están definiendo nuevos protocolos específicos para la distribución de etiquetas, como lo es el LDP y el Protocolo de Distribución de Etiquetas Basado en Restricciones (CR_LPD por sus siglas en inglés). RSVP es preferido por IETF, LDP por Cisco y el CR_LPD por Nokia.

Las diferentes variaciones en el intercambio de etiquetas son:

- LDP: Mapea los destinos IP (unicast) en etiquetas.
- RSVP, CR_LDP: Es usado para ingeniería de tráfico y reserva de recursos.
- BGP: Para etiquetas externas (VPN).

2.2.13 Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

- Ingeniería de tráfico.
- Diferenciación de niveles de servicio mediante Clase de Servicio (CoS por sus siglas en inglés).
- Servicio de redes privadas virtuales (VPN por su siglas en ingles).
- **Ingeniería de Tráfico**

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera de evitar que un subconjunto (enlaces, equipos, entre otros) de la

red se sature mientras otro subconjunto de la misma se encuentra infrautilizado, mejorando el rendimiento de la red global.

Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente. En casos de congestión de algunos enlaces, el problema se resolvería añadiendo más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos).

MPLS es una herramienta efectiva para aplicarla con ingeniería de tráfico ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.
- Permite hacer Enrutamiento Basado en Restricciones (CBR por sus siglas en inglés), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad).

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM por debajo, todo ello de manera más flexible y con menores costes de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

- **CoS**

MPLS está diseñado para poder cursar servicios diferenciados, según el modelo DiffServ del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de CoS, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios

tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP.

De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

- El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.
- Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda (i.e. un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico best-effort).
- **VPN**

Las Redes Virtuales Privadas (VPN por sus siglas en ingles), se construye basado en conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intranet/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces. Las ventajas que MPLS ofrece para IP VPNs son:

- Proporcionar un modelo "acoplado" o "inteligente", ya que la red MPLS conoce de la existencia de VPNs (lo que no ocurre con túneles ni PVCs).
- Evita la complejidad de los túneles y PVCs.

- Provee de un servicio sencillo: una nueva conexión afecta a un solo enrutador y tiene mayores opciones de crecimiento modular.
- Permite mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.
- Permite aprovechar las posibilidades de ingeniería de tráfico para las poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación, entre otros.), lo que es necesario para un servicio completo VPN.

2.2.14 Rendimiento de una red

El rendimiento de red se refiere a las medidas de calidad de servicio de un producto de telecomunicaciones desde el punto de vista del cliente.

Cuando se trabaja con redes es de suma importancia conocer la manera en cómo se están comunicando los datos, para de esta manera realizar un análisis que permita determinar la calidad del enlace de comunicaciones. Para esto es necesario analizar el comportamiento de la red y de esta manera estimar su rendimiento, debido a que una red mal configurada o con un pobre rendimiento puede ocasionar grandes pérdidas de tiempo, bajas en la productividad y entre otros, ya que en sistemas de comunicaciones de gran tamaño esto es muy importante.

Para poder resolver problemas que se puedan presentar es necesario conocer a profundidad todos los parámetros de la red en cuestión además de realizar un monitoreo de la misma para poder detectar cualquier anomalía, con estas herramientas se puede hacer un diagnóstico acertado de cualquier tipo de eventualidad para poder corregirla a tiempo. Los parámetros más comunes para chequear el comportamiento de una red son la eficiencia, throughput y el retraso o latencia que sufren los paquetes debido a las congestiones que pueden encontrar entre el origen y el destino.

- **Arquitectura de rendimiento de una red**

El rendimiento en una red está compuesto por los niveles de capacidad, el retardo y la confiabilidad, mantenimiento y disponibilidad. (RMA por sus siglas en ingles). En una Red es de suma importancia mantener niveles óptimos en estos componentes, ya que los diferentes flujos de información generados por los usuarios, dispositivos o aplicaciones pueden verse fuertemente afectados en sus actividades debido a variaciones de los niveles de rendimiento.

Se entiende entonces por arquitectura de rendimiento el conjunto de mecanismos que se utilizan para configurar, operar, gestionar, disponer y listar los recursos en la red que soportan los tráficos de flujo de información.

- **Capacidad**

La capacidad se puede definir genéricamente como la habilidad que tiene el sistema para lograr la transferencia de información a través de la red. Comúnmente al término de capacidad está relacionado con términos como:

- Ancho de banda: es la capacidad que tiene una red para transmitir datos a través de ella, normalmente se refiere a la cantidad de datos que se pueden transmitir en determinado momento a través de la red. Comúnmente es medido en bits por segundo (bit/s) o en sus múltiplos.
- Throughput: se refiere a la tasa promedio de datos o mensajes que han sido transferidos exitosamente y sin errores en la red de un nodo a otro.
- Goodput: es la cantidad de bits de información utilizables, que se envía en la red a un destino determinado, por unidad de tiempo.

- **Retardo**

Es la cantidad de tiempo que se toma la transferencia de una unidad de información a través del sistema desde un origen a un destino.

- **RMA** El acrónimo en inglés provienen de los vocablos "reliability, maintainability, y availability" que en español se traducen como "confiabilidad, mantenimiento y disponibilidad":
- Confiabilidad (reliability): es un indicador de la frecuencia de fallos que ocurren en la red y sus componentes, y representa las interrupciones no programadas de los servicios.
- Mantenimiento (maintainability): es una medición estadística del tiempo que se tarda la red para volver a estar en óptimas condiciones después de haber sufrido una interrupción en sus funciones de manera inesperada.
- Disponibilidad (availability): es la relación que existe entre la cantidad de fallas que sufren las misiones críticas en el sistema y la cantidad de tiempo que le toma a ese sistema recuperarse y trabajar adecuadamente.
- **Mecanismos de rendimiento**

Los mecanismos proporcionan los medios para identificar los tipos de tráfico de flujo, medir sus características temporales y adoptar diversas medidas para mejorar el rendimiento de los flujos individuales, grupales, o para todos los flujos de la red en general. Algunos de los cuales tenemos:

- Calidad de Servicio: se utiliza para la determinar, ajustar e interpretar los niveles de prioridad en los flujos de tráficos.
- Priorizar, gestión de tráfico, planificación y las colas:
    - Priorizar: proceso por el cual se determinar qué usuarios, aplicaciones, dispositivos, flujos y conexiones obtendrán el servicio delante de los demás o conseguir un mayor nivel de servicio.
    - Gestión de tráfico: consiste en el control de admisión y acondicionamiento del tráfico.
    - Planificación: mecanismo que determina el orden en el que el tráfico se procesa para su transmisión. La planificación usa niveles de

prioridad para determinar qué flujos de tráfico se procesan primero y con más frecuencia.

- Colas: Es el proceso donde se ponen en espera o se almacenan los paquetes IP dentro de un dispositivo de red mientras esperan para su procesamiento.

- Acuerdos de nivel de servicio: son los contratos que se establecen entre proveedor y cliente, en donde el proveedor se compromete a prestar sus servicios de acuerdo a los parámetros previamente discutidos con el usuario y el alcance de la responsabilidad si no se cumplen esas responsabilidades por parte del proveedor.
- Políticas: reglas que pueden ser informales o formales acerca de cómo son los recursos de red (y por tanto también el rendimiento) se distribuirán entre los usuarios, aplicándose también a los niveles de acceso que tendrá cada tipo de usuario, a la computación, el almacenamiento u otros recursos que estén disponibles para los usuarios.
- **Rendimiento en una red MPLS**

MPLS no está relacionada a ninguna tecnología subyacente. Fue diseñado en el mismo tiempo que ATM y Frame Relay como un protocolo de enrutamiento de paquetes diseñada para simplificar y mejorar el rendimiento.

ATM y Frame Relay son tecnologías que ya no se implementan en la actualidad, mientras que el protocolo MPLS es empleado ofreciendo redes escalables, de alto rendimiento, mejor utilización del ancho de banda, congestión de red reducida y una mejor experiencia para el usuario final.

A diferencia de las demás tecnologías de enrutamiento de paquetes MPLS puede ser aplicado a cualquier tecnología de transmisión de datos, por medio de etiquetas. Al entrar un paquete a un dominio MPLS se le coloca una etiqueta mediante la cual el paquete tomara una ruta ya predeterminada llamada LSP y pasara por los distintos LSR que constituyen la red MPLS hasta llegar al borde del dominio

MPLS a un dispositivo llamado LER el cual cumple la función de dispositivo frontera entre la dominio MPLS y el dominio IP removiendo la etiqueta colocada al principio del proceso y así el paquete continuara su ruta mediante su dirección IP de destino, así de esta manera disminuye el retardo de un paquete desde el inicio hasta el final de su trayectoria. Al implementar el protocolo MPLS en una red aumentara satisfactoriamente su rendimiento por medio de las aplicaciones que ofrece siendo una de ellas ingeniería en tráfico que por medio de la cual se pueden mejorar los mecanismos de rendimiento de una red para así cumplir con las expectativas del cliente y ofrecerle una calidad de servicio.

2.2.15 OSPF

Para realizar el análisis del rendimiento y los parámetros de una red MPLS usaremos como algoritmo de enrutamiento OSPF.

OSPF es un protocolo de enrutamiento de estado de enlace popular que se puede ajustar de muchas maneras. Algunos de los métodos de ajuste más comunes incluyen la manipulación del proceso de elección del Router Designado/ Router Designado de Respaldo (DR/BDR por su siglas en inglés), la propagación de rutas predeterminadas, el ajuste de las interfaces OSPFv2 y OSPFv3 y la habilitación de la autenticación.

Una etiqueta representa una clase FEC, pero no representa una ruta particular a través de la red. En general, la ruta a través de la red continúa siendo elegida por los algoritmos de enrutamiento de capa 3. Es decir, en cada salto cuando se busca una etiqueta, el siguiente salto elegido está determinado por el algoritmo de enrutamiento dinámico.

Se implementa con frecuencia y se desarrolló como un reemplazo para el protocolo de enrutamiento vector distancia RIP**.** Sin embargo, OSPF presenta ventajas importantes en comparación con RIP, ya que ofrece una convergencia más rápida y escala a implementaciones de red mucho más grandes. Las características de OSPF:

- **Sin clase**: fue diseñado como un protocolo sin clase, de modo que admite Máscaras de Subred de Longitud Variable (VLSM por su siglas en inglés) y Enrutamiento entre Dominios Sin Clases (CIDR por su siglas en inglés).
- **Eficaz**: los cambios de **enrutamiento** desencadenan actualizaciones de **enrutamiento** (no hay actualizaciones periódicas). Usa el algoritmo SPF para elegir la mejor ruta.
- **Convergencia rápida**: propaga rápidamente los cambios que se realizan a la red.
- **Escalable**: funciona bien en redes pequeñas y grandes. Se pueden agrupar los routers en áreas para admitir un sistema jerárquico.
- **Seguro**: admite la autenticación de síntesis de mensaje con el Algoritmo de Resumen del Mensaje 5(MD5 por sus siglas en inglés). Cuando están habilitados, los routers OSPF solo aceptan actualizaciones de enrutamiento cifradas de peers con la misma contraseña compartida previamente.
- **DR/BDR**

Los routers en el mismo dominio de multidifusión o en el extremo de un enlace punto-a-punto forman enlaces cuando se descubren los unos a los otros. En un segmento de red Ethernet los routers eligen a un DR y BDR que actúan como hubs para reducir el tráfico entre los diferentes routers. OSPF puede usar tanto multidifusiones como unidifusiones para enviar paquetes de bienvenida y actualizaciones de enlace-estado.

- **Autenticación.**

Esto garantiza que los routers sólo aceptarán información de enrutamiento de otros routers que estén configurados con la misma contraseña o información de autenticación. OSPF pueden configurarse para encriptar y autenticar su información de enrutamiento.

- **Encaminamiento, routers y áreas.**

OSPF organiza un AS en áreas. Estas áreas son grupos lógicos de routers cuya información se puede resumir para el resto de la red. Un área es una unidad de

enrutamiento, es decir, todos los routers de la misma área mantienen la misma información topológica en su base de datos de estado-enlace (Link State Database): de esta forma, los cambios en una parte de la red no tienen por qué afectar a toda ella, y buena parte del tráfico puede ser "parcelado" en su área.

2.2.16 Link State Database (LSDB).

Conjunto de las LSA de todos los routers y redes del sistema autónomo. También se conoce como base de datos topológica. Todos los routers dentro de un área tienen la misma LSDB.

2.2.17 Link State Advertisement (LSA).

Los LSA (Link State Advertisements) son, como dicen sus siglas en inglés, actualizaciones del estado de los enlaces, es decir, son los paquetes que contienen toda la información referente a rutas, quien se conecta con quien, interfaces, costos, entre otros. Cada vez que una interfaz levanta o cae, son los LSA quienes llevan esta información a todos los routers. Obviamente juegan un papel fundamental en el funcionamiento del OSPF, es por ello que para un buen diseño y troubleshoot (solucionar problemas) debemos conocerlos y entenderlos. Existen diferentes tipos de LSA, los cuales describo a continuación:

- LSA Type 1 (Router LSA): Un LSA tipo 1 es quien lleva la identificación de cada router (Router-id) dentro de un área y los enlaces que lo conectan. Cada router que hable OSPF crea un LSA tipo 1 para sí mismo, y luego lo envía dentro del área al que pertenece. Este LSA es transmitido hacia cada neighbour y viceversa, hasta que todos tengan la misma copia de LSA. Si aún no se ha elegido ningún DR, muestra una lista de las interfaces con sus subredes, máscaras y costos. Si ya se eligió el DR entonces muestra la IP del DR.
- LSA Type 2 (Network LSA):Los LSA tipo 2 son enviados dentro del área por el DR y contienen las redes que tiene conectadas y sus máscaras, ayudando así a moldear la topología de la red.

- LSA Type 3 (Network summary): Los LSA tipo 1 y 2 solo fluyen dentro de un área, o sea los ABR no los transmiten. Ellos generan LSA tipo 3 para cada subred en un área y luego las publica en las otras áreas, permitiendo que las mismas aprendan sobre ellas. Hay que acotar que, aunque se llamen "Network summary" los LSA tipo 3 no son utilizados para hacer sumarización.
- LSA Type 4 (ASBR Summary): Son como los tipo 3, pero pública son las rutas necesarias para llegar a un ASBR.
- LSA Type 5 (External LSA): Los LSA Tipo 5 son creados por los ASBR y contienen las rutas que son redistribuidas por otro protocolo de enrutamiento o por rutas estáticas.

2.2.18 Información utilizada por OSPF.

OSPF mantiene tres tablas:

- Tabla de ruteo: El objetivo de cualquier protocolo de ruteo, lograr una tabla que dada una red de destino indique el camino para alcanzarla.
- Tabla de adyacencias (o de vecinos): En esta tabla se mantiene la información sobre los vecinos con los cuáles se realizan intercambios OSPF.
- Tabla de topología (o base de datos de LSA): en esta tabla se almacenan todos los LSA recibidos de toda la red. Los LSA son paquetes OSPF que contienen información sobre rutas (red y camino para alcanzarla). De esta manera es como un router OSPF conoce la topología completa de la red. De hecho, utilizando la tabla de topología es posible dibujar toda la red con los costos de cada enlace.
- **Algoritmo de Dijkstra.**

OSPF utiliza el algoritmo de Dijkstra para determinar la mejor ruta a seguir. También se denomina algoritmo SPF (Shortest Path First). Fue formulado por Edsger Dijkstra. OSPF activa sus actualizaciones con cada cambio en la topología de la red, lo que reduce el tiempo de convergencia. A partir de una actualización, un enrutador crea una base de datos topológica que permite calcular la accesibilidad a las redes

gracias al cálculo de un árbol de la topología de la que el enrutador es la raíz. Este es un proceso que ejecuta cada router OSPF por sí mismo y sin intervención de ningún otro router.

- **Tipos de router en OSPF.**

Un router OSPF clásico es capaz de encaminar cualquier paquete destinado a cualquier punto del área en el que se encuentra (**enrutamiento** intra-área). Para el **enrutamiento** entre distintas áreas del AS (**enrutamiento** inter-área) y desde el AS hacia el exterior (**enrutamiento** exterior), OSPF utiliza routers especiales que mantienen una información topológica más completa que la del área en la que se sitúan. Así, pueden distinguirse:

- Router fronterizo de área (ABR por sus siglas en ingles), que mantienen la información topológica de su área y la conectan con el resto de las áreas, permitiendo encaminar paquetes a cualquier punto de la red (inter-arearouting).
- Router fronterizo del Sistema Autónomo (ASBR por sus siglas en ingles), que permiten encaminar paquetes fuera del AS en que se alojen, es decir, a otras redes conectadas al Sistema Autónomo o resto de Internet.

Un paquete generado en la red será enviado, de forma jerárquica, a través del área si su destino es conocido por el emisor; al ABR del área correspondiente si el destino es inter-área; este lo enviará al router del área de destino, si este se encuentra en el AS; o al ASBR si el destino del paquete es exterior a la red (desconocida por el ABR).

- **Áreas**

Para que OSPF sea más eficaz y escalable, este protocolo admite el **enrutamiento** jerárquico mediante áreas. Un área OSPF es un grupo de routers que comparten la misma información de estado de enlace en sus LSDB.OSPF se puede implementar de dos maneras:

- OSPF de área única**:** Todos los routers se encuentran en un área llamada “área backbone” (área 0).
- OSPF multiárea**:** OSPF se implementa mediante varias áreas, de manera jerárquica. Todas las áreas deben conectarse al área backbone (área 0). Los routers que interconectan las áreas se denominan “routers fronterizos de área” (ABR).

Con OSPF multiárea, se puede dividir un AS grande en áreas más pequeñas, a fin de admitir el **enrutamiento** jerárquico. Con el **cual** se sigue produciendo el **enrutamiento** entre áreas, y muchas de las operaciones de **enrutamiento** que implican una gran exigencia para el procesador, como volver a calcular la base de datos, estos se guardan en un área. (ver figura 9)

- **Distancia administrativa de OSPF.**

OSPF tiene una distancia administrativa predeterminada de 110.

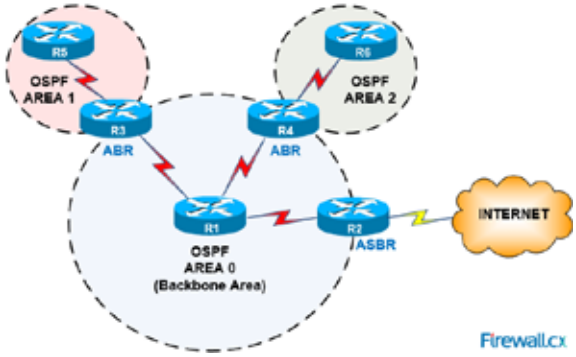


Figura 9. Áreas de OSPF.

Fuente: http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/OSPF/Ruteo-OSPF.pdf (2018).

- **Métrica OSPF.**

Su medida de métrica se denomina cost (Costo), y tiene en cuenta diversos parámetros tales como el ancho de banda y la congestión de los enlaces. La fórmula para calcular el costo es el ancho de banda de referencia dividido por el ancho de banda de la interfaz. Por ejemplo, en el caso de Ethernet, es 100 Mbps/10 Mbps = 10, donde el numerador es lo que se llama "Ancho de banda de referencia" y puede ser

cambiado por otro número arbitrario en la configuración (pero debe ser igual en todos los routers).

2.2.19 Border Gateway Protocol (BGP).

Es un protocolo mediante el cual se intercambia información de **enrutamiento** o ruteo entre AS.

Entre los sistemas autónomos de los ISP se intercambian sus tablas de rutas a través del protocolo BGP. Este intercambio de información de **enrutamiento** se hace entre los routers externos de cada sistema autónomo, los cuales deben soportar BGP. Se trata del protocolo más utilizado para redes con intención de configurar un Exterior Gateway Protocol.

La forma de configurar y delimitar la información que contiene e intercambia el protocolo BGP es creando lo que se conoce como sistema autónomo. Cada sistema autónomo (AS) tendrá conexiones o, mejor dicho, sesiones internas (iBGP) y además sesiones externas (eBGP).

El protocolo de gateway fronterizo (BGP) es un ejemplo de protocolo de gateway exterior (EGP). BGP intercambia información de **enrutamiento** entre sistemas autónomos a la vez que garantiza una elección de rutas libres de bucles. Es el protocolo principal de publicación de rutas utilizado por las compañías más importantes de ISP en Internet. BGP toma decisiones de **enrutamiento** basándose en políticas de la red, o reglas que utilizan varios atributos de ruta BGP.BGP realiza tres tipos de Routers:

- Routers Interautónomo.
- Routers Intrautónomo.
- Routers de pasc.

Ø **Relaciones entre AS**

Las relaciones que existen entre distintos sistemas autónomos son principalmente de peering de tránsito. En este sentido las relaciones de peering consisten en un enlace para comunicar dos sistemas autónomos con el fin de reducir costes, latencia, pérdida de paquetes y obtener caminos redundantes.

Un escenario que se suele repetir es uno llamado “Multihoming”. Este término hace referencia a un cliente que contrata a dos proveedores de tránsito, lo que implica que existen dos rutas de salida, de modo que se deberá decidir entre un camino u otro dependiendo de ciertas especificaciones, necesidades o simples políticas que se impongan en el sistema autónomo. (ver figura 10)

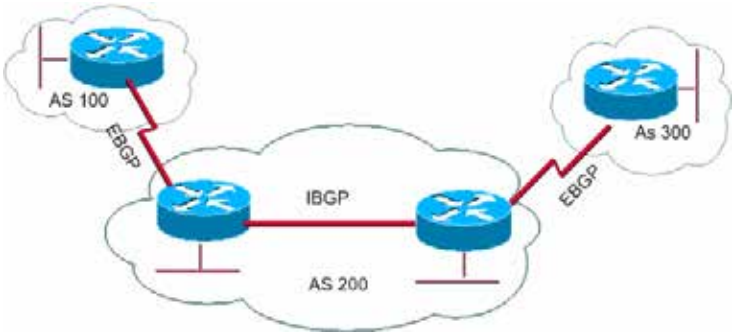


Figura 10. Relación entre sistemas autónomos.

Fuente: “Redes de comunicaciones”,
RedIRIS (2009).

2.2.20 QoS

Consiste en reconocer los diferentes flujos de tráfico provenientes de diferentes aplicaciones. Una vez que se ha reconocido el flujo, se puede proceder a especificar de qué forma se trata cada flujo de tráfico en la red. De esta forma se puede priorizar un tipo de tráfico sobre otro al utilizar los recursos de la red, como por ejemplo priorizar el trafico sensible a retardos y pérdidas (“real-time”). El esquema de calidad de servicio permite controlar el acceso a los recursos disponibles.

Cabe destacar que, “Una de las características clave de MPLS, comparado con redes tradicionales como Frame Relay y ATM, es que está diseñado para proveer servicios garantizados. Es decir, que según los requisitos de los usuarios, permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz interactiva” (Redford, 2004, pág. 35).

Por otro lado la IETF (Internet Engineering Task Force) ha propuesto nuevas arquitecturas que podrían dar solución a los requerimientos de Calidad de Servicios actuales gracias al uso de nuevas tecnologías tales como IPv6. Estas arquitecturas: Arquitectura de Servicios Diferenciados DiffServ, Arquitectura de Servicios Integrados IntServ y además se encuentra la arquitectura actual bajo el esquema BestEffort.

- **Importancia de QoS**

En los últimos años el tráfico de redes ha aumentado considerablemente, la necesidad de transmitir cada vez más información en menos tiempo, como video y audio en tiempo real (streaming media) cada vez más, ya que la mayoría de los casos esto no es posible y además es limitado. Es aquí donde la administración efectiva de recursos que provee QoS entra a relucir.

- **Beneficios de QoS**

QoS trabaja a lo largo de la red y se encarga de asignar recursos a las aplicaciones que lo requieran, dichos recursos se refieren principalmente al ancho de banda. Para asignar estos recursos QoS se basa en prioridades, algunas aplicaciones podrán tener más prioridades que otras, sin embargo se garantiza que todas las aplicaciones tendrán los recursos necesarios para completar sus transacciones en un periodo de tiempo aceptable.

En resumen, “QoS otorga mayor control a los administradores sobre sus redes, mejora la interacción del usuario con el sistema y reduce costos al asignar recursos con mayor eficiencia (bandwidth). Mejora el control sobre la latencia (Latency y jitter) para asegurar la capacidad de transmisión de voz sin interrupciones y por ultimo disminuye el porcentaje de paquetes desechados por los enrutadores: confiabilidad. MPLS impone un marco de trabajo orientado a conexión en un ambiente de Internet basado en IP (Internet Protocol) y facilita el uso de contratos de tráfico QoS exigentes” (Lloyd, 2001, p.87).

- **Métodos básicos para QoS**

Existen dos métodos básicos para brindar QoS:

- **Con reserva:** en este método se reservan recursos explícitamente. En este caso la red clasifica el flujo de paquetes entrantes y manipula esta identificación para proveer un servicio diferenciado.
- **Sin reserva:** en este método no existen recursos reservados explícitamente. El tráfico se clasifica en un tipo de clase y la red provee servicio a las distintas clases basándose en su prioridad. Es necesario que la red diferencie el tráfico, controlando la cantidad de tráfico de una determinada clase permitida, para mantener la calidad de servicio que se le brinda a otros paquetes de la misma clase.

2.2.21 Parámetros de QoS

La ITU-T define parámetros de calidad de servicio con los cuales se basa para definir los diferentes requerimientos de las aplicaciones así como de los clientes hacen a la red del proveedor a través del LSA. Estos parámetros varían de tráfico en tráfico y de cliente en cliente, según los requerimientos y los aspectos técnicos de la red. Los parámetros que se mencionan se pueden utilizar para los diferentes tipos de especificaciones para la evaluación de la calidad de funcionamiento de la red en lo referente a rendimiento de velocidad, exactitud del envío, seguridad en el funcionamiento y disponibilidad de la transmisión de los diferentes paquetes IP a nivel mundial ya sea de extremo a extremo, punto a punto y a tramos de la red. Los son:

- Rendimiento: se define como los datos reales en forma de bits que viajan con éxito a través de un canal de comunicación a la red terminal.
- Retardo (Relay): se refiere al tiempo que dura en transmitirse un bit desde su origen hasta su destino. Es un parámetro que se emplea para medir el máximo retardo en una red de extremo a extremo.
- Variaciones de retardo (Jitter): expresa la variación experimentada entre dos retardos consecutivos durante la transmisión y procesamiento de datos. El

Jitter puede amortiguarse mediante el incremento de buffers (buffering) en los receptores lo que a su vez, incrementa el retardo extremo a extremo.

- Pérdida de paquetes (Loss): este parámetro se refiere a la pérdida de paquetes de una comunicación.
- Ancho de Banda (Bandwidth): es la capacidad de transportar información a través de un canal de comunicación. Este canal puede ser analógico o digital.
- Latencia (Latency): un método para medir la Latencia es ver cuánto tiempo se demora un dispositivo en procesar un paquete. Este dispositivo puede ser un router, un sistema completo de comunicaciones que incluye routers y enlaces, en muchos casos hablar de latencia es sinónimo de retardo (relay).

2.2.22 Clase de Servicio (CoS, Class of Service)

La mayoría de las herramientas QoS clasifican el tráfico. El cual permite a cada clase de tráfico recibir un trato diferente con respecto a otras clases de tráfico. Estos diferentes tipos de tráfico, en terminología QoS se les llama típicamente clases de servicio. La clasificación permite a los dispositivos decidir qué paquetes son parte de cada clase de servicio.

Las herramientas de clasificación y marcado de tráfico no solo clasifican paquetes en clases de servicio, sino que también marcan los paquetes en la misma clase de servicio con el mismo valor en un campo en el encabezado. Al marcar los paquetes, otras herramientas QoS que examinan el paquete más tarde, pueden examinar los bits de marca para que sea más fácil clasificar los paquetes.

Casi todas las herramientas QoS usan la clasificación en algún nivel. Para poner un paquete en una cola de espera diferente a otro paquete.

CoS es un esquema de prioridad que emplea el protocolo 802.1Q, esta proporciona un método de asignación de etiquetas a los paquetes con información sobre la prioridad.

El valor de la clase de servicio está dado entre 0 y 7 la cual emplea el protocolo 802.1p el cual se encuentra dentro de la etiqueta de CoS específicamente en el campo

de priority, este valor es agregado al encabezado de la capa 2 de los paquetes, donde el 0 es la prioridad más baja y el 7 la prioridad más alta.

- **Etiqueta CoS**

  Esta constituida por 3 campos. (Ver figura 11) los cuales son:

- Priority Code Point (PCP): también conocido como prioridad de usuario, este campo de 3 bits se refiere a la prioridad del IEEE 802.1P. El campo indica el nivel de prioridad de la trama que se puede utilizar para el priorización del tráfico. El campo puede representar 8 niveles (0 a 7).
- Cannonical Format Indicator (CFI): el indicador del formato canónico es un campo de 1 bit. Si el valor de este campo es 1, la dirección MAC está en el formato no canónico. Si el valor es 0, la dirección MAC está en el formato canónico.
- VLAN Identifier: el identificador de VLAN es un campo de 12 bits. Identifica únicamente el VLA N al cual la trama pertenece. El campo puede tener un valor entre 0 y 4095.

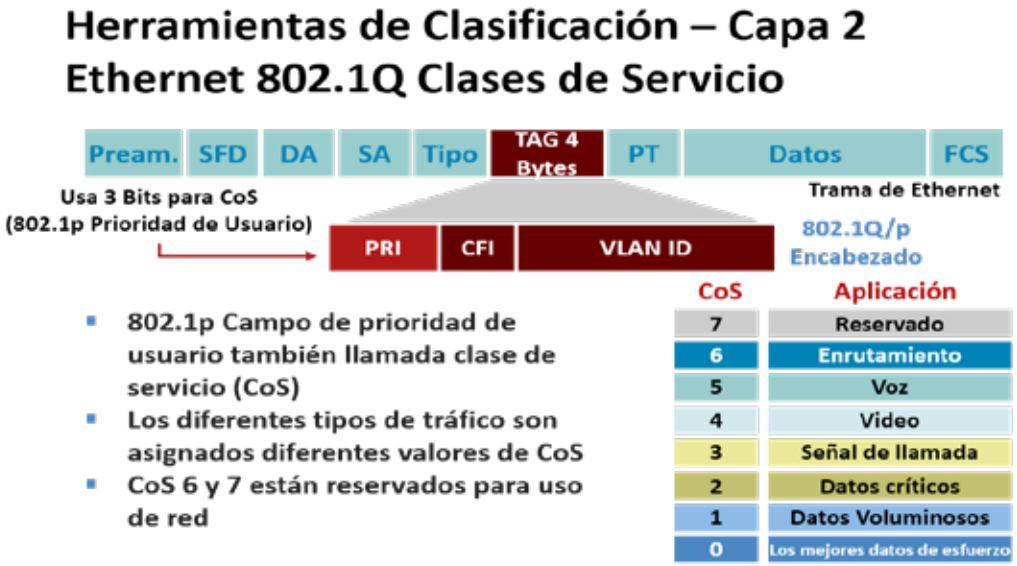


Figura 11. Etiqueta CoS

Fuente:https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html (2015).

2.2.23 Type of Service (ToS)

Es un campo de 8 bits de la cabecera IPv4 para definir ToS (Type of Service) del que se utilizan los 3 bits más significativos para definir la precedencia (IP Precedence). El bit menos significativo debe valer 0.

En diciembre de 1998, se restructura y se definen los Differentiated Services Code Points (DSCPs) que utilizan los 6 bits más significativos del campo. Los dos bits restantes definen el Explicit Congestion Notification (ECN), que se utiliza para informar que se están rechazando paquetes por congestión.

Figura 12. Etiqueta ToS

Fuente:https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html (2015).

2.2.24 Relaciones entre CoS y ToS.

Dado que inicialmente se utilizaba IP Precedence para definir las calidades de servicio junto con los Class Selectors, y en cómo comentaba anteriormente, en 1998

se definen los códigos DSCP que proporcionan más opciones con las que controlar el tráfico. La relación entre ellos se muestra en la tabla 1.

Tabla 1. Relación entre precedencia IP y DSCP códigos.

Nombre	Precedencia IP		DSCP Códigos		Selector de clase	
	Valor	Binario	Valor	Binario	Valor	Binario
Normal	0	000	0	000 000	CS0	000 000
Prioridad	1	001	8	001 000	CS1	001 000
Inmediato	2	010	16	010 000	CS2	010 000
Rápido	3	011	24	011 000	CS3	011 000
Rápido-Fuera de tiempo	4	100	32	100 000	CS4	100 000
Critico	5	101	40	101 000	CS5	101 000
Control de internet	6	110	48	110 000	CS6	110 000
Control de Red	7	111	56	111 000	CS7	111 000

Fuente. José Escalona (2019).

2.2.25 Tecnologías para el soporte de QoS

En la actualidad, el soporte de Calidad de Servicio está basado principalmente en dos arquitecturas estándar: La arquitectura de Servicios Integrados (IntServ) y la Arquitectura de Servicios Diferenciados (DiffServ). La Arquitectura de Servicios

Integrados es utilizada principalmente en Redes de Acceso debido a que se adapta fácilmente a las necesidades de recursos de los usuarios pero a su vez tiene problemas de escalabilidad debido al agotamiento de los recursos de la red.

Por otro lado, la Arquitectura de Servicios Diferenciados es muy escalable (soporta una gran cantidad de usuarios) pero a cambio, no puede adaptarse fácilmente a las necesidades de recursos de los usuarios. Por tanto, DiffServ es utilizada principalmente en Redes de Transporte. Una tercera parte dentro de este escenario son las redes MPLS que soportan los principios de Ingeniería de tráfico.

Adicionalmente," MPLS puede complementarse con la Arquitectura de Servicios Integrados o con la Arquitectura de Servicios Diferenciados para soportar QoS de una mejor manera en una Internet. Estas tecnologías se explicarán a continuación" (Deering, 2002, p. 77).

2.2.26 IntServ.

El modelo de arquitectura IntServ estuvo motivado por las necesidades de las aplicaciones en tiempo real, como video remoto, conferencia multimedia, visualización y realidad virtual. Proporciona una forma de ofrecer la calidad de servicio (QoS) de extremo a extremo que requieren las aplicaciones en tiempo real mediante la gestión explícita de los recursos de red para proporcionar QoS a flujos de paquetes de usuarios específicos. Utiliza la reserva de recursos y los mecanismos de control de admisión como bloques de construcción clave para establecer y mantener la QoS.

IntServ utiliza el Protocolo de reserva de recursos (RSVP) para señalar explícitamente las necesidades de QoS del tráfico de una aplicación a lo largo de los dispositivos en la ruta de extremo a extremo a través de la red. Si cada dispositivo de red a lo largo de la ruta puede reservar el ancho de banda necesario, la aplicación de origen puede comenzar a transmitir. RSVP no transporta datos de aplicaciones, sino que es más bien un protocolo de control de Internet, como el Protocolo de mensajes de control de Internet (ICMP), el Protocolo de administración de grupos de Internet

(IGMP) o los protocolos de enrutamiento. RSVP también se conoce como Protocolo de configuración de reserva de recursos (RSVP).

RSVP es utilizado por un host para solicitar QoS específicos de la red para el flujo o flujo de datos de la aplicación en particular. La solicitud de RSVP generalmente resulta en la reserva de recursos en cada nodo a lo largo de la ruta de datos.

- **Arquitectura RVSP**
- Sesión RVSP: es un flujo de datos para el que se ha requerido reserva de recursos, identificado por su destino y por un protocolo de transporte particular. Sus componentes son:
  - Dirección IP destino: dirección IP destino de los paquetes (unicast o multicast).
  - Identificador del protocolo IP transporte.
  - Puerto destino (opcional).
- Descriptor de flujo: se llama así a una petición de reserva realizada por un sistema final. Está compuesto de:
  - Flowspec: especifica la calidad de servicio deseada. Incluye:
    - Dos parámetros numéricos: Rspec, que define especiaciones de reserva requerida (Reserve) y Tspec, que describe el flujo de datos del emisor (Traffic)
- Especificación de filtro *(*filterspec*):* define los paquetes de datos que reciben la QoS especificada en el flowspecs.
- Merging: en los diferentes nodos que se van atravesando en la red por el camino de datos, se va realizando un proceso de concentración de los diferentes mensajes de petición de reservas.
- Estado de reserva en cada nodo: el softstate RSVP se crea y refresca periódicamente por mensajes Path y Resv.

- Estilos de reserva: una petición de reserva incluye un conjunto de opciones que se conocen como el estilo de reserva. Las distintas combinaciones de estas opciones conforman los tres estilos de reserva en uso, Wildcar-Filter (WF), Fixed-Filter (FF) y Shared-Explicit (SE).
    - WildcardFilter: todos los receptores comparten una reserva, cuyo tamaño es el mayor de las solicitudes de recursos de los receptores. Todos los emisores pueden usar recursos reservados.
    - Fixed-Filter: sólo el emisor o emisores especificados en este tipo de reserva, pueden usar los recursos reservados.
    - SharedExplicit: se crea una reserva única compartida por los emisores seleccionados.

- **Mensajes RSVP**

Hay dos tipos de mensajes generales en RSVP, PATH y RESV. La solicitud inicial comienza con un mensaje PATH. El mensaje PATH describe el flujo específico que utilizará esta reserva. Por lo tanto, incluye las direcciones IP de origen y destino, así como el protocolo IP, como TCP o UDP, y cualquier número de puerto. El mensaje PATH también incluye la velocidad de bits promedio solicitada y el tamaño de ráfaga.

El mensaje PATH es recibido por un enrutador ascendente, o quizás por el destino final. Si es recibido por un enrutador intermedio, este debe analizar la solicitud y decidir si puede cumplirla. En última instancia, si la solicitud es aceptada, el enrutador creará un nuevo mensaje PATH, solicitando la misma reserva de recursos del siguiente enrutador ascendente, pero especificándose como la fuente. Los mensajes PATH siempre fluyen desde el solicitante hacia el destino. En general, sin especificar tipos de QoS un mensaje Path, contiene:

- Sender Template: Parámetro por el cual se describe el formato de los paquetes que el emisor generará.
- Sender Tspec: Describe el tráfico que la aplicación estima que generará.

- Adspec: Información sobre la QoS y propiedades de la aplicación.
- Dirección del PHOP: Necesaria para poder encaminar los mensajes Resv.

Los mensajes RESV fluyen en la dirección opuesta. Los mensajes CONFIRMAR RESV describen la velocidad de bits detallada real y las características de retardo requeridas para cumplir con la solicitud PATH. Si un enrutador ascendente no tiene el recurso necesario para cumplir con la solicitud, responde con un mensaje RESV ERROR.

- **Funcionamiento de RVSP**

Un host de RSVP que necesita enviar un flujo de datos con QoS específica transmitirá un mensaje de ruta de RSVP cada 30 segundos que viajará a lo largo de las rutas de unidifusión o multidifusión preestablecidas por el protocolo de enrutamiento de trabajo. Si el mensaje de ruta llega a un enrutador que no comprende RSVP, ese enrutador reenvía el mensaje sin interpretar el contenido del mensaje y no reservará recursos para el flujo.

Aquellos que desean escucharlos envían un mensaje correspondiente de resv (abreviatura de "Reserva") que luego rastrea el camino hacia el remitente. El mensaje resv contiene las especificaciones de flujo. Cuando un enrutador recibe el mensaje de resv de RSVP:

- Hacer una reserva basada en los parámetros de solicitud. Para esto, el control de admisión y el control de la política procesan los parámetros de solicitud y pueden indicar al clasificador de paquetes que maneje correctamente el subconjunto seleccionado de paquetes de datos o negociar con la capa superior cómo debe realizarse el manejo del paquete. Si no pueden admitir la reserva solicitada, envían un mensaje de rechazo para avisar al oyente.
- Reenvíe la solicitud en sentido ascendente (en la dirección del remitente). En cada nodo, el mensaje resv, flowpec puede ser modificado por un nodo de

reenvío (por ejemplo, en el caso de una reserva de flujo de multidifusión, las solicitudes de reserva pueden fusionarse).

- Los enrutadores almacenan la naturaleza del flujo y también la controlan. Todo esto se hace en estado suave, por lo que si no se escucha nada durante un período de tiempo determinado, el lector se desconectará y la reserva se cancelará. Esto resuelve el problema si el remitente o el receptor se bloquean o se cierran incorrectamente sin cancelar primero la reserva. Los enrutadores individuales pueden, a su elección, controlar el tráfico para verificar que cumpla con las especificaciones de flujo.

2.2.26 DiffServ

Differentiated Services es un protocolo de QoS propuesto por IETF en el RFC 2475 y RFC 2474 que permite distinguir diferentes clases de servicio marcando los paquetes. Consiste en un método para marcar o etiquetar paquetes, permitiendo a los routers modificar su comportamiento de envío. Cada tipo de etiqueta representa un determinado tipo de QoS y el tráfico con la misma etiqueta se trata de la misma forma. DiffServ divide el tráfico en unas pocas clases y los recursos se asignan con base a las clases (y no a los flujos individuales como IntServ), lo que hace que esta arquitectura no sufra el problema de agotamiento de recursos de la red.

La arquitectura DiffServ define el campo DiffServ (DS), que reemplaza al campo ToS en IPv4 para tomar decisiones de **comportamiento por salto** (per-hop behaviour, PHB) sobre la clasificación de paquetes y las funciones de acondicionamiento de tráfico, como medición, marcado, conformado y vigilancia. (ver figura 13).

Figura 13. Campo DiffServ.

Fuente:https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-policing/28882-carcounters.html (2015).

El campo DiffServ estandarizado del paquete se marca con un valor para que el paquete reciba un tratamiento de reenvío particular o PHB, en cada nodo de la red.

El DSCP predeterminado es 000 000. Los DSCP de selector de clase son valores que son compatibles con versiones anteriores con IP precedente. Al convertir entre la precedencia de IP y DSCP, se haga coincidir los tres bits más significativos.

Caracteristicas de DiffServ

- Toma ventaja de las propiedades escalables de las herramientas QoS basadas en clases para diferencias entre tipos de paquetes, con la meta de “diferenciar servicios en Internet”.
- En una red simple, los paquetes deberían ser marcados al ingreso a un punto dentro de la red, con otros dispositivos realizando elecciones QoS basados en el campo marcado.
- El campo marcado estará en el encabezado IP y no en el encabezado de la capa de enlace de datos, ya que el encabezado IP permanece a lo largo de toda la red.
- Entre redes, los paquetes pueden ser reclasificados y remarcados al ingresar dentro de otra red.
- Para facilitar el marcado, el encabezado IP ha sido redefinido al incluir un campo de 6 bits llamado DSCP, el cual permite 64 clasificaciones diferentes.

2.2.27 Arquitectura DiffServ

- **Routers**

Para el control del tráfico DiffServ tiene dos tipos de enrutadores:

- Routers frontera: los nodos frontera y los nodos interiores .Solo los nodos frontera clasifican tráfico y marcan paquetes.
- Routers intermedios: mientras que los nodos interiores usan las clases codificadas en la cabecera del paquete (llamadas clases de retransmisión o forwarding equivalence class) para determinar el tratamiento de los paquetes.

- **Clasificación y marcado de paquetes**

El tráfico de red que ingresa a un dominio DiffServ está sujeto a clasificación y condicionamiento. Un clasificador de tráfico puede inspeccionar muchos parámetros diferentes en los paquetes entrantes, como la dirección de origen, la dirección de destino o el tipo de tráfico y asignar paquetes individuales a una clase de tráfico específica. Los clasificadores de tráfico pueden respetar cualquier marca DiffServ en los paquetes recibidos o pueden optar por ignorar o anular esas marcas. (Ver tabla 2)

El comportamiento por salto está determinado por el campo DS en el encabezado IP. El campo DS contiene el valor DSCP de 6 bits. La Notificación de congestión explícita (ECN) ocupa los 2 bits menos significativos del campo TOS de IPv4 y el campo de clase de tráfico (TC) de IPv6. En la práctica, la mayoría de las redes utilizan los siguientes comportamientos por salto comúnmente definidos:

- PHB de reenvío predeterminado (DF), que generalmente es el tráfico de mejor esfuerzo.
- PHB de reenvío acelerado (EF): dedicado al tráfico de baja pérdida y baja latencia.
- PHB de Envío seguro (AF) : garantiza la entrega en las condiciones prescritas
- Selector de clase PHBs, que mantienen la compatibilidad entre el campo DSCP y el campo de precedencia de IP.

Tabla 2. Niveles de Precedencia.

Nivel de precedencia	Descripción
7	Se mantiene igual (la capa de enlace y el protocolo de enrutamiento se mantienen activos)
6	Permanece igual (usado para protocolos de enrutamiento IP)
5	Reenvió exprés (EF)
4	Clase 4
3	Clase 3
2	Clase 2
1	Clase 1
0	Mejor esfuerzo

Fuente. José Escalona (2019).

- **Reenvió por defecto**

Un PHB de reenvío predeterminado (DF) es el único comportamiento requerido. Esencialmente, cualquier tráfico que no cumpla con los requisitos de cualquiera de las otras clases definidas usa DF. Normalmente, DF tiene las mejores características de reenvío de esfuerzo. El DSCP recomendado para DF es 0.

- **Expedición expedita**

El IETF define el comportamiento del reenvío acelerado EF en RFC 3246. El EF PHB tiene las características de bajo retardo, baja pérdida y bajo jitter. Estas características son adecuadas para servicios de voz, video, conexión punto a punto y otros servicios en tiempo real. El tráfico EF a menudo recibe una prioridad estricta en la cola sobre todas las demás clases de tráfico. Debido a que una sobrecarga de tráfico de EF causará demoras en la cola y afectará la fluctuación y la tolerancia de retardo dentro de la clase, el tráfico de EF a menudo se controla estrictamente a través del control de admisión, vigilancia y otros mecanismos. . El DSCP recomendado para el reenvío acelerado es 101110 en decimal es 46 y hexadecimal 2E.

- **Reenvió Asegurado**

El IETF define el comportamiento de reenvío asegurado en RFC 2597 y RFC 3260. El reenvío asegurado permite proporcionar seguridad de entrega garantizando una cierta cantidad de ancho de banda a una clase de AF y permite el acceso a un ancho de banda adicional, si está disponible de lo contrario existe la posibilidad de una caída del paquete. (Ver tabla 4)

Hay cuatro clases de AF, AF1x a AF4x. Dentro de cada clase, hay tres probabilidades de caída. Dependiendo de la política de una red dada, los paquetes pueden seleccionarse para un PHB en función del rendimiento requerido, demora, fluctuación, pérdida o según la prioridad de acceso a los servicios de red.

Las clases 1 a 4 se denominan clases de AF. La siguiente tabla ilustra la codificación DSCP para especificar la clase AF con la probabilidad. Los bits DS5, DS4 y DS3 definen la clase; los bits DS2 y DS1 especifican la probabilidad de caída; el bit DS0 siempre es cero.

Tabla 3. Grupos de comportamiento de reenvío asegurado (AF).

	Clase 1	**Clase 2**	**Clase 3**	**Clase 4**
Baja probabilidad de caída	AF11 (DSCP 10)	AF21 (DSCP 18)	AF31 (DSCP 26)	AF41 (DSCP 34)
Probabilidad de caída media	AF12 (DSCP 12)	AF22 (DSCP 20)	AF32 (DSCP 28)	AF42 (DSCP 36)
Alta probabilidad de caída	AF13 (DSCP 14)	AF23 (DSCP 22)	AF33 (DSCP 30)	AF43 (DSCP 38)

Fuente. José Escalona (2019).

Alguna medida de prioridad y equidad proporcional se define entre el tráfico en diferentes clases. En caso de que se produzca congestión entre las clases, se da

prioridad al tráfico en la clase más alta. En lugar de utilizar una cola de prioridad estricta, es probable que se utilicen algoritmos de servicio de cola más equilibrados, como la cola justa o la cola justa ponderada (WFQ). Si se produce una congestión dentro de una clase, los paquetes con mayor prioridad de descarte se descartan primero. Para evitar problemas asociados con la caída de la cola

- **Selector de Clase**

Antes de DiffServ, las redes IPv4 podían usar el campo Precedencia en el byte ToS del encabezado IPv4 para marcar el tráfico de prioridad. El octeto ToS y la precedencia de IP no se utilizaron ampliamente. El IETF acordó reutilizar el octeto ToS como el campo DS para redes DiffServ. Con el fin de mantener la compatibilidad con los dispositivos de red que aún utilizan el campo de Precedencia, DiffServ define el PHB Selector de clase.

Los puntos de código del selector de clase son de la forma binaria 'xxx000'. Los tres primeros bits son los bits de precedencia IP. Cada valor de precedencia de IP se puede asignar a una clase DiffServ. CS0 es igual a IP precedencia 0, CS1 a IP precedencia 1, y así sucesivamente. Si se recibe un paquete de un enrutador que no es compatible con DiffServ que usó marcas de precedencia IP, el enrutador DiffServ todavía puede entender la codificación como un punto de código de selector de clase.

2.2.28 Administración de congestión y colas

La espera es diseñada para acomodar la congestión temporal en una interfaz de dispositivo de red salvando los paquetes en exceso en los buffers hasta que el ancho de banda esté disponible.

El mecanismo predeterminado en la mayoría de las interfaces es Primero en entrar primero en salir (FIFO). Algunos tipos de tráfico tienen requisitos de retardo/fluctuación más exigentes. De esta manera, uno de los siguientes mecanismos alternativos para formar la cola se deben configurar o habilitar por defecto:

- Weighted Fair Queueing (WFQ)
- Class-Based Weighted Fair Queueing (CBWFQ)

- Almacenamiento en cola con latencia baja (LLQ), que en realidad es CBWFQ con cola de prioridades (PQ) (conocido como PQCBWFQ)
- Envío a cola prioritario (PQ)
- Almacenamiento en cola personalizado (CQ)

2.2.29 Calidad de servicio en MPLS

Se implementara como tecnología de soporte de QoS, DiffServ para construir el modelo de simulación, logrando así implementar QoS en MPLS permitiéndoles a los administradores de red proporcionar tipos diferenciados de servicio a través de una red MPLS. El servicio diferenciado satisface una variedad de requisitos al suministrar para cada paquete transmitido el tipo particular de servicio especificado para ese paquete por su QoS. El servicio se puede especificar de diferentes maneras, por ejemplo, utilizando la configuración de bits de precedencia de IP en los paquetes de IP.

Al proporcionar un servicio diferenciado, MPLS QoS ofrece clasificación de paquetes, evitación de congestión y gestión de congestión. La tabla 4 enumera estas funciones y sus descripciones.

Cuando se envían paquetes IP de un sitio a otro, el campo de precedencia de IP (los primeros tres bits del campo DSCP en el encabezado de un paquete IP) especifica la QoS. Sobre la base de la marca de precedencia IP, el paquete recibe el tratamiento deseado, con el porcentaje de ancho de banda permitido para esa calidad de servicio. Si la red del proveedor de servicios es una red MPLS, los bits de precedencia de IP se copian en el campo EXP MPLS en el borde de la red. Sin embargo, es posible que el proveedor de servicios desee establecer una QoS para un paquete MPLS en un valor diferente determinado por la oferta del servicio. (ver tabla 4)

Tabla 4. Proceso de QoS en MPLS.

Servicio	Función QoS	Descripción
Clasificación de paquetes	Tasa de acceso comprometida (CAR por sus siglas en ingles). Los paquetes se clasifican en el borde de la red antes de asignar las etiquetas.	Clasifica los paquetes de acuerdo a las tasas de transmisión de entrada o salida. Le permite configurar los bits experimentales de MPLS o los bits de precedencia de IP o DSCP (lo que sea apropiado).
Evitar la congestión	Detección temprana aleatoria ponderada (WRED por su siglas en ingles). Las clases de paquetes se diferencian en función de la probabilidad de caída.	Supervisa el tráfico de red para evitar la congestión al eliminar paquetes según la Precedencia de IP o los bits DSCP o el campo experimental MPLS.
Gestión de la congestión	CBWFQ. Las clases de paquetes se diferencian según el ancho de banda y el retardo acotado.	Un sistema de programación automatizada que utiliza un algoritmo de cola para asegurar la asignación de ancho de banda a diferentes clases de tráfico de red.

Fuente. José Escalona (2019).

Esta característica le permite al proveedor de servicios configurar el campo experimental MPLS en lugar de sobrescribir el valor en el campo de precedencia IP que pertenece a un cliente. El encabezado IP permanece disponible para el uso del cliente; la calidad del servicio de un paquete IP no se modifica a medida que el paquete viaja a través de la red MPLS. La Figura 14 muestra una red MPLS que conecta dos sitios de una red IP que pertenece a un cliente.

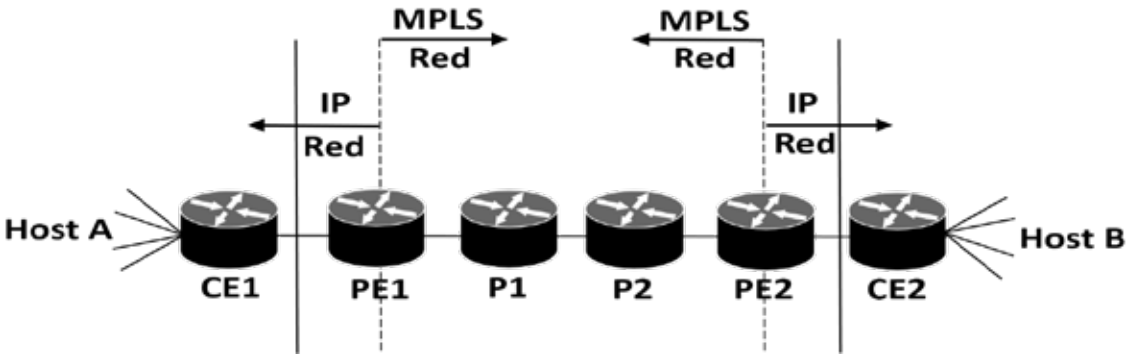


Figura 14. Red MPLS.

Fuente:https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-policing/28882-carcounters.html (2015).

En la Figura 14, los símbolos tienen los siguientes significados que se muestran en la Tabla 5.

Tabla 5. Símbolos del dispositivo.

Símbolo	Significado
CE1	Enrutador Perimetral del Cliente1
PE1	Proveedor de servicios de enrutador de borde (ingreso LSR)
P1	Enrutador del proveedor de servicios dentro del núcleo de la red del proveedor de servicios
P2	Enrutador del proveedor de servicios dentro del núcleo de la red del proveedor de servicios
PE2	Proveedor de servicios de enrutador de borde (egreso LSR)
CE2	Enrutador Perimetral del Cliente2

Fuente. José Escalona (2019)

En la figura 14, ocurre el siguiente comportamiento:

- Los paquetes llegan como paquetes IP a PE1, el enrutador perimetral del proveedor (también conocido como enrutador de conmutación de etiquetas de ingreso).
- PE1 envía los paquetes como paquetes MPLS.
- Dentro de la red del proveedor de servicios, *no hay un campo de precedencia de IP* para que el mecanismo de cola pueda verlo porque los paquetes son paquetes MPLS. Los paquetes siguen siendo paquetes MPLS hasta que llegan a PE2, el enrutador perimetral del proveedor.
- PE2 elimina la etiqueta de cada paquete y reenvía los paquetes como paquetes IP.

Esta mejora de la calidad de servicio de MPLS permite a los proveedores de servicios clasificar los paquetes según su tipo, interfaz de entrada y otros factores al configurar (marcar) cada paquete dentro del campo experimental de MPLS sin cambiar la precedencia de IP o el campo DSCP. Por ejemplo, los proveedores de servicios pueden clasificar los paquetes con o sin considerar la velocidad de los paquetes que recibe PE1.

2.2.30 Simulación y Modelo

La simulación es uno de los métodos cuantitativos más ampliamente utilizados para tomar decisiones. Es un método de aprender acerca de un método real experimentando con un modelo que representa el sistema. El modelo de simulación contiene las expresiones matemáticas y relaciones lógicas que describen cómo calcular el valor de los datos de salida dados los valores de los datos de entrada. Cualquier modelo de simulación tiene dos datos de entrada: controlables y probabilísticos.

Cuando realiza un experimento de simulación, un analista selecciona el valor, o valores, de los datos de entrada controlables. Luego los valores de los datos de entrada probabilísticos se generan al azar. El modelo de simulación utiliza los valores de datos de entrada controlables y los valores de los datos probabilísticos para

calcular el valor, o valores de los datos de salida. Realizando una serie de experimentos con varios valores de los datos de entrada controlables, el analista aprende cómo los valores de los datos controlables afectan o cambian el resultado del modelo de simulación.

Después de revisar los resultados de simulación, el analista con frecuencia es capaz de recomendar datos de entrada controlables que darán el resultado deseado del sistema real.

- **Etapas para realizar un estudio en simulación**
- Definición del sistema: consiste en estudiar el contexto del problema, identificar los objetivos del proyecto, especificar los índices de medición de la efectividad del sistema, establecer los objetivos específicos del modelamiento y definir el sistema que se va a modelar un sistema de simulación.
- Formulación del modelo: una vez definidos con exactitud los resultados que se espera obtener del estudio, se define y construye el modelo con el cual se obtendrán los resultados deseados. En la formulación del modelo es necesario definir todas las variables que forman parte de él, sus relaciones lógicas y los diagramas de flujo que describan en forma completa el modelo.
- Colección de datos: es importante que se definan con claridad y exactitud los datos que el modelo va a requerir para producir los resultados deseados.
- Implementación del modelo en la computadora: con el modelo definido, el siguiente paso es decidir qué lenguaje de programación (como Fortran, Algol, Lisp, entre otros.) o qué paquete de software se va a utilizar para procesar el modelo en la computadora y obtener los resultados deseados.
- Verificación: el proceso de verificación consiste en comprobar que el modelo simulado cumple con los requisitos de diseño para los que se elaboró. Se trata de evaluar que el modelo se comporta de acuerdo a su diseño.

- Validación del sistema: a través de esta etapa se valoran las diferencias entre el funcionamiento del simulador y el sistema real que se está tratando de simular. Las formas más comunes de validar un modelo son:
    - La opinión de expertos sobre los resultados de la simulación.
    - La exactitud con que se predicen datos históricos.
    - La exactitud en la predicción del futuro.
    - La comprobación de falla del modelo de simulación al utilizar datos que hacen fallar al sistema real.
    - La aceptación y confianza en el modelo de la persona que hará uso de los resultados que arroje el experimento de simulación
- Experimentación: la experimentación con el modelo se realiza después que este haya sido validado. La experimentación consiste en comprobar los datos generados como deseados y en realizar un análisis de sensibilidad de los índices requeridos.
- Interpretación: en esta etapa del estudio, se interpretan los resultados que arroja la simulación y con base a esto se toma una decisión. Es obvio que los resultados que se obtienen de un estudio de simulación colabora a soportar decisiones del tipo semi-estructurado.
- Documentación: dos tipos de documentación son requeridos para hacer un mejor uso del modelo de simulación. La primera se refiere a la documentación del tipo técnico y la segunda se refiere al manual del usuario, con el cual se facilita la interacción y el uso del modelo desarrollado.
- **Modelos de simulación**

La experimentación puede ser un trabajo de campo o de laboratorio. El modelo de método usado para la simulación seria teórico, conceptual o sistémico.

Después de confirmar la hipótesis podemos ya diseñar un teorema. Finalmente si este es admitido puede convertirse en una teoría o en una ley.

- Modelo teórico: el modelo teórico debe contener los elementos que se precisen para la simulación. Un ejemplo con trabajo de laboratorio es un programa de estadística con ordenador que genere números aleatorios y que contenga los estadísticos de la media y sus diferentes versiones: cuadrática-aritmética-geométrica-armónica. Además debe ser capaz de determinar la normalidad en términos de probabilidad de las series generadas. La hipótesis de trabajo es que la media y sus versiones también determinan la normalidad de las series. Es un trabajo experimental de laboratorio. Si es cierta la hipótesis podemos establecer la secuencia teorema, teoría, ley. Es el modelo principal de todo una investigación científica, gracias a ello podemos definir o concluir la hipótesis, las predicciones, etc.
- Modelo conceptual: desea establecer por un cuestionario y con trabajo de campo, la importancia de la discriminación o rechazo en una colectividad y hacerlo por medio de un cuestionario en forma de una simulación con una escala de actitud. Después de ver si la población es representativa o adecuada, ahora la simulación es la aplicación del cuestionario y el modelo es el cuestionario para confirmar o rechazar la hipótesis de si existe discriminación en la población y hacia qué grupo de personas y en que cuestiones. Gran parte de las simulaciones son de este tipo con modelos conceptuales.
- Modelo sistémico: el modelo sistémico se construye utilizando como metodología la dinámica de sistemas. Se simula el sistema social en una de sus representaciones totales. El análisis de sistemas es una representación total. Un plan de desarrollo en el segmento de transportes con un modelo de ecología humana, por ejemplo. El énfasis en la teoría general de sistemas es lo adecuado en este tipo de simulaciones. Este método, que es para un sistema complejo, es sumamente abstracto, y no se limita a la descripción del sistema, sino que debe incluir en la simulación las entradas y salidas de energía y los procesos de homeostasis (mecanismo autoregulatorio con el medio que rodea

al sujeto), de autopoiesis (capacidad de un sistema de reproducción y de mantenerse a si mismo) y de realimentación. Tanto el programa de estadística como la escala de actitud y el sistema total, son perfectas simulaciones de la realidad y modelizan todos los elementos en sus respectivas hipótesis de trabajo. Son también un microclima y el ambiente o el escenario en los procesos de simulación/experimentación. Otras propiedades que deben contener las simulaciones es que sean repetibles indefinidamente. Que eviten el efecto de aprendizaje que incita al encuestador a rellenar él mismo los cuestionarios y que se podrá evitar con algún control, que sean flexibles o mejorables y que no sea invasivo o cambiar la población de las muestras sucesivas.

- **Simulación por computadora**

Es un intento de modelar situaciones de la vida real por medio de un programa de computadora, lo que requiere ser estudiado para ver cómo es que trabaja el sistema. Ya sea por cambio de variables, quizás predicciones hechas acerca del comportamiento del sistema.

La simulación por computadora se ha convertido en una parte útil del modelado de muchos sistemas naturales en física, química y biología, y sistemas humanos como la economía y las ciencias sociales (sociología computacional), así como en dirigir para ganar la penetración (profundidad) su comportamiento cambiará cada simulación según el conjunto de parámetros iniciales supuestos por el entorno.

Tradicionalmente, el modelado formal de sistemas ha sido a través de un modelo matemático, que intenta encontrar soluciones analíticas a problemas que permiten la predicción del comportamiento de un sistema de un conjunto de parámetros y condiciones iniciales. La simulación por computadora es frecuentemente usada como un accesorio para, o sustitución de, sistemas de modelado para los cuales las soluciones analíticas de forma cerrada simple no son posibles. Ahí se encuentran muchos tipos diferentes de simulación por computadora, la

característica común que todas ellas comparten es el intento por generar una muestra de escenarios representativos para un modelo en que una enumeración completa de todos los estados posibles sería prohibitivos o imposibles. Varios paquetes de software existen para modelar por computadora, como Vensim, Stella o Powerim, y así la simulación se hace sin gran esfuerzo (por ejemplo: la simulación Montecarlo y el modelado estocástico como el Simulador de Riesgo).

Es cada vez más común escuchar acerca de simulaciones a muchas clases designadas como "ambientes sintéticos". Esta etiqueta ha sido adoptada al ampliar la definición de "simulación", que abarca virtualmente cualquier representación computarizada

2.2.31 Simulador GNS3

GNS3 es un software utilizado por cientos de miles de ingenieros de redes a nivel mundial para emular, configurar, probar y solucionar problemas de redes virtuales y reales. GNS3 le permite ejecutar una pequeña topología que consta de solo unos pocos dispositivos en su computadora portátil, a aquellos que tienen muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube.

GNS3 está activamente desarrollado y respaldado, y cuenta con una comunidad en crecimiento de más de 800,000 miembros. Al unirse a la comunidad GNS3 se unirá a otros estudiantes, ingenieros de redes, arquitectos y profesionales que han descargado GNS3 más de 10 millones de veces hasta la fecha. GNS3 se utiliza en empresas de todo el mundo, incluidas las compañías Fortune 500.

GNS3 puede ayudarlo a prepararse para exámenes de certificación como Cisco CCNA, pero también lo ayudará a probar y verificar implementaciones del mundo real. Jeremy Grossman, el desarrollador original de GNS3, creó el software para ayudarlo a estudiar sus certificaciones CCNP. Gracias a ese trabajo original, hoy se puede usar para ayudarlo a hacer lo mismo sin pagar costosos equipos.

GNS3 ha permitido a los ingenieros de red visualizar dispositivos de hardware reales durante más de 10 años. Originalmente solo emulaba dispositivos Cisco que usaban software llamado Dynamips, GNS3 ahora ha evolucionado y admite muchos

dispositivos de múltiples proveedores de red, incluidos conmutadores virtuales Cisco, Cisco ASA, Brocadev Routers, conmutadores Cumulus Linux, instancias Docker, HPE VSR, múltiples dispositivos Linux y muchos otros.

GNS3 no solo es compatible con dispositivos Cisco. A menudo se discute con Cisco porque eso es lo que la mayoría de los ingenieros de redes están interesados en conocer. Sin embargo, muchos otros proveedores comerciales y de código abierto son compatibles hoy con GNS3. Ahora puede probar la interoperabilidad entre muchos proveedores e incluso probar configuraciones esotéricas usando tecnologías de red con SDN, NFV, Linux y Docker.

- **arquitectura de GNS3**

GNS3 consta de dos componentes de software:

  - Software GNS3 todo en uno (GUI)
  - Servidor/Máquina Virtual GNS3

- **Software GNS3 todo en uno**

Esta es la interfaz gráfica de usuario (GUI) de GNS3 y la parte de software necesaria para la operación de GNS3. Este paquete instala el software todo en uno en su PC local (Windows, MAC, Linux), con lo cual puede crear sus topologías utilizando el software incluido.

- **Máquina Virtual GNS3**

Cuando se crea topologías en GNS3 se está utilizando la interfaz gráfica de usuario (GUI), los dispositivos creados deben estar alojados y ejecutados por una máquina virtual o servidor. Se tiene algunas opciones:

- **Servidor local GNS3**

Se ejecuta localmente en la misma PC donde instaló el software todo en uno GNS3. Si, por ejemplo, está utilizando una PC con Windows, tanto la GUI GNS3 como el servidor local GNS3 se están ejecutando como procesos en Windows. Procesos adicionales como Dynamips también se ejecutarán en su PC.

- **Máquina Virtual GNS3**

Si se decide usar la máquina virtual GNS3 (recomendado), puede ejecutar la máquina virtual GNS3 localmente en su PC utilizando software de virtualización como VMware Workstation o Virtualbox; o puede ejecutar la máquina virtual GNS3 de forma remota en un servidor utilizando VMwareESXi o incluso en la nube.

Usted puede usar GNS3 sin usar la máquina virtual GNS3. Esta es una buena manera de comenzar desde el principio, pero esta configuración es limitada y no ofrece tantas opciones con respecto al tamaño de topología y los dispositivos admitidos. Si desea crear topologías GNS3 más avanzadas o desea incluir dispositivos como los dispositivos Cisco VIRL (IOSvL2, IOSvL3, ASAv) u otros dispositivos que requieran Qemu, se recomienda la máquina virtual GNS3 (y a menudo se requiere).

- **Emulación y Simulación en GNS3**

GNS3 admite tanto dispositivos simulados como emulados.

GNS3 imita o emula el hardware de un dispositivo y ejecuta imágenes reales en el dispositivo virtual. Por ejemplo, puede copiar el IOS de Cisco desde un enrutador Cisco real y físico y ejecutarlo en un enrutador Cisco virtual emulado en GNS3.

GNS3 simula las funciones y la funcionalidad de un dispositivo como un interruptor. No está ejecutando sistemas operativos reales, como Cisco IOS, sino más bien un dispositivo simulado desarrollado por GNS3, como el conmutador GNS3 de capa 2.

- **Consideraciones entre la Simulación y Emulación en GNS3**

Las líneas entre la simulación y la emulación se difuminan un poco en estos días. Ahora puede ejecutar imágenes Cisco VIRL que son imágenes de imágenes reales del sistema operativo de Cisco que se ejecutan en hardware virtual estandarizado. GNS3 emula el hardware que requieren las imágenes VIRL para ejecutarse.

No se preocupe demasiado por la diferencia entre la simulación y la emulación, excepto en los siguientes puntos:

- Dynamips es una tecnología más antigua que emula el hardware de Cisco. Utiliza imágenes reales de Cisco IOS. Es bueno para las topologías de tipo CCNA básico, pero tiene una serie de limitaciones, como el hecho de admitir únicamente versiones anteriores de Cisco IOS (12.X) que tampoco son compatibles o están actualizadas activamente por Cisco.
- Las imágenes de Cisco recomendadas para usar con GNS3 son las de Cisco VIRL (IOSv, IOSvL2, IOS-XRv, ASAv). Estas imágenes son compatibles y Cisco las actualiza activamente. Las imágenes admiten versiones actuales de Cisco IOS (15.X) y brindan la mejor experiencia de usuario y escala.

- **Requerimientos del emulador, simulador de red GNS3**

GNS3 es una plataforma que permite simular topologías de red con imágenes de vendors como Cisco y Juniper, entre otros. A continuación se muestran los requerimientos para la instalación del software GNS3. Tutorial

- **Compatibilidad con Windows**

GNS3 es compatible con los siguientes sistemas operativos de Windows:

- Windows 7 SP1 (64 bit).
- Windows 8 (64 bit).
- Windows 10 (64 bit).
- Windows Server 2012 (64 bit).
- Windows Server 2016 (64 bit).

- **Requerimientos Mínimos**

Tabla 6. Requerimientos mínimos GNS3 para entorno Windows.

Ítem	Requerimientos Mínimos
Sistema Operativo	Windows 7 (64 bit) o superior
Procesador	2 o más núcleos lógicos
Virtualización	Se requieren extensiones de virtualización. Es posible que deba habilitar esto a través del BIOS de su computadora.
Memoria	4 GB RAM
Espacio en disco	1GB de espacio disponible (la instalación es < 200MB).
Notas adicionales	Es posible que necesite almacenamiento adicional para su sistema operativo e imágenes de los equipos.

Fuente: https://telectronika.com/articulos/que-es-gns3/

Los requisitos de hardware enumerados aquí son requisitos mínimos para un entorno GNS3 pequeño. Si desea crear entornos complejos con muchos dispositivos, sus requisitos de hardware aumentarán.

- **Requerimientos Recomendados**

Los siguientes son los requisitos recomendados para un entorno Windows GNS3:

Tabla 7. Requerimientos recomendados GNS3.

Ítem	Requerimientos Recomendados
Sistema Operativo	Windows 7 (64 bit) o superior
Procesador	4 o más núcleos lógicos – AMD-V / RVI Series o Intel VT-X / EPT
Virtualización	Se requieren extensiones de virtualización. Es posible que deba habilitar esto a través del BIOS de su computadora.
Memoria	16 GB RAM
Espacio en disco	Disco de Estado Sólido (SDD) 35 GB de espacio disponible
Notas adicionales	La virtualización de dispositivos consume mucho procesador y memoria, por lo tanto, más es mejor, tener en cuenta si el dispositivo configurado correctamente supera la RAM y la potencia de procesamiento.

Fuente: https://telectronika.com/articulos/que-es-gns3/

Los requisitos de hardware enumerados aquí son requisitos recomendados para un entorno pequeño GNS3. Si desea crear entornos complejos con muchos dispositivos, sus requisitos de hardware aumentarán.

- **Requerimientos Óptimos**

Los siguientes son los requisitos óptimos para un entorno Windows GNS3:

Tabla 8. Requerimientos óptimos GNS3.

Ítem	Requerimientos Óptimos
Sistema Operativo	Windows 7 (64 bit) o superior
Procesador	i7 CPU
Virtualización	8 o más núcleos lógicos – AMD-V / RVI Series o Intel VT-X / EPT
Memoria	Se requieren extensiones de virtualización. Es posible que deba habilitar esto a través del BIOS de su computadora.
Espacio en disco	32 GB RAM
Notas adicionales	Disco de Estado Sólido (SDD) 80 GB de espacio disponible
Adicional Notes	La virtualización de dispositivos consume mucho procesador y memoria, por lo tanto, más es mejor, tener en cuenta si el dispositivo configurado correctamente supera la RAM y la potencia de procesamiento.

Fuente: https://telectronika.com/articulos/que-es-gns3/

2.2.32 Definición de términos

Paquete: Se considera que un paquete es cada uno de los bloques en que se divide la información para enviar, corresponde a la capa de red del Modelo OSI, como por ejemplo, en el caso del protocolo IP. Siendo el paquete la unidad de datos de protocolo (PDU) de la capa de red.

Trama: en redes una trama es una unidad de envío de datos. Viene a ser el equivalente de paquete de datos o Paquete de red, en el Nivel de enlace de datos del modelo OSI.

Ethernet.

Protocolo: Es el conjunto de reglas que rigen la comunicación.

Red: Son múltiples computadoras conectadas entre ellas que utilizan un sistema de comunicaciones. Su objetivo es que las computadoras se comuniquen y compartan archivos.

Red de área local (LAN): Hace referencia a una red local o un grupo de redes locales interconectadas que están bajo el mismo control administrativo.

Red de área extensa (WAN): Es una Red que abarca un área geográfica más amplia que una red de área local (LAN) sobre redes de comunicaciones públicas.

Red de área metropolitana (MAN): Es una red que abarca una ciudad, está compuesta por diversos edificios interconectados mediante backbones inalámbricos o de fibra óptica.

Binario: Es el sistema de numeración que se caracteriza por los unos y los ceros (1=activado, 0=desactivado).

Bit: Es un dígito binario, que toma un valor de 0 ó 1. Son unidades de comunicación y almacenamiento de información en computación.

Bit más significativo: Es la posición de bit en un número binario que tiene el mayor valor. A veces se refiere al bit que se encuentra más a la izquierda.

WI-FI: Wifi es una tecnología de comunicación inalámbrica que permite conectar a internet equipos electrónicos, mediante el uso de radiofrecuencias o infrarrojos para la trasmisión de la información. Wifi o Wi-Fi es originalmente una abreviación de la marca comercial *Wireless Fidelity*

Router: Es un dispositivo de hardware que permite la interconexión de ordenadores en red. El router o enrutador es un dispositivo que opera en capa tres de nivel de 3. Así, permite que varias redes u ordenadores se conecten entre sí y, por ejemplo, compartan una misma conexión de Internet**.**

Buffer: Memoria de almacenamiento temporal de información que permite transferir los datos entre unidades funcionales con características de transferencia diferentes.

Switch: es un dispositivo que permite que la conexión de computadoras y periféricos a la red para que puedan comunicarse entre sí y con otras redes. Switch es una palabra en inglés usada en el área de informática para referirse al controlador de interconexión entre varios dispositivos

Backbone: se refiere a las principales conexiones troncales de Internet. Está compuesta de un gran número de routers comerciales, gubernamentales,

universitarios y otros de gran capacidad interconectados que llevan los datos a través de países, continentes y océanos del mundo mediante cables de fibra óptica.

Host: es un ordenador que funciona como el punto de inicio y final de las transferencias de datos. Más comúnmente descrito como el lugar donde reside un sitio web. Un host de Internet tiene una dirección de Internet única (dirección IP) y un nombre de dominio único o nombre de host.

CAPÍTULO III

MARCO METODOLÓGICO

Para Arias, F. (2012): “La metodología del proyecto incluye el tipo o tipos de investigación, las técnicas y los instrumentos que serán utilizados para llevar a cabo la indagación. Es el “cómo” se realizará el estudio para responder al problema planteado. (p. 111). Es así, como se da a conocer entonces en el presente capítulo, el abordaje metodológico llevado a cabo para abordar el problema planteado en cuanto al análisis del rendimiento de una red MPLS con calidad de servicio mediante un simulador GNS3. En este orden de ideas, el capítulo comprende todo lo referente al tipo, nivel y diseño de la investigación, población y muestra, así como técnicas e instrumentos de recolección de datos.

3.1 Tipo de Investigación

La investigación descriptiva, para Arias, F. (2012), “consiste en la caracterización de un hecho, fenómeno, individuo o grupo, con el fin de establecer su estructura o comportamiento. Los resultados de este tipo de investigación se ubican en un nivel intermedio en cuanto a la profundidad de los conocimientos se refiere”. (Pág. 24). Siendo el objetivo de la presente investigación, analizar el rendimiento de una red MPLS con calidad de servicio mediante el simulador GNS3, se busca describir los parámetros de desempeño y rendimiento de una red que utiliza el protocolo MPLS con calidad de servicio para entender el comportamiento de la misma, por tal razón, la presente investigación se adapta a lo descrito anteriormente por el autor y se desarrollara bajo el tipo Descriptivo.

3.2 Diseño de Investigación

Para Arias, F. (2012): “El diseño de investigación es la estrategia general que adopta el investigador para responder al problema planteado”. (Pág. 28). En este sentido, la presente investigación utilizo información brindada por el simulador GNS3 para analizar el rendimiento de una red MPLS con calidad de servicio, por

tanto, se apega a un diseño de investigación experimental, el cual se define según Hernández, Fernández y Baptista (2012), como “el diseño que se utiliza cuando el investigador pretende establecer el posible efecto de una causa que se manipula”. (pág. 123).

3.3 Nivel de Investigación

Según Arias (2012), el nivel de investigación puede definirse como “el grado de profundidad con que se aborda un objeto o fenómeno” (p.47). El tipo de investigación a realizar determina los niveles que es preciso desarrollar” (p.101). En este sentido, bajo la realidad de la problemática de investigación aquí planteada, el nivel de investigación bajo la cual se desarrolló la investigación es de campo, ya que según Arias (2012), es aquella “donde se recolectan los datos directamente de la realidad donde ocurren los hechos…, el investigador obtiene la información pero no altera las condiciones existentes.

Según lo citado por el autor, el análisis del rendimiento de una red MPLS con calidad de servicio mediante un simulador GNS3, permite recoger la información de forma directa y además se describió la conducta de la red sin alterar los resultados arrojados por el simulador. De forma tal que es el nivel que se adapta a la investigación presente.

3.4 Técnicas e Instrumentos de recolección de información.

Según Arias (2012), “Se entiende por técnica de investigación, el procedimiento o forma particular de obtener datos o información” (pág. 67). En el caso particular de la presente investigación, la técnica a utilizada fue la observación directa o estructurada, ya que el investigador se dispuso a observar el comportamiento de la red MPLS con calidad de servicio mediante la aplicación del simulador GNS3.

De la misma forma, en relación al instrumento a utilizar para la recolectar la información que permita el análisis del rendimiento de la red mencionada, se utilizó una lista de cotejo que permitio registrar el rendimiento de la red MPLS con calidad de servicio para determinar las ventajas del uso de este protocolo. Cabe destacar que el uso de este instrumento responde a lo planteado por Arias (2012), quien define que: "Un instrumento de recolección de datos es cualquier recurso, dispositivo o formato (en papel o digital), que se utiliza para obtener, registrar o almacenar información". (pág. 68)

3.5 Fases Metodológica

Fase I: Estudio de los fundamentos de MPLS en cuanto a estructura y diseño de red.

Para esta fase se investigarán e identificaron los fundamentos teóricos relacionados a las redes MPLS con calidad de servicio y se seleccionó el simulador a emplear que será el GNS3. Tal investigación se apoyó en las múltiples bibliografías que existen sobre la materia, en los recursos disponibles de la Universidad José Antonio Páez y en profesores expertos en el tema.

Posteriormente se filtró toda la información para resumir en los puntos más importantes sobre el método de detección de errores en estudio que fueron tomados en cuenta al momento de desarrollar el programa y el módulo detector de errores de manera que fueron expuestos en las prácticas de laboratorio de la materia transmisión de datos.

Fase II: Parámetros de calidad de servicio aplicables a una red basada en MPLS

En esta fase se determinaron los parámetros de calidad de servicio aplicables a una red basada en MPLS para tener los estándares de trabajo al momento de la aplicación del simulador GNS3

Fase III: Aplicación del simulador GNS3 a las redes basadas en MPLS con calidad de servicio

En esta fase se aplicó el GNS3 donde se simuló el rendimiento de la red MPLS con calidad de servicio para determinar los parámetros de la calidad de servicio aplicables a una red MPLS

Fase IV: Determinar los parámetros de desempeño y el rendimiento de una red MPLS con calidad de servicio

Se procedio a informar los parámetros de desempeño que tiene la red MPLS con calidad de servicio, estudiar los fundamentos en cuanto a estructura y diseño de red para finalmente dar el análisis del rendimiento de la red, dando así cumplimiento a los objetivos planteados en aras de dar una respuesta al problema planteado.

CAPÍTULO IV
RESULTADOS

4.1 Fase I: Estudio de los fundamentos de MPLS en cuanto a estructura y diseño de red.

Una vez estudiada la situación actual mediante distintos métodos como lo son la observación directa y el análisis de los puntos críticos, se logró determinar los aspectos más importantes que se desarrollaron en el proyecto.

4.1.1. Observación Directa.

La red a estudiar se construyó en base a una topología tipo malla en el núcleo de la red la cual permite que cada nodo esté conectado a todos los nodos de la red, de esta manera es posible llevar los mensajes de un nodo a otro nodo por distintos caminos y así evitar una interrupción en las comunicaciones. Debido a este criterio se aplicó como protocolo de IGP el protocolo OSPF el cual nos permite separar la red en áreas siendo nuestro núcleo de la red el área 0 y las áreas periféricas al núcleo de la red son la 1 ,2 y 99. También ofrece un balanceo de carga el cual permite el envío de paquetes repartido equitativamente entre todas las interfaces para evitar una congestión.

4.2. Fase II: Parámetros de calidad de servicio aplicables a una red basada en MPLS

Después de lograr el óptimo funcionamiento del protocolo OSPF, se implementó una política de calidad de servicio a lo largo de toda la red desde el marcado de paquetes por medio del protocolo DSCP hasta políticas QoS para el tráfico saliente de cada interfaz para darle prioridad a cierto tipo de tráfico sensible al retardo y congestiones. Por ultimo en el núcleo de la red (Área 0) se configuro el protocolo MPLS para aumentar el rendimiento de la misma.

4.2.1. Etapas de la simulación

Etapa 1.- Direccionamiento IP:

· Configuración y asignación de direcciones IP en todas las interfaces de la red, en la siguiente tabla se muestra el direccionamiento IP. Ver tabla 1

Tabla 09: de direccionamiento IP.

Dispositivo	Interfaz	Dirección IP	Mascara de Subred	Gateway predeterminado	Servidor DNS
R1	Gig. 0/0	192.168.1.1	255.255.255.240	No aplicable	No aplicable
	Gig. 0/0	192.168.1.17	255.255.255.240	No aplicable	No aplicable
R2	Gig. 0/0	192.168.1.30	255.255.255.240	No aplicable	No aplicable
	Gig. 1/0	192.168.1.229	255.255.255.252	No aplicable	No aplicable
	Gig. 2/0	192.168.1.233	255.255.255.252	No aplicable	No aplicable
	Gig. 3/0	192.168.1.249	255.255.255.252	No aplicable	No aplicable
R3	Gig. 0/0	192.168.1.230	255.255.255.252	No aplicable	No aplicable
	Gig. 0/1	192.168.1.241	255.255.255.252	No aplicable	No aplicable
R4	Gig. 0/0	192.168.1.234	255.255.255.252	No aplicable	No aplicable
	Gig. 1/0	192.168.1.237	255.255.255.252	No aplicable	No aplicable
	Gig. 2/0	201.211.202.1	255.255.255.0	No aplicable	No aplicable
R5	Gig. 0/0	192.168.1.250	255.255.255.252	No aplicable	No aplicable
	Gig. 0/1	192.168.1.253	255.255.255.252	No aplicable	No aplicable
R6	Gig. 0/0	192.168.1.238	255.255.255.252	No aplicable	No aplicable
	Gig. 1/0	192.168.1.242	255.255.255.252	No aplicable	No aplicable
	Gig. 2/0	192.168.1.49	255.255.255.240	No aplicable	No aplicable
	Gig. 3/0	192.168.1.254	255.255.255.252	No aplicable	No aplicable
R7	Gig. 0/0	192.168.1.62	255.255.255.240	No aplicable	No aplicable
	Gig. 0/1	192.168.1.33	255.255.255.240	No aplicable	No aplicable

ISP	Gig. 0/0	201.211.202.2	255.255.255.0	No aplicable	No aplicable
	Gig. 0/1	10.8.1.1	255.255.255.0	No aplicable	No aplicable
R9 (Internet)	Gig. 0/0	10.8.2.1	255.255.255.0	No aplicable	No aplicable
	Gig. 1/0	10.8.1.2	255.255.255.0	No aplicable	No aplicable
	Gig. 2/0	10.8.3.1	255.255.255.0	No aplicable	No aplicable
	Lo1.	172.16.2.1	255.255.255.255	No aplicable	No aplicable
Servidor HTTP	Fa. 0	10.8.2.2	255.255.255.0	10.8.2.1	10.8.3.2
Servidor DNS	Fa. 0	10.8.3.2	255.255.255.0	10.8.3.1	No aplicable
SW1	Fa. 0/24	No aplicable	No aplicable	192.168.1.1	No aplicable
SW2	Fa. 0/24	No aplicable	No aplicable	192.168.1.33	No aplicable
PC-1	Fa. 0	192.168.1.14	255.255.255.240	192.168.1.1	10.8.3.2
PC-2	Fa. 0	192.168.1.46	255.255.255.240	192.168.1.33	10.8.3.2

Etapa 2.- Configuración de OSPF como protocolo de enrutamiento:

· Se configura OSPF en 4 áreas.

· El área 1 y 2 como áreas totally-stup, área 0 (núcleo de la red) y área 99 (área standard).

· Se configuro la elección de un DR y BDR en cada interfaz, en las la int. Gig 0/0 en el R1 y la int. Gig. 0/1 en el R2 solo hay la elección de un DR no hay BDR.

· Se definió una velocidad de referencia en cada área. En área 1, 2 y 99 la velocidad de referencia es 100Mpbs y en el área 0 1000Mbps. Por lo que la métrica llamada cost en OSPF es 1 en toda la red.

· Tanto como el área 1 y 2 se configuraron interfaces pasivas las cuales son la int. Gig 0/0 en el R1 y la int. Gig. 0/1 en el R2.

· Se aplicó una codificación de mensajes MD5 en cada interfaz de la red mediante el protocolo OSPF, las únicas interfaces que no se les aplico son la int. Gig 0/0 en el R1 y la int. Gig. 0/1 en el R2.

· Se configuro una ruta por defecto en el router ISP en la int. Gig. 0/1 para simular una conexión a internet y se distribuyó por toda el dominio OSPF, es decir, cuando un equipo se quiere comunicar con una red y no se encuentra en el dominio OSPF el paquete será enviado por ahí.

· También se configuro una ruta estática en el router ISP que se distribuyó por todo el dominio OSPF. La cual corresponde a una dirección loopback del router 0 dentro del cluster.

· Se creó un cluster para simular internet dentro del cual tenemos internet mediante una conexión DSL y que nos comunica con servidor DNS y un servidor HTTP. En el servidor HTTP se configuro una página mediante HTML con un parecido a Google y en el servidor DNS su respectiva dirección IP, esto se hizo para realizar pruebas. Ver figura 15

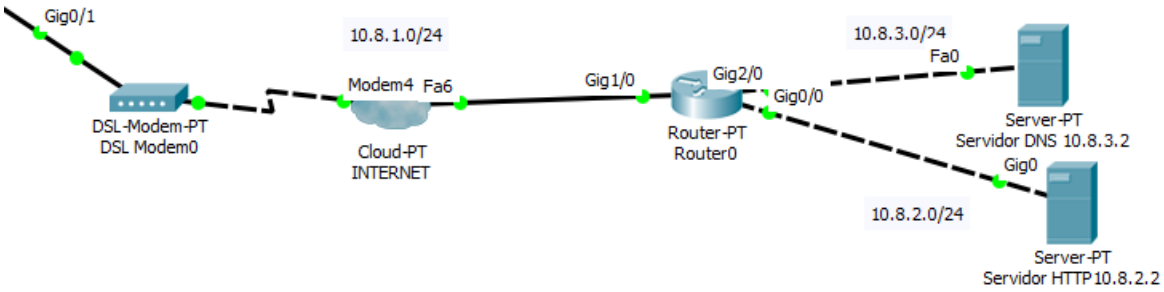


Figura 15: pruebas
Fuente: José Escalona

Etapa 3.- Configuración de una política de calidad de servicio:

· Clasificación de trafico
  - o Crear lista de acceso para definir el tráfico de VOIP y Video Streaming.
  - o Crear Clases para definir tráfico HTTP, Telnet, SSH, FTP, TFTP, IMAP, POP3, SMTP.

· Política de Marcado de paquetes configurados en las int. Gig. 0/0 del R1 área 1, int. Gig. 0/1 del R7 área 2 y int. Gig. 2/0 del R4 área 99.

· Política QoS para tráfico saliente de todas las interfaces.

- Política QoS para Tráfico de subida y bajada de nuestro ISP, configurado en la int. Gig. 0/0 del ISP área 99.
- Aplicar políticas en las interfaces correspondientes.

Etapa 4.- Configuración de MPLS en el núcleo de la red (área 0).

Etapa 5.- Configuraciones inicialices de un router y switch:

- Configuración de contraseñas de niveles de seguridad.
- Configuración de mensaje de seguridad.
- Configuración de tiempo de sesión de niveles de seguridad.
- Configuración de evitar la búsqueda DNS en líneas de comando.

4.2.2 Simulaciones paralelas

Se simulo la misma topología de red en dos simuladores diferentes los cuales son:

1.- Packet Tracert.

2.- GNS3.

Esto debido que el simulador Packet Tracert no soporta el protocolo MPLS, en el simulador Packet Tracert se pudo configurar un protocolo de enrutamiento llamado OSPF y calidad de servicio, mientras en GNS3 se configuro lo mismo y adicional el protocolo MPLS con algunos cambios en la configuración de calidad de servicio y el cluster que simula internet en Packet Tracert.

4.2.2.1 Red simulada en Packet Tracert:

En esta simulación se configura como IGP el protocolo OSPF el cual se dividió en 4 áreas, las cuales son área 1 área, 2 área 0 y área 99 para lograr un mejor rendimiento y descentralizar todo el enrutamiento de la red, el núcleo de la red es el área 0 que por medio de ella se logra comunicación entre las demás áreas. En el área 0 se aplicó el concepto de redundancia el cual se basa en más conexiones para evitar que si se cae una interfaz no se pierda la comunicación. Ver en figura 16

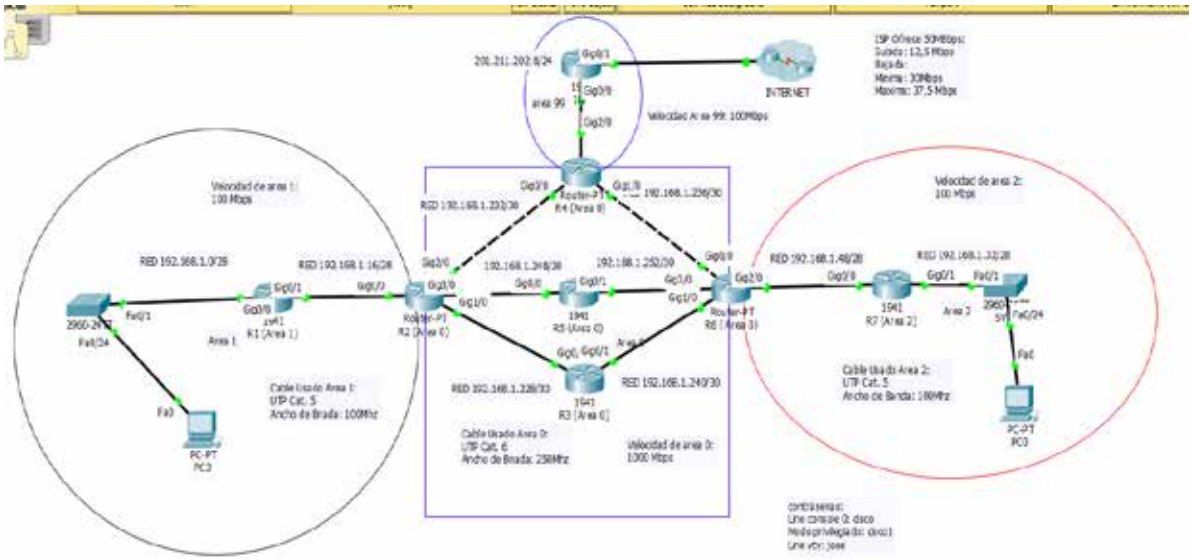


Figura 16: ***Red simulada en Packet Tracert***
Fuente: José Escalona

Configuración de OSPF como protocolo de enrutamiento

Especificaciones OSPF del área 1:

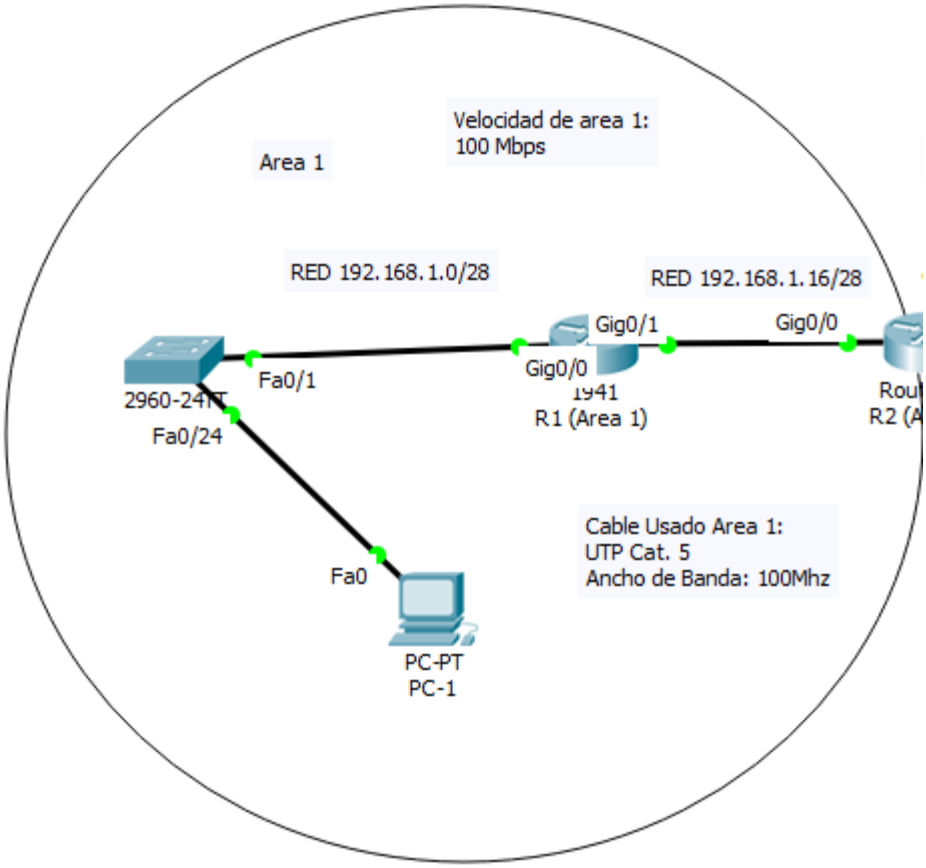
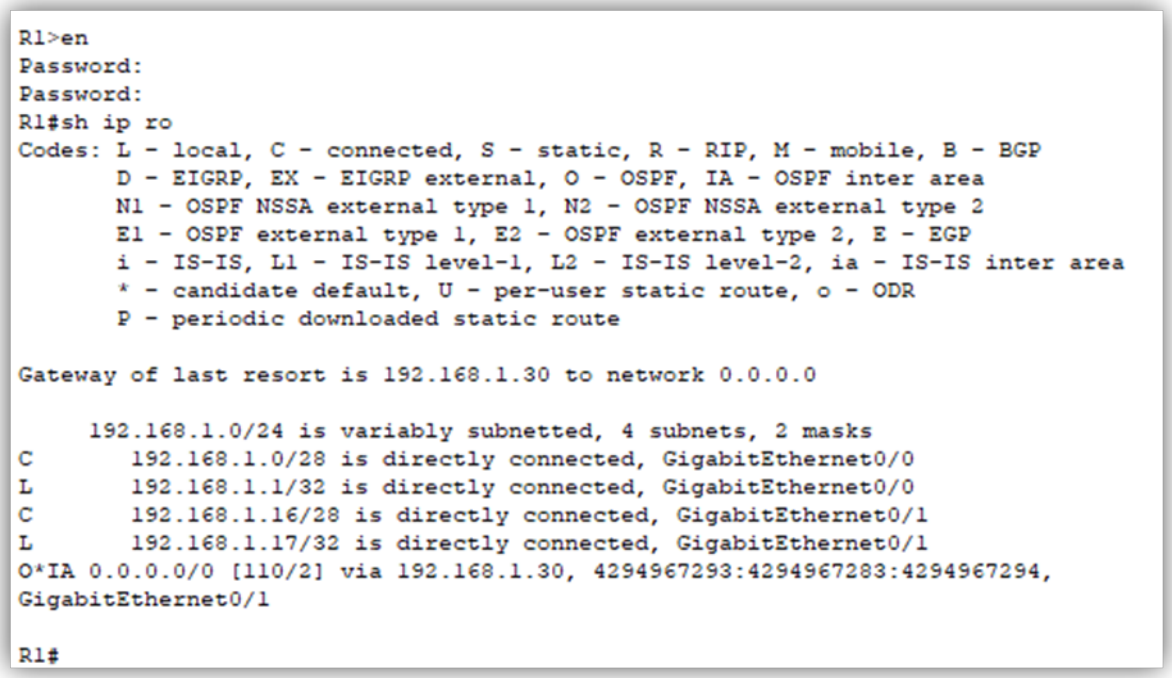


Figura 17: Área 1
Fuente: José Escalona

- Cada interfaz del área 1 tiene un ancho de banda de 100Mbps y son full dúplex.
- Los routers involucrados en esta área son el router 1 y 2, donde el router 1 es un router interno del área mientras el router 2 es un ABR debido que comunica el área 1 con el área 0.
- La interfaz Gig. 0/0 del router R1 se configuro como interfaz pasiva, es decir, no se enviaran mensajes OSPF a través de ella.
- En OSPF se pueden configurar diferentes tipos de áreas para simplificar las tablas de enrutamiento, en el área 1 se configuro un tipo de área totally-stub la cual crea una ruta por defecto en la tabla de enrutamiento a través del ABR del área en este casa del R2 para comunicarse con las direcciones IP de otras áreas

u otros sistemas autónomos, es decir, la aplicación de este tipo de área quita los mensajes LSA tipo 3 y tipo 5 del protocolo OSPF que corresponden a direcciones IP de otras áreas (tipo 3) y direcciones IP de otros sistemas autónomos (tipo 5). En la tabla de enrutamiento de la imagen 4 podemos observar que la ruta por defecto se creó a través de la int. Gig. 0/1 del R1 y podemos observar que solo se muestran las redes conectadas directamente al router.

- En OSPF la métrica se llama cost el cual se utiliza para definir cuál interfaz es mejor para mandar un paquete y se puede observar en la tabla de enrutamiento. La métrica se calcula mediante la división de una velocidad de referencia definida por OSPF entre la velocidad de la interfaz, en el área 1 se definió 100 Mbps la velocidad de referencia entre 100 Mbps que es la velocidad de cada interfaz nos da un cost 1. Cuando se va a enviar un paquete de una red a otra se suma el cost de cada interfaz hasta llegar a la red de destino, por eso cada red tiene un cost diferente eso se aprecia en la tabla de enrutamiento, lo ideal es que el cost de cada interfaz sea 1. En la imagen 4 podemos observar en la tabla de enrutamiento que el cost de la ruta por defecto es 2 vía a la interfaz Gig. 0/1 del R1 ya que suma las dos interfaces del router hasta llegar al R2 para enviar paquetes a otras redes.



```
R1>en
Password:
Password:
R1#sh ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 192.168.1.30 to network 0.0.0.0

     192.168.1.0/24 is variably subnetted, 4 subnets, 2 masks
C       192.168.1.0/28 is directly connected, GigabitEthernet0/0
L       192.168.1.1/32 is directly connected, GigabitEthernet0/0
C       192.168.1.16/28 is directly connected, GigabitEthernet0/1
L       192.168.1.17/32 is directly connected, GigabitEthernet0/1
O*IA 0.0.0.0/0 [110/2] via 192.168.1.30, 4294967293:4294967283:4294967294,
GigabitEthernet0/1

R1#
```

Figura 18:
Fuente: José Escalona

· Se aplicó una codificación de mensajes MD5 mediante el protocolo OSPF a la interfaz Gig0/1 del R1 y Gig0/0 del router R2, para evitar la vulnerabilidad de los paquetes, es decir, si un intruso quiere analizar los paquetes. A la interfaz Gig 0/0 no se le aplico ninguna configuración de codificación.

· Elección de DR Y BDR, en cada red se define un DR y BDR el cual es el encargado de distribuir los mensajes que contienen las direcciones IP y recibe constantemente mensajes de los otros routers del área esto se hace para no saturar la red, cada interfaz es una red. Para asignar un DR y BDR se toman los siguientes criterios:

- Router-id.
- Prioridad de la interfaz.
- Dirección IP más alta.

Tabla 10: de DR Y BDR Área 1

		Área 1					
Router	Interfaz	Router-id	Prioridad de interfaz	R	DR	Drother	RED
1	ig. 0/0	1.0.0.1	1	SI	NO	NO	192.168.1.0/28
	ig.0/1	1.0.0.1	255	SI	NO	NO	192.168.1.16/28
2	ig. 0/0	2.0.1.0	254	NO	SI	NO	192.168.1.16/28

Fuente:

Especificaciones OSPF del área 0:

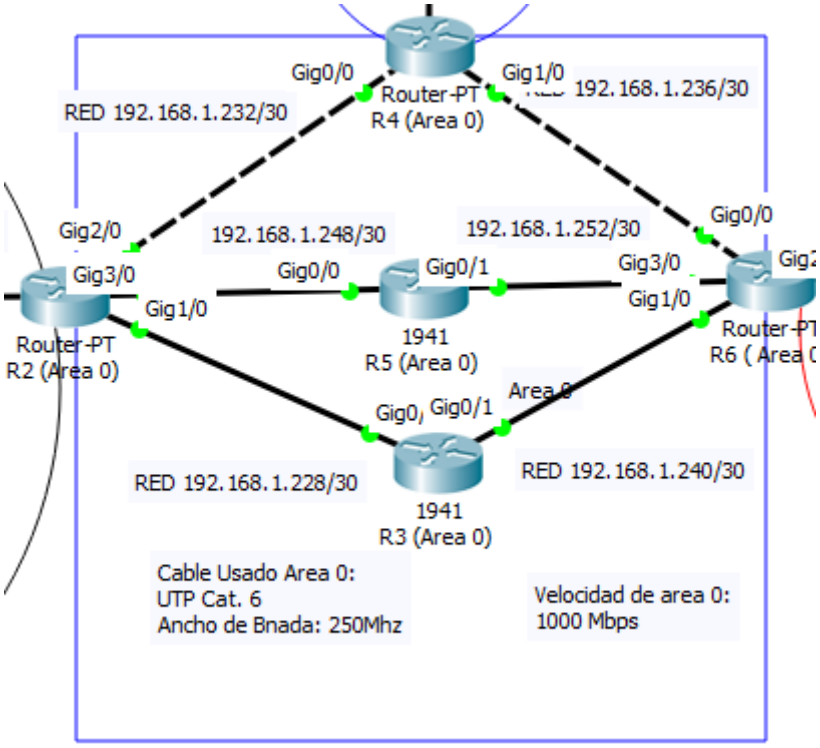


Figura 19:
Fuente: José Escalona

- Cada interfaz del área 0 tiene un ancho de banda de 1000Mbps y son full dúplex.
- Los routers involucrados en esta área son el router 2, 3, 4, 5 y 6 donde el router 3 y 5 son routers internos del área mientras el router 2, 4 y 6 son ABR debido que comunican 3 áreas las cuales son área 1, 2 y 99 respectivamente con el área 0.

- En esta area no se confguro ninguna interfaz pasiva.
- Esta area se configuro como area estandar que es el area por defecto de OSPF. En la imagen 5 podemos observar la tabla de enrutamiento del router 5 en donde se muestran todas las direcciones IP del area 1, 2 , 99 y de la misma area 0, a difrencia de las areas 1 y 2 que son areas totally-stub explicado anteriormente.

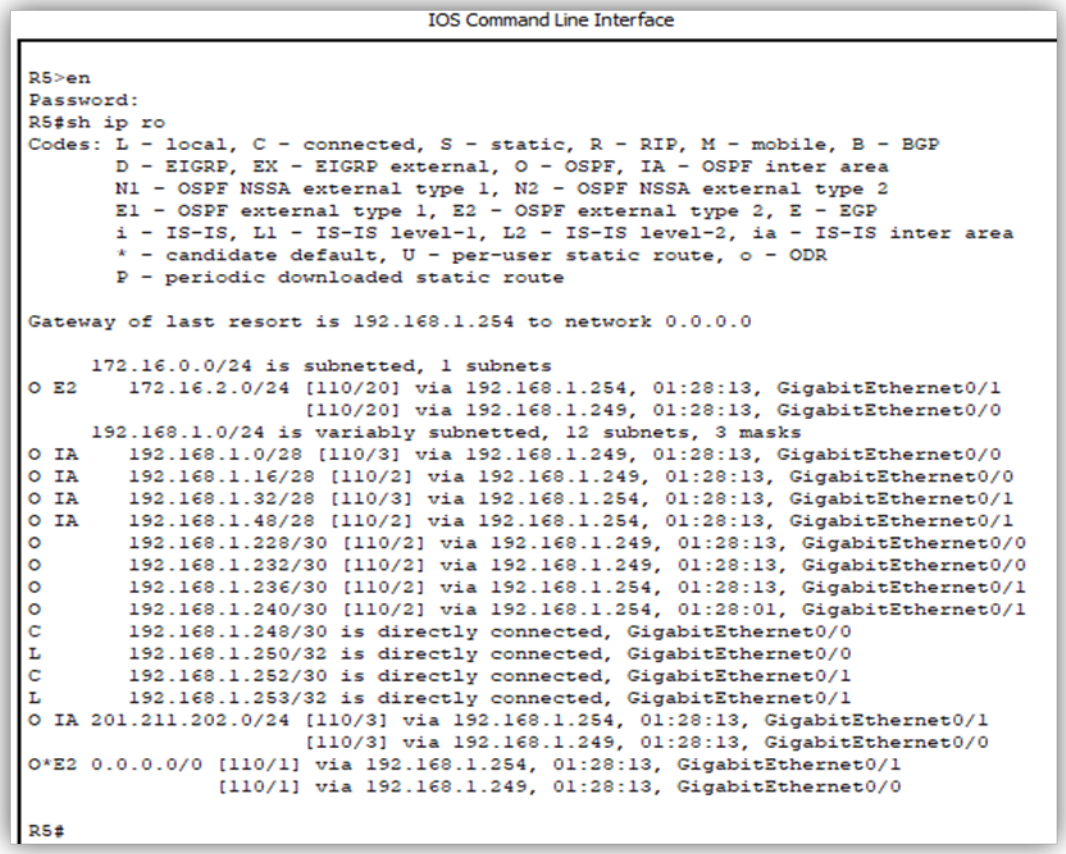


Figura 20:
Fuente: José Escalona

- Se definió 1000 Mbps la velocidad de referencia entre 1000 Mbps que es la velocidad de cada interfaz nos da un cost 1. En la imagen 5 podemos observar el cost de las diferentes rutas de la red que es la suma del cost de cada interfaz de esa ruta.

- Se aplicó una codificación de mensajes MD5 mediante el protocolo OSPF en todas las interfaces del área 0.
- Elección de DR Y BDR, en la siguiente tabla se muestra el DR y BDR de cada red del área 0.

Tabla 11: de eleccion DR y BDR area 0

Área 0							
Router	Interfaz	Router-id	Prioridad de interfaz	DR	BDR	Drother	RED
2	Gig. 1/0	2.0.1.0	0	NO	NO	I	192.168.1.228/30
	Gig. 2/0	2.0.1.0	0	NO	NO	SI	192.168.1.232/30
	Gig.3/0	2.0.1.0	0	NO	NO	SI	192.168.1.248/30
3	Gig. 0/0	3.0.0.0	1	SI	NO	NO	192.168.1.228/30
	Gig. 0/1	3.0.0.0	1	SI	NO	NO	192.168.1.240/30
4	Gig. 0/0	4.0.0.99	1	SI	NO	NO	192.168.1.232/30
	Gig. 1/0	4.0.0.99	1	SI	NO	NO	192.168.1.236/30
5	Gig. 0/0	5.0.0.0	1	SI	NO	NO	192.168.1.248/30
	Gig. 0/1	5.0.0.0	255	SI	NO	NO	192.168.1.252/30
6	Gig.0/0	6.0.0.2	0	NO	NO	SI	192.168.1.236/30
	Gig. 1/0	6.0.0.2	0	NO	NO	SI	192.168.1.240/30
	Gig. 3/0	6.0.0.2	1	NO	SI	NO	192.168.1.252/30

Especificaciones OSPF del área 2:

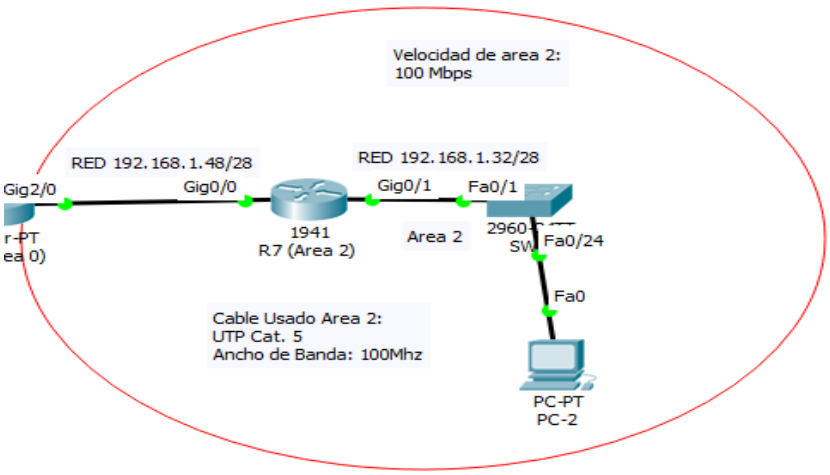


Figura 21:
Fuente: José Escalona

- Cada interfaz del área 2 tiene un ancho de banda de 100Mbps y son full dúplex.
- Los routers involucrados en esta área son el router 6 y 7 donde el router 7 es un router interno del área mientras el router 6 es un ABR debido que comunica el área 2 con el área 0.
- La interfaz Gig. 0/1 del router R1 se configuro como interfaz pasiva, es decir, no se enviaran mensajes OSPF a través de ella.
- Esta area se configuro como area totally-stub, al igual que el area 1 expliacado anteriotmrnte. En la imagen 6 podemos observar la tabla de enrutamiento del router 7.

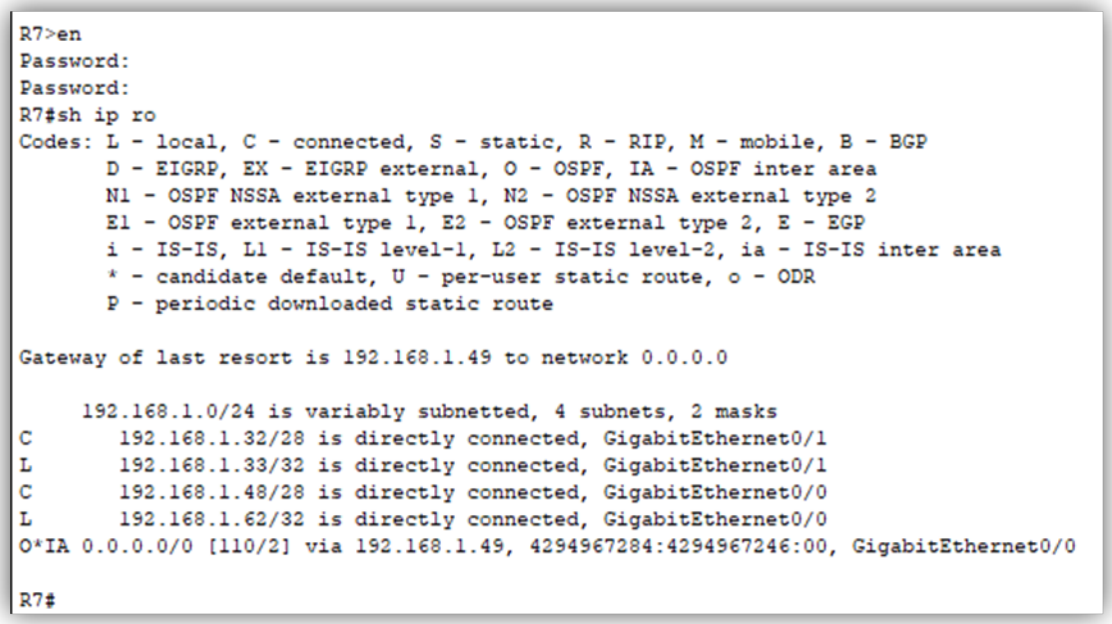


Figura 22:
Fuente: José Escalona

- Se definió 100 Mbps la velocidad de referencia entre 100 Mbps que es la velocidad de cada interfaz nos da un cost 1. En la imagen 6 podemos observar la ruta por defecto creada por el router 6 para dirigir los paquetes fuera del

área 2 debido que es un área totally-stub y ahí apreciamos el cost de la ruta que es la suma de la int. Gig. 0/0 y Gig. 0/1 del router 7.

- Se aplicó una codificación de mensajes MD5 mediante el protocolo OSPF a la interfaz Gig2/0 del R6 y Gig0/0 del router R7, para evitar la vulnerabilidad de los paquetes, es decir, si un intruso quiere analizar los paquetes. A la interfaz Gig 0/1 no se le aplico ninguna configuración de codificación.
- Elección de DR Y BDR, en la siguiente tabla se muestra el DR y BDR de cada red del área 2.

Tabla 12. de eleccion DR y BDR Area 2

Area 2							
Router	Interfaz	Router-id	Prioridad de interfaz	DR	BDR	Drother	RED
R6	Gig. 2/0	6.0.0.2	254	NO	SI	NO	192.168.1.48/28
R7	Gig. 0/0	7.0.0.2	255	SI	NO	NO	192.168.1.48/28
	Gig. 0/1	7.0.0.2	0	SI	NO	NO	192.168.1.32/28

Especificaciones OSPF del Área 99:

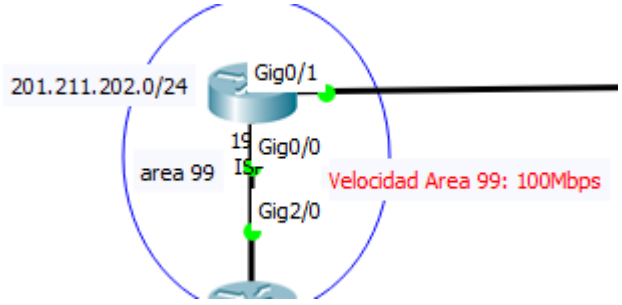


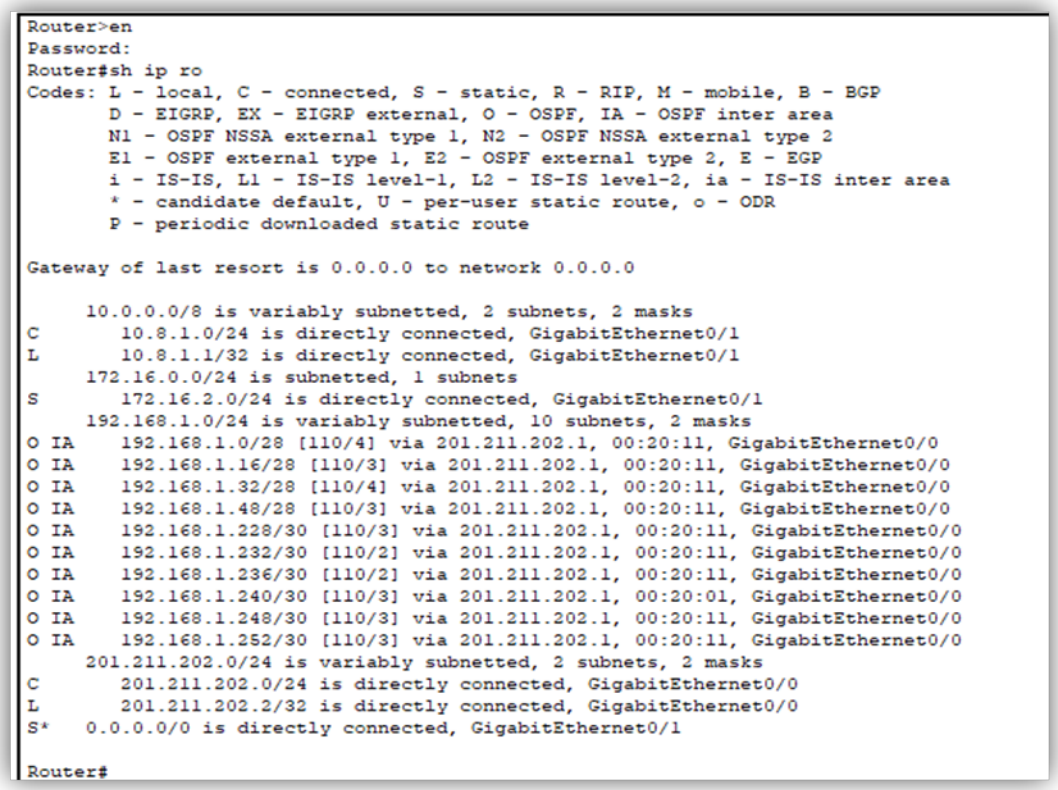
Figura 23:
Fuente: José Escalona

- Cada interfaz del área 99 tiene un ancho de banda de 100Mbps y son full dúplex.
- Los routers involucrados en esta área son el router 4 y ISP donde el router ISP es un router ASBR debido que comunica dos sistemas autónomos los cuales

son el dominio OSPF y el dominio de internet mientras el router 4 es un ABR debido que comunica el área 99 con el área 0.

- En esta area no se confguro ninguna interfaz pasiva.
- Esta area se configuro como area estandar que es el area por defecto de OSPF.

En la imagen 6 podemos observar la tabla de enrutamiento del router ISP en donde se muestran todas las direcciones IP del area 1, 2 , 0 y de la misma area 99, a difrencia de las areas 1 y 2 que son areas totally-stub explicado anteriormente.



```
Router>en
Password:
Router#sh ip ro
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, E - EGP
       i - IS-IS, L1 - IS-IS level-1, L2 - IS-IS level-2, ia - IS-IS inter area
       * - candidate default, U - per-user static route, o - ODR
       P - periodic downloaded static route

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C       10.8.1.0/24 is directly connected, GigabitEthernet0/1
L       10.8.1.1/32 is directly connected, GigabitEthernet0/1
     172.16.0.0/24 is subnetted, 1 subnets
S       172.16.2.0/24 is directly connected, GigabitEthernet0/1
     192.168.1.0/24 is variably subnetted, 10 subnets, 2 masks
O IA    192.168.1.0/28 [110/4] via 201.211.202.1, 00:20:11, GigabitEthernet0/0
O IA    192.168.1.16/28 [110/3] via 201.211.202.1, 00:20:11, GigabitEthernet0/0
O IA    192.168.1.32/28 [110/4] via 201.211.202.1, 00:20:11, GigabitEthernet0/0
O IA    192.168.1.48/28 [110/3] via 201.211.202.1, 00:20:11, GigabitEthernet0/0
O IA    192.168.1.228/30 [110/3] via 201.211.202.1, 00:20:11, GigabitEthernet0/0
O IA    192.168.1.232/30 [110/2] via 201.211.202.1, 00:20:11, GigabitEthernet0/0
O IA    192.168.1.236/30 [110/2] via 201.211.202.1, 00:20:11, GigabitEthernet0/0
O IA    192.168.1.240/30 [110/3] via 201.211.202.1, 00:20:01, GigabitEthernet0/0
O IA    192.168.1.248/30 [110/3] via 201.211.202.1, 00:20:11, GigabitEthernet0/0
O IA    192.168.1.252/30 [110/3] via 201.211.202.1, 00:20:11, GigabitEthernet0/0
     201.211.202.0/24 is variably subnetted, 2 subnets, 2 masks
C       201.211.202.0/24 is directly connected, GigabitEthernet0/0
L       201.211.202.2/32 is directly connected, GigabitEthernet0/0
S*   0.0.0.0/0 is directly connected, GigabitEthernet0/1

Router#
```

Figura 24:

Fuente: José Escalona

- Se definió 1000 Mbps la velocidad de referencia entre 1000 Mbps que es la velocidad de cada interfaz nos da un cost 1. En la imagen 6 podemos observar el cost de las diferentes rutas de la red que es la suma del cost de cada interfaz de esa ruta.

- Se aplicó una codificación de mensajes MD5 mediante el protocolo OSPF en todas las interfaces del área 99, excepto en la int. Gig. 0/1 del router ISP la cual no pertenece al área 99 sino a otro sistema autónomo AS.
- En el router ISP se configuro una ruta por defecto 0.0.0.0/0 via a la int. Gig. 0/1 y redistrubuida en todo el dominio OSPF, la cual simboliza a internet ya que cualquier paquete que vaya dirigido a una red que no este en el dominio OSPF sera enviado por esa interfaz a internet.
- Tambien podemos ver que en la tabla de enrutamiento del ISP esta una ruta estatica 172.16.2.0/24 via la int. Gig. 0/1, la cual es redistrubuida por todo el dominio OSPF pero no se mostrara en la tablas de enrutamiento del R1 y R7 debido que las areas 1 y 2 son totally-stub. Se configuro esta ruta estatica para simbolizar otro sistema autonomo y como redistrubuir la misma en el dominio OSPF.
- Elección de DR Y BDR, en la siguiente tabla se muestra el DR y BDR de cada red del área 99.

Tabla 13: de eleccion DR y BDR Area 99.

Area 99							
Router	Interfaz	Router-id	Prioridad de interfaz	DR	BDR	Drother	RED
R4	Gig. 2/0	4.0.0.99	255	SI	NO	NO	201.211.202.0/24
ISP	Gig. 0/0	8.0.0.0	0	NO	NO	SI	201.211.202.0/24

Especificaciones Cluster (Nube que simula internet):

- Cada interfaz del cluster tiene un ancho de banda de 100Mbps y son full dúplex.
- El cluster se realizó con la finalidad de simular a internet, podemos observar en la imagen 2 que está conformado por una conexión a internet a través de la tecnología de DSL aun router el cual posee dos interfaces a las cuales están conectadas una aun servidor HTTP simulando la página de Google con una IP

10.8.2.2 y en la otra un servidor DNS el cual traduce dicha dirección IP en un nombre de dominio es cual es www.google.com.ve.

· Dicho router siguiendo la numeración es el R9, en el cual se configuro una ruta por defecto para dar respuesta a las peticiones HTTP Y DNS realizadas en la red mostrada en la imagen 3.

· El cluster que simula internet se denomina un sistema autónomo ya que trata de un conjunto de redes IP y routers que se encuentran bajo el control de una misma entidad y que poseen una política de enrutamiento diferente. En nuestro casa nuestra red maneja una política de enrutamiento dinámico OSPF y el cluster que es internet otra.

4.2.3. Configuración de una política de calidad de servicio

4.2.3.1. Creación de listas de acceso

Las listas de acceso se crearon con la finalidad de definir el tráfico VOIP y Video Streaming. En el tráfico VOIP se definió un rango de puertos UDP que va del 16384 al 32767 y para TCP el puerto 1720, mientras que en el trafico Video Streaming se definió el puerto UDP 554, a continuación se muestran los comando empleados los cuales se configuran en el modo configuración global del router en este casa trabajaremos en la configuración del R1 la cual es igual a la del R4 y R7 ya que en ellos se implementara la política de marcado de paquetes en la cual se usan las listas de acceso. (Ver anexo L)

4.2.3.2. Creación de clases

Se crearon 5 clases las cuales englobaran todo el tráfico en la red y cada una de ellas será marcada con un código DSCP diferente por medio del cual será tratada de manera diferente a lo largo de toda la red. Las cuales la podemos observar con detalle en la siguiente tabla:

Tabla 14. Tipos de clases

Nombre de Clase	Protocolos Definidos	Lista de acceso Definidas
Clase VOIP	NINGUNO	Lista de acceso 101
Clase Video Streaming	NINGUNO	Lista de acceso 102
Clase Trafico Importante	HTTP, Telnet y SSH	NINGUNO
Clase Trafico Medio	FTP, TFTP, IMAP, POP3 y SMTP	NINGUNO
Clase default	El resto de trafico	NINGUNO

(ver anexo M)

4.2.4. Política de Marcado de paquetes

Esta política consiste en marcar las clases mediante una codificación DSCP la cual está estructurada en un conjunto de clases de alta, media y baja prioridad como también una clase de máximo esfuerzo denominada ef para paquetes sensibles a latencia y congestión. Esto lo podemos observar en las tablas 2 y 3 del marco teórico. Esta política de marcado solo se aplicara para el tráfico de entrada en 3 interfaces de la red las cuales son int. Gig. 0/0 del R1 área 1, int. Gig. 0/1 del R7 área 2 y int. Gig. 2/0 del R4área 99, debido que por medio de ellas entra todo el tráfico al núcleo de la red. En la siguiente tabla podemos observar el marcado de cada clase dependiendo del tráfico definidas en ellas y su prioridad. (Ver anexo N)

Tabla 15. Marcado de paquetes.

Clases	Marcado	Prioridad
Clase VOIP	EF	MUY ALTA
Clase Video Streaming	EF	MUY ALTA
Clase Trafico Importante	AF13	ALTA
Clase Trafico Medio	AF22	MEDIA
Clase default	0	NINGUNA

4.2.5. Política QoS para tráfico saliente de todas las interfaces.

Ahora procedemos a configurar la política que vamos aplicar en todo el tráfico saliente de cada interfaz de la red, esto es lo que denomina calidad de servicio, que sería como van hacer ser tratados todas los paquetes de las diferentes clases definidas

anteriormente a lo largo de toda la red hasta su destino. En la siguiente tabla vamos a ver los criterios que se le asignaron a cada clase.

Primero se procede a crear las clases en las cuales se definirá los 5 tipos de codificación DSCP marcados en las interfaces de tráfico entrante definidas anteriormente, esto con el fin del paquete que venga marcado con una de esas codificaciones será tratado con los diferentes criterios que hemos definido para cada clase a lo largo de toda la red.

Los criterios fueron tomados por medio de los valores necesarios para que se pueda cumplir con el objetivo de garantizar un buen servicio, en el caso de VOIP su ancho de banda de operación está entre 30 Kbps a 128 Kbps y se definió en 400 Kbps con una prioridad de baja latencia LLQ que no es más que una cola con privilegios y apartada de las colas de las demás clases, en el caso del video Streaming su ancho de banda de operación es 384 Kbps a 20 Mbps y se definió en 25 Mbps con una prioridad de latencia baja LLQ. En el caso de la clase de tráfico importante se definió un ancho de banda de 10Mbps con una política shape de 16Mbps la cual se activa cuando nos excedemos del ancho de banda hasta un límite de 16Mbps, retrasando paquetes que excedan el límite establecido y por último se configuro una prevención de congestión propia de cisco llamada WRED basado en la codificación DSCP, en la clase de trafico medio se aplicó lo mismo pero se definió un ancho de banda 15 Mbps con una política shape de 20 Mbps y la clase default se estableció un sistema de cola llamada WFQ con 16 colas con un máximo de 25 paquetes por cola. En la imagen 7 podemos apreciar cómo funciona la política shape. (Ver anexo O)

Tabla 16. Criterios de tráfico saliente.

Clases	Ancho de Banda	Ancho de Banda con LLQ	Política de tráfico shape	Prevención de congestión	Cola normal (WFQ)
Clase VOIP		400Kbps			
Clase Video Streaming		25Mbps			
Clase Trafico Importante	10Mbps		16Mbps	WRED basado en DSCP.	
Clase Trafico Medio	15Mbps		20Mbps	WRED basado en DSCP.	
Clase default					Números de colas 16. Máximo de paquetes por cola 25.

Cuando asignamos un valor DSCP a la clase creada no es más que al momento de salir el paquete como trafico saliente de cada interfaz y debido a que este ya viene previamente marcado por la política de marcado que definimos como trafico entrante en algunas interfaces anteriormente va a coincidir el código DSCP con una de las clases creadas en la política QoS y dependiendo la clase que sea será tratado con diferentes criterios en el trafico saliente de cada interfaz en toda la red.

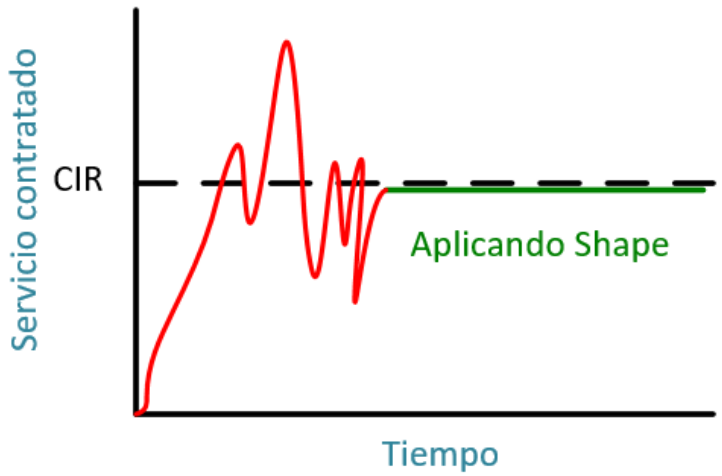


Figura 25:
Fuente: José Escalona

4.2.6. Política QoS para Tráfico de subida y bajada de nuestro ISP.

En el router ISP se aplicaron unas políticas de trafico de subida y de bajada en base a las velocidades de subida y bajada que nos ofrece nuestro ISP que la podemos observar en la tabla de servicio ofrecido por ISP. Las políticas aplicadas se definen para establecer un ancho de banda para la transferencia de información de un servidor FTP Y HTTP.

Tabla 17. Servicio ofrecido por ISP.

Velocidad ofrecida por el ISP	50 Mbps
Velocidad de subida	12,5 Mbps
Velocidad mínima de bajada	30 Mbps
Velocidad máxima de bajada	37, 5 Mbps

Primero se crea una política de trafico de subida dentro de la cual utilizaremos la clase default para definir criterios a implementar los cuales son el establecimiento de un ancho de banda 12,5 Mbps que es la velocidad máxima de subida ofrecida por nuestro ISP, luego se crea una clase llamada tráfico de bajada donde se definen los protocolos FTP y HTTP, creamos una política de bajada para definir los criterios dentro de la clase tráfico de bajada los cuales son un ancho de banda de 10 Mbps con una política shape de 15 Mbps, dentro de la misma política en la clase default definimos un ancho de banda 15 Mbps y una política shape 22, 5 Mbps, los criterios tomados en la política de trafico de bajada se basaron en las velocidades de bajada mínima y máxima ofrecidas por nuestro ISP. En la siguiente Tabla podemos observar los criterios aplicados.

Tabla 18. Política de subida y bajada ISP.

Política	Clase	Política Shape	Ancho de Banda
Trafico de subida	Default		12,5 Mbps
Trafico de bajada	Trafico de bajada	15 Mbps	10 Mbps
	Default	22,5 Mbps	15 Mbps

(Ver anexo P)

4.2.7. Aplicar políticas en las interfaces correspondientes.

Por ultimo falta aplicar las políticas de marcado y QoS a los routers en las interfaces correspondientes, ya sea para marcar el tráfico entrante en las interfaces que corresponda como los criterios de ancho de banda, prioridad LLQ, política shape y WFQ en tráfico saliente de la demás interfaces. Lo podemos observar con más detalle en la tabla de política de marcado y QoS. (Ver anexo Q)

Tabla 19. Política de marcado y QoS

Router	Interfaces	Política de Marcado de Paquetes		Política QoS	
		Entrada	Salida	Entrada	Salida
R1	Gig. 0/0	Aplicada	No aplicada	No aplicada	Aplicada
	Gig. 0/0	No aplicada	No aplicada	No aplicada	Aplicada
R2	Gig. 0/0	No aplicada	No aplicada	No aplicada	Aplicada
	Gig. 1/0	No aplicada	No aplicada	No aplicada	Aplicada
	Gig. 2/0	No aplicada	No aplicada	No aplicada	Aplicada
	Gig. 3/0	No aplicada	No aplicada	No aplicada	Aplicada
R3	Gig. 0/0	No aplicada	No aplicada	No aplicada	Aplicada
	Gig. 0/1	No aplicada	No aplicada	No aplicada	Aplicada
R4	Gig. 0/0	No aplicada	No aplicada	No aplicada	Aplicada
	Gig. 1/0	No aplicada	No aplicada	No aplicada	Aplicada
	Gig. 2/0	Aplicada	No aplicada	No aplicada	Aplicada
R5	Gig. 0/0	No aplicada	No aplicada	No aplicada	Aplicada
	Gig. 0/1	No aplicada	No aplicada	No aplicada	Aplicada
R6	Gig. 0/0	No aplicada	No aplicada	No aplicada	Aplicada
	Gig. 1/0	No aplicada	No aplicada	No aplicada	Aplicada
	Gig. 2/0	No aplicada	No aplicada	No aplicada	Aplicada
	Gig. 3/0	No aplicada	No aplicada	No aplicada	Aplicada
R7	Gig. 0/0	No aplicada	No aplicada	No aplicada	Aplicada
	Gig. 0/1	Aplicada	No aplicada	No aplicada	Aplicada
ISP	Gig. 0/0	No aplicada	No aplicada	No aplicada	Aplicada
	Gig. 0/1	No aplicada	No aplicada	No aplicada	Aplicada

4.3. Fase III: Aplicación del simulador GNS3 a las redes basadas en MPLS con calidad de servicio

Con lo explicado anteriormente culminamos la etapa de calidad de servicio, pero es importante destacar que los comandos empleados para la marcación en el R1 área 1 son los mismos empleados en los routers R7 área 2 y R4 área 99, de la misma formar los comandos utilizados para configurar la política QoS en todos los routers

de la red y de igual manera para aplicar las políticas en las interfaces correspondientes.

4.3.1.Configuración de MPLS en el núcleo de la red (área 0).

Debido que el simulador packet tracert no soporta el protocolo MPLS no lo pudimos implementar por lo que más adelante en la red simulada en GNS3 veremos su configuración.

4.3.2. Configuraciones inicialices de un router y switch.

Procederemos a hacer las configuraciones iniciales de un router y switch las cuales son contraseñas de niveles de seguridad, mensaje de seguridad, tiempo de sesión de niveles de seguridad y Evitar la búsqueda DNS en líneas de comando. (ver anexo R).

La configuración mostrada en el router 1 será la misma para los demás routers y switches de toda la res al igual que las contraseñas definidas en los comandos

4.3.3. Red simulada en GNS3

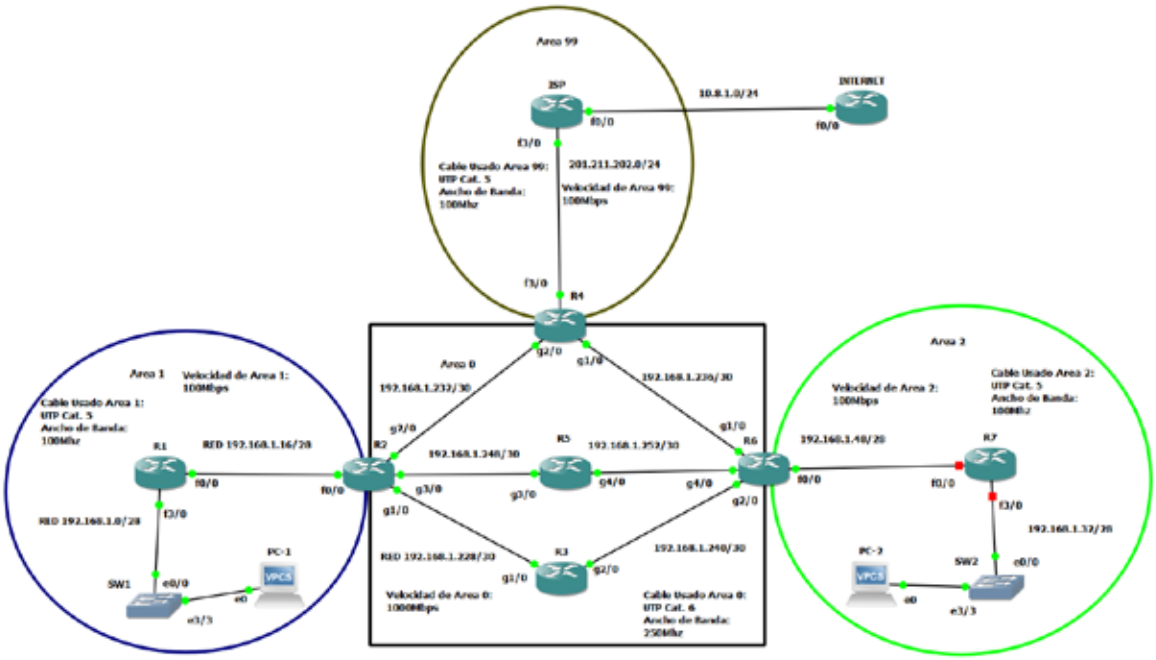


Figura 26:
Fuente: José Escalona

Después de lo explicado anteriormente procederemos a la explicación al detalle de la red simulada en GNS3 como lo realizamos con la red simulada en packet tracert. La red simulada en GNS3 posee la misma configuración de la etapa 1 direccionamiento IP, de la etapa 2 configuración OSPF como protocolo de enrutamiento con la diferencia que no se puedo aplicar un cluster debido a limitaciones del simulador pero se realizó de otra formar, la etapa 3 configuración de una política de calidad de servicio se configuro de igual formar que packet tracert con un ligero cambio en la configuración de política de trafico de subida aplicada al router ISP, la etapa 4 configuración de MPLS en el núcleo de la red (área 0) no se pudo realizar en el simulador packet tracert por no soportar el protocolo MPLS mientras que en GNS3 se configuro perfectamente que será explicado con detalle más adelante y la última etapa configuraciones inicialices de un router y switch se realizó de la misma forma que en el simulador packet tracert sin ningún cambio.

Configuración de OSPF como protocolo de enrutamiento

4.3.3.1. Especificaciones Router R9 (Simula internet):

Explicado lo anterior solo especificaremos el ligero cambio que mencionamos sobre el cluster que no se pudo realizar por limitaciones del simulador GNS3, el cual se sustituyó con un router que simulara internet, la única configuración que se realizó en el router fue definir una ruta por defecto 0.0.0.0/0 para dar respuesta a los diferentes tipos de trafico dirigidos a la dirección IP de la misma interfaz donde se configuro la ruta por defecto la cual es int. f0/0 ya que fue la única interfaz configurada en el router. En la imagen lo podemos observar.

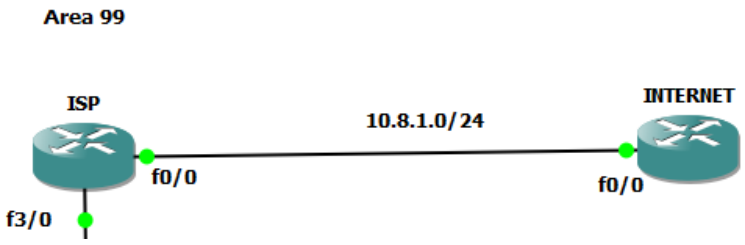


Figura 27:
Fuente: José Escalona

4.3.3.2. Configuración de una política de calidad de servicio

Las políticas de marcado y QoS no tuvieron ningún cambio en esta simulación, solo se realizó una modificación en la configuración y aplicación de la política de trafico de subida configurada en el router ISP. Se aplicó una política police la cual se diferencia de la política shape que en vez de retrasar los paquetes cuando superan el límite establecido los descarta, también definimos que cada 100 ms se enviara 156250 bytes (1250000 bits) el cual se denomina bc y por ultimo definimos que la cantidad por exceso a enviar es de 312500 bytes (2500000 bits) se denomina be, es decir, que durante 100 ms se va a transmitir una ráfaga de 1250000 bits (paquete o paquetes de ese tamaño) hasta un máximo de 2500000 bits (paquete o paquetes de ese tamaño), cuando se excede del máximo establecido se descartan los paquetes pero si se mantiene en el margen establecido se transmitirán, es importante resaltar que el comando police no se pudo configurar en la red simulada en packet tracert ya que este no lo soporta y por eso lo aplicamos en el simulador GNS3. A continuación veremos los comandos y formulas empleadas y en la imagen 9 la configuración aplicada al router ISP y al imagen 10 como actúa el comando police.

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

Despejamos y calculamos bc

$$bc = tc * CIR = 100x10^{-3} ms * 12{,}5 Mbps = 1250000\ bits$$

Lo transformamos a bytes dividiendo entre 8 el resultado ya que 1 byte son 8 bits

$$\frac{1250000}{8} = 156250\ bytes$$

Ahora calculamos be

$$be = 2 * bc = 2 * 156250 = 312500\ bytes$$

Leyenda:

CIR= Tasa de transferencia garantizada (mayormente los que nos ofrece nuestro ISP).

tc= Tiempo que durara una ráfaga en ser transmitida.

bc= Tamaño de ráfaga normal.

be= Tamaño de ráfaga de exceso. (Ver anexo S)

```
ISP#show policy-map
  Policy Map DOWN_TRAFICO
    Class TRAFICO-BAJADA
      bandwidth 10000 (kbps)
      Average Rate Traffic Shaping
      cir 15000000 (bps)
    Class class-default
      bandwidth 15000 (kbps)
      Average Rate Traffic Shaping
      cir 22500000 (bps)

  Policy Map UP_TRAFICO
    Class class-default
     police cir 12500000 bc 156250 be 312500
       conform-action transmit
       exceed-action drop
       violate-action drop

ISP#
```

Figura 28:
Fuente: José Escalona

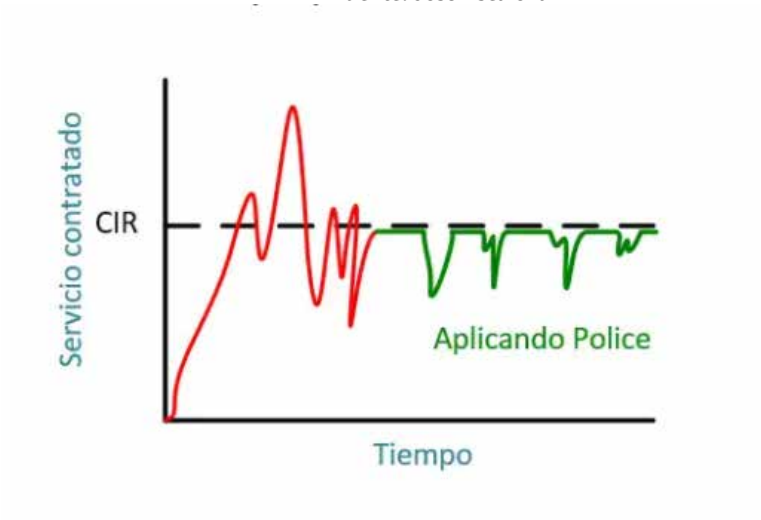


Figura 29:
Fuente: José Escalona

4.3.3.3. Configuración de MPLS en el núcleo de la red (área 0).

Se aplicó una configuración del protocolo MPLS en el área 0 para mejorar el rendimiento de la red, para trabajar con etiquetas en vez de direcciones IP de esta forma el envío de paquetes es más rápido y fiable, como el protocolo MPLS trabaja en base al protocolo de enrutamiento OSPF se configuro de siguiente manera primero se activó él IP Cisco Envió Exprés (CEF por su siglas en ingles) que es una tecnología avanzada de conmutación de capa 3 que se utiliza principalmente en redes centrales para mejorar el rendimiento general de la red, luego se definieron interfaces loopback en cada router dentro del área 0 para ser usados como router-id en el proceso MPLS después se definió el protocolo LDP y el router-id para el proceso MPLS en cada router y por último se activó MPLS en todas las interfaces de cada router por medio del protocolo OSPF. En la tabla de router-id MPLS podemos observar cómo será identificado cada router en el proceso MPLS y en la imagen 11 como se ven activadas las interfaces con MPLS del R5 que de igual forma estarán activadas para cualquier router. (Ver anexo T)

Tabla 20. Router-id MPLS

Router	Interfaz Loopback	Router-id	Área
R2	2.0.1.0/32	2.0.1.0	0
R3	3.0.0.0/32	3.0.0.0	0
R4	4.0.0.0/32	4.0.0.0	0
R5	5.0.0.0/32	5.0.0.0	0
R6	6.0.0.2/32	6.0.0.2	0

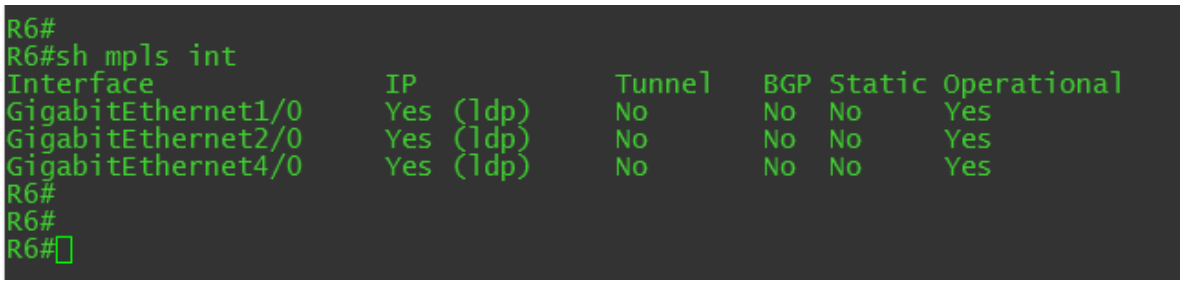


Figura 30
Fuente: José Escalona

Configuraciones inicialices de un router y switch.

Esta configuración se realizó de igual manera que en la red simulada en packet tracert.

4.4. Fase IV: Determinar los parámetros de desempeño y el rendimiento de una red MPLS con calidad de servicio

En función a la simulación aplicada, se puede observar que la red MPLS con QoS permite:

- Incorporar la velocidad de conmutación del nivel 2 al nivel 3. Sin embargo es una cualidad básica pues hay suficiente velocidad en los routers como para soportar varios tipos de interfaces
- Permite causar tráfico con diferentes calidades de clases de servicio
- Ofrece crear de manera sencilla VPN
- Permite además realizar TE o ingeniería de trafico lo cual a su vez permite mover parte del tráfico de datos a caminos menos susceptibles a sufrir fallos

4.4.1. Resultados y verificación

Por consiguiente se muestra y analiza los resultados del estudio y diseño de la red simulada en packet tracert y GNS3 con plataforma IP-MPLS y calidad de servicio. Los resultados que se muestran van desde la arquitectura de la red, hasta las configuraciones avanzadas y comportamiento de los equipos de red.

Seguidamente, Después de haber realizado todas las configuraciones previas podemos decir que aumentamos el rendimiento de una red, de pasar de una simple red con enrutamiento IP a una red con enrutamiento MPLS en el núcleo de la misma (área 0) basado en OSPF y las diferentes configuraciones que realizamos para lograr un óptimo funcionamiento y por último la configuración de una política de calidad de servicio para priorizar trafico sensible a latencias como mecanismos de prevenciones de congestiones.

Por último, procederemos a verificar la conectividad de un extremo al otro de la red por medio de dos pc, a ver el funcionamiento del núcleo de la red configurado con MPLS y como se marca el tráfico para ser tratado a lo largo de la misma por las diferentes políticas de calidad de servicio que aplicamos.

· Verificación y resultados de la configuración OSPF mediante la captura de paquetes con Wiresharek mediante el simulador GNS3.

Se Realizó una captura de paquetes en la int. f3/0 del R1 del área 1 con wiresharek. Ver figura 31

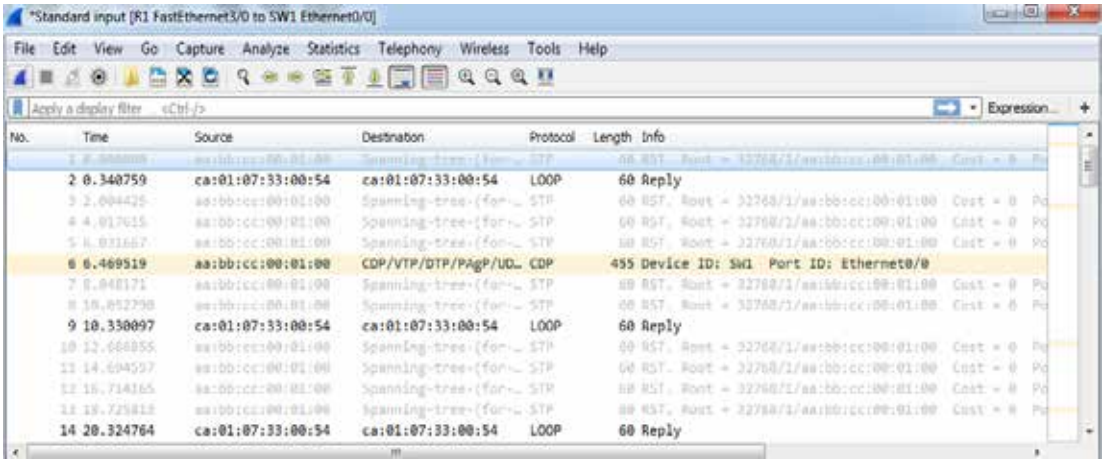


Figura 31
Fuente: José Escalona

En la imagen podemos observar que no hay mensajes hello de OSPF porque la interfaz f3/0 del R1 se configuro como interfaz pasiva al igual que la interfaz f3/0 del R7.

Ahora realizaremos un capture de pantalla de la int. g3/0 del R2. Ver figura 32

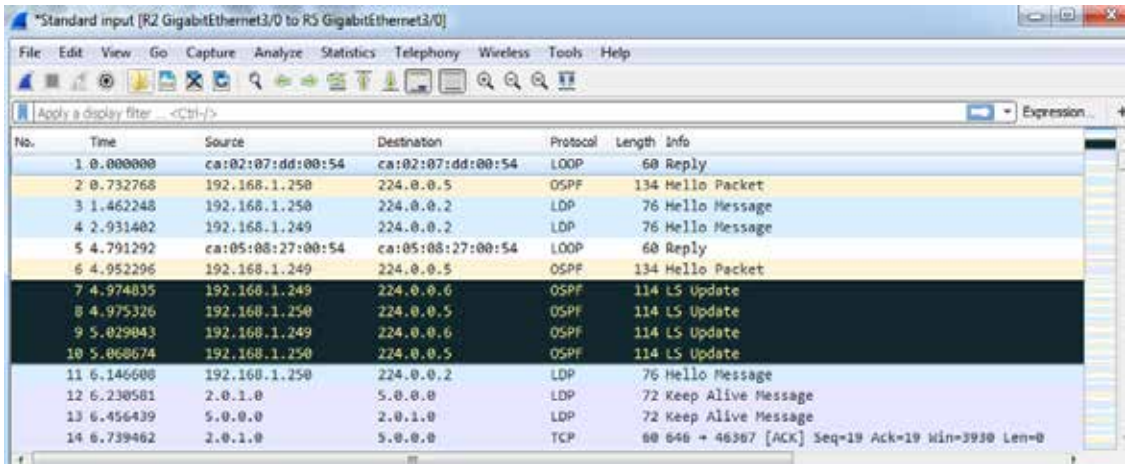


Figura 32:
Fuente: José Escalona

Podemos observar en esta imagen los mensajes hello OSPF que nos permiten la comunicación entre router vecinos y son LSA tipo 1. Este tipo de mensajes lo vamos a ver en todo el dominio OSPF excepto en las interfaces que se configuraron de manera pasiva. Con estas dos imágenes pudimos verificar el funcionamiento de OSPF.

· Verificar conectividad de la PC-1 a la PC-2

Procederemos a realizar un ping entre la PC-1 y la PC-2 en el simulador GNS3 para verificar la conectividad de la red y así comprobar que hemos realizado una configuración de enrutamiento prefecta. Ver figura 33

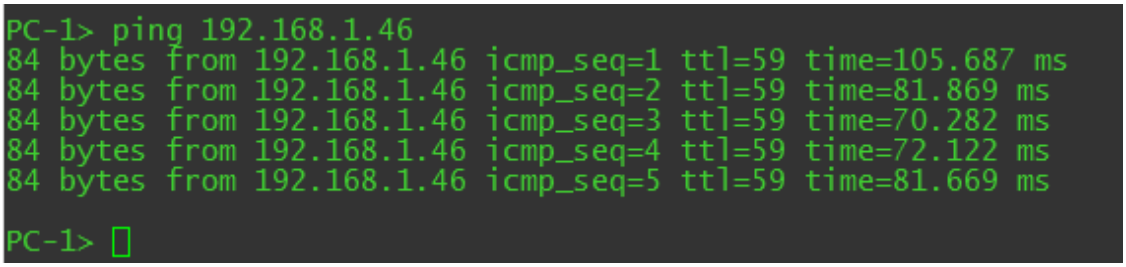


Figura 33:
Fuente: José Escalona

Como resultado del ping realizo entre PC-1 y PC-2 podemos observar que llegaron satisfactoriamente los 5 paquetes ICMP lo que nos comprueba la conectividad en la red.

· Verificar conectividad de la PC-2 a la PC-1

Ahora procederemos a realizar un ping entre la PC-2 y la PC-1 en el simulador GNS3 para verificar la conectividad en sentido contrario de la red. Ver figura 34

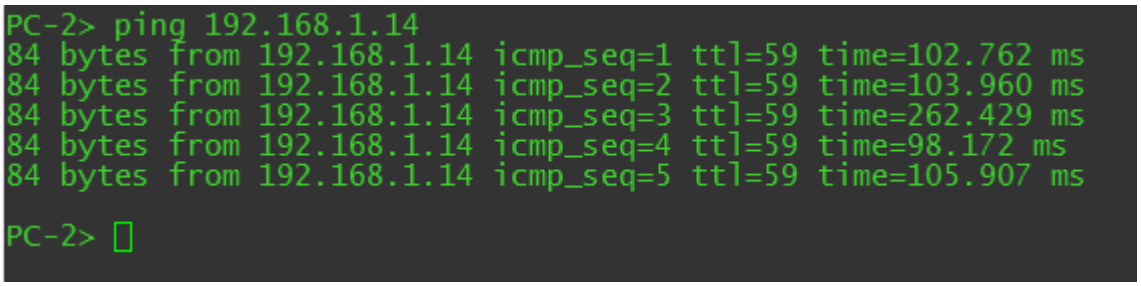


Figura 34:
Fuente: José Escalona

Como resultado del ping realizo entre PC-2 y PC-1 podemos observar que llegaron satisfactoriamente los 5 paquetes ICMP lo que nos comprueba la conectividad en sentido contrario de la red.

· Verificar conectividad entre PC-1 e ISP

Realizamos un entre PC-1 y nuestro router proveedor de internet en el simulador GNS3 para verificar nuestra conexión a internet. Ver figura 35

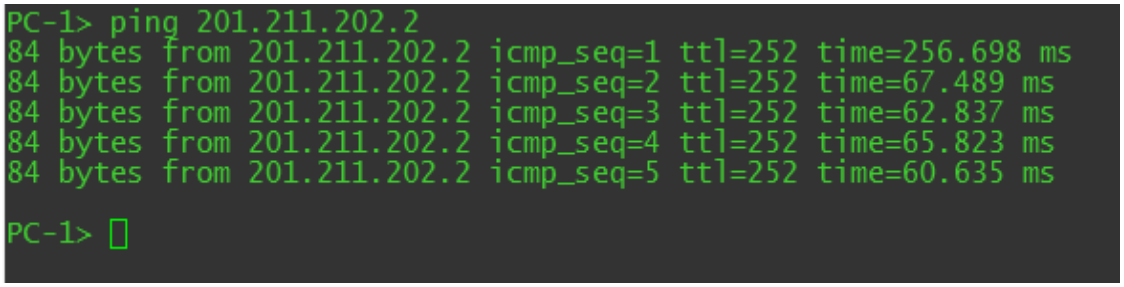


Figura 35:
Fuente: José Escalona

Como resultado observamos que hay conectividad entre PC-1 y router ISP lo que nos permite acceder a internet.

Verificar conexión a internet mediante la petición HTTP de la página de google configurada en packet tracert.

Entramos al explorador de la PC-1 en el simulador packet tracert y colocamos en el buscador www.google.com.ve y le damos a *go*, lo cual hace la petición HTTP ahora esperamos la respuesta.

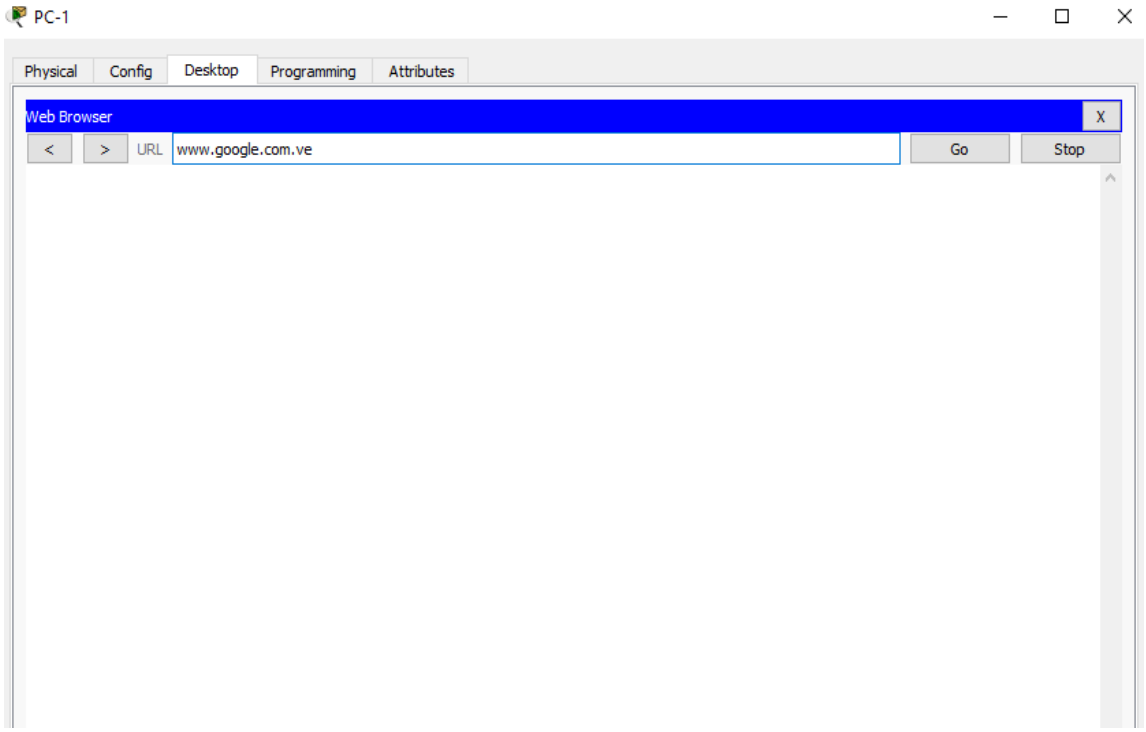


Figura 36:
Fuente: José Escalona

Luego de a ver realizado la petición HTTP el paquete se dirige al ABR del área 1 para buscar en su tabla de enrutamiento la dirección IP asociada a ese nombre de dominio como no la encontrara la mandara a la ruta por defecto establecida en el router ISP que simula internet y de ahí nos mandara un paquete con la respuesta HTTP la cual será el contenido de la página web. Ver Figura 37

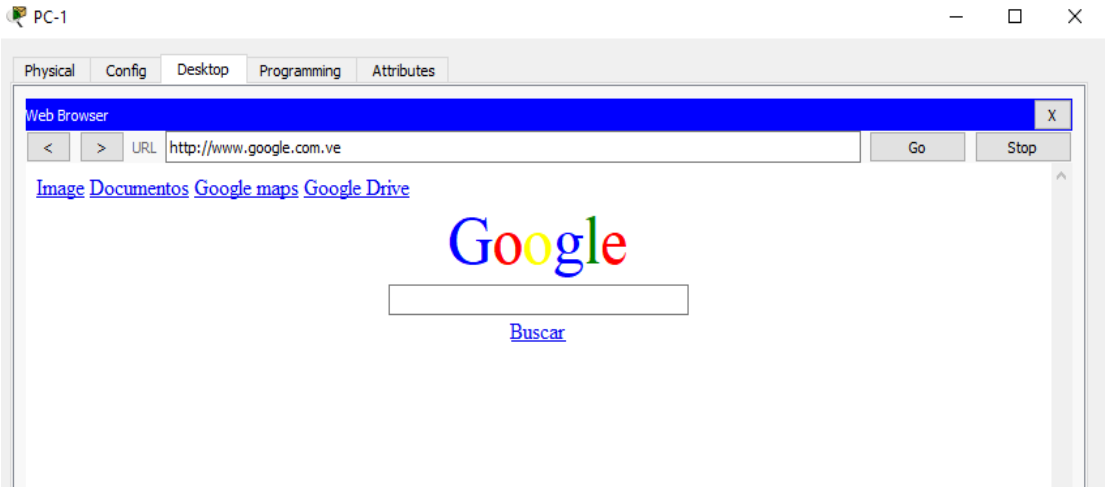


Figura 37:
Fuente: José Escalona

Proceso de marcado de paquetes debido a la política de marcado aplicada a las interfaces de tráfico entrante en los routers que dan ingreso de paquetes al núcleo de la red.

Realizaremos de nuevo una petición a la página de www.google.com.ve para ver cómo es marcado por el código DSCP de la clase que corresponde el trafico HTTP. Primero se realiza la petición ver figura 38.

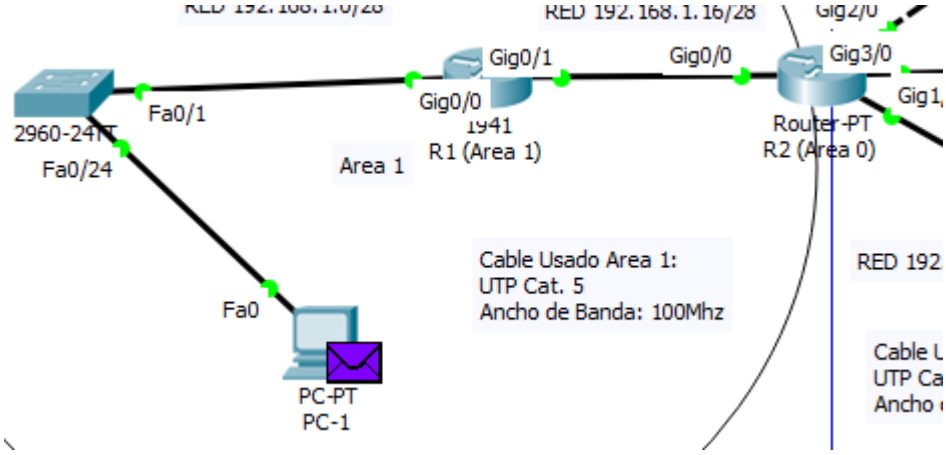


Figura 38:
Fuente: José Escalona

Luego se encuentra en la entrada de la interfaz Gig. 0/0 del R1 donde será marcada, en la imagen 20 podemos observar que antes de pasar por la entrada del int. Gig. 0/0 del R1 no está marcado el paquete y lo podemos observar en el encabezado del paquete.

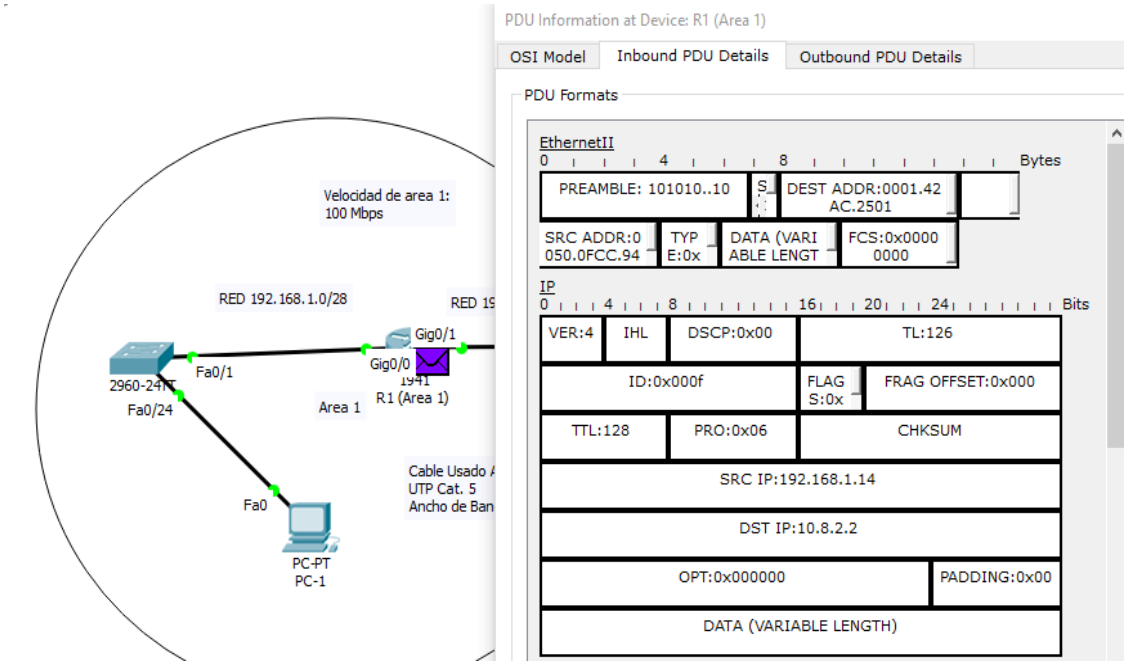


Figura 39:
Fuente: José Escalona

Ahora observamos que después de pasar por la int. Gig. 0/0 del R1 el paquete queda marcado con el código DSCP: 0x0e en hexadecimal que transformado en binario corresponde al código af13 que es la clase de tráfico importante donde se encuentra definido el protocolo HTTP. Ver figura 40

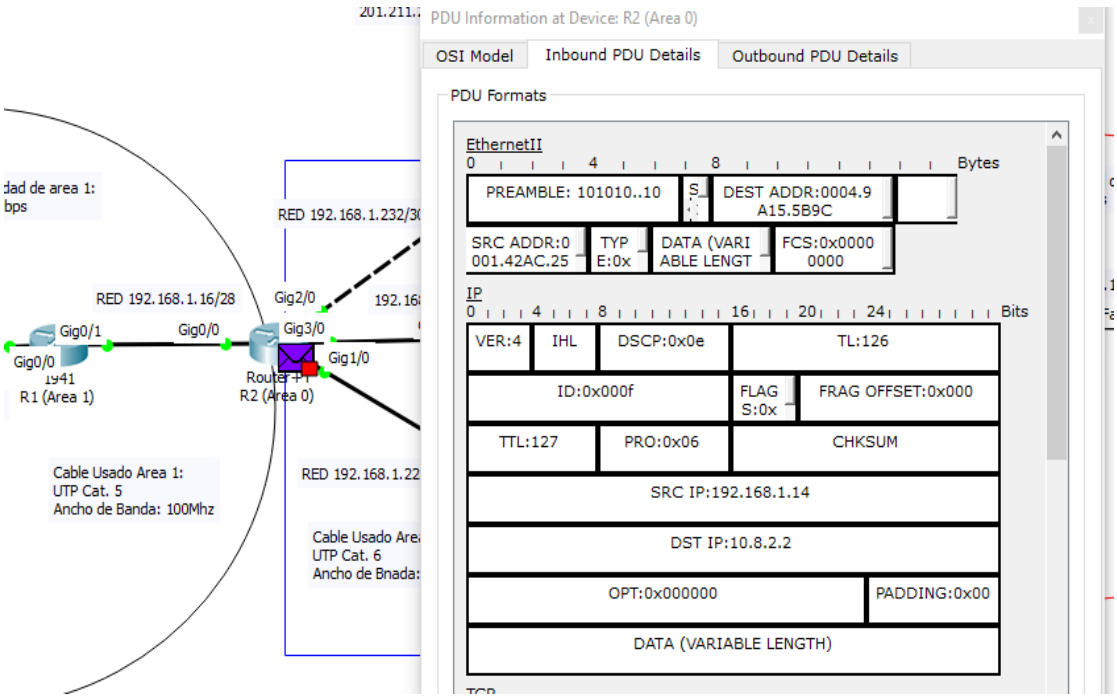


Figura 40:
Fuente: José Escalona

El paquete después de ser marcado va a hacer tratado de manera especial a lo largo de toda la red por la política QoS aplicada en todas las interfaces de tráfico saliente, podemos observar que el paquete verifico la tabla de enrutamiento del ABR del área 1 y no encontró coincidencia por lo que lo mando a la ruta por defecto del ISP. Ver figura 41

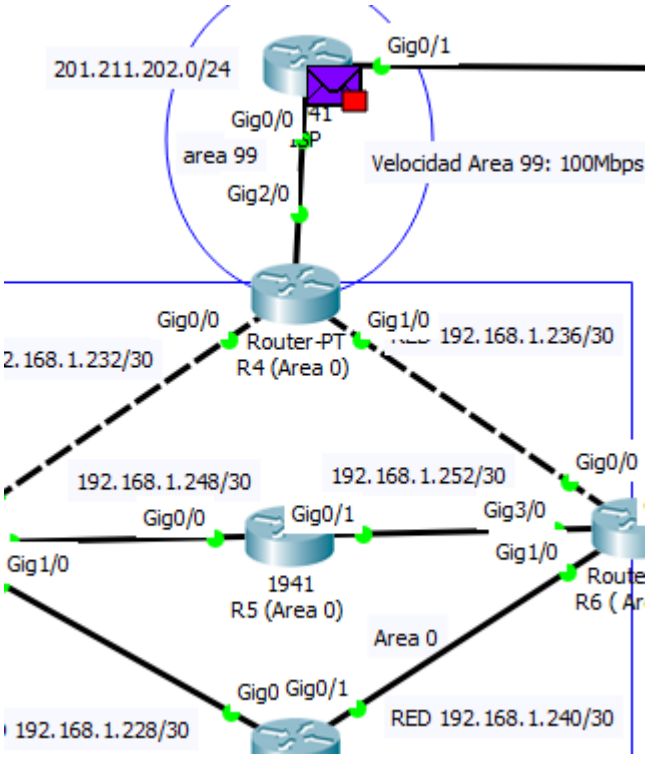


Figura 41:
Fuente: José Escalona

Por ultimo podemos observar que cuando el paquete viene de internet ya no está marcado pero cuando entra de nuevo al núcleo de la red área 0 por medio del R4 es marcado de nuevo y recibe de nuevo un tratamiento especial hasta llegar a su destino. Ver figuras 42 y 43.

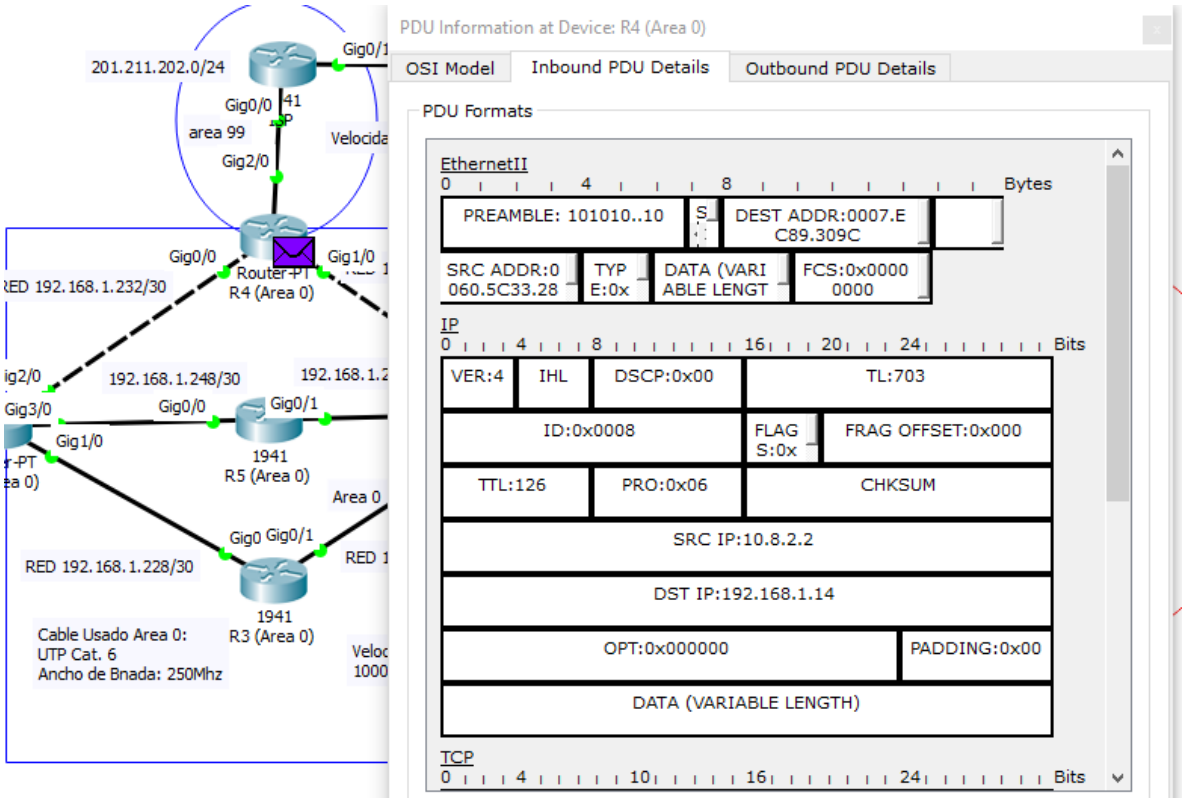


Figura 42:
Fuente: José Escalona

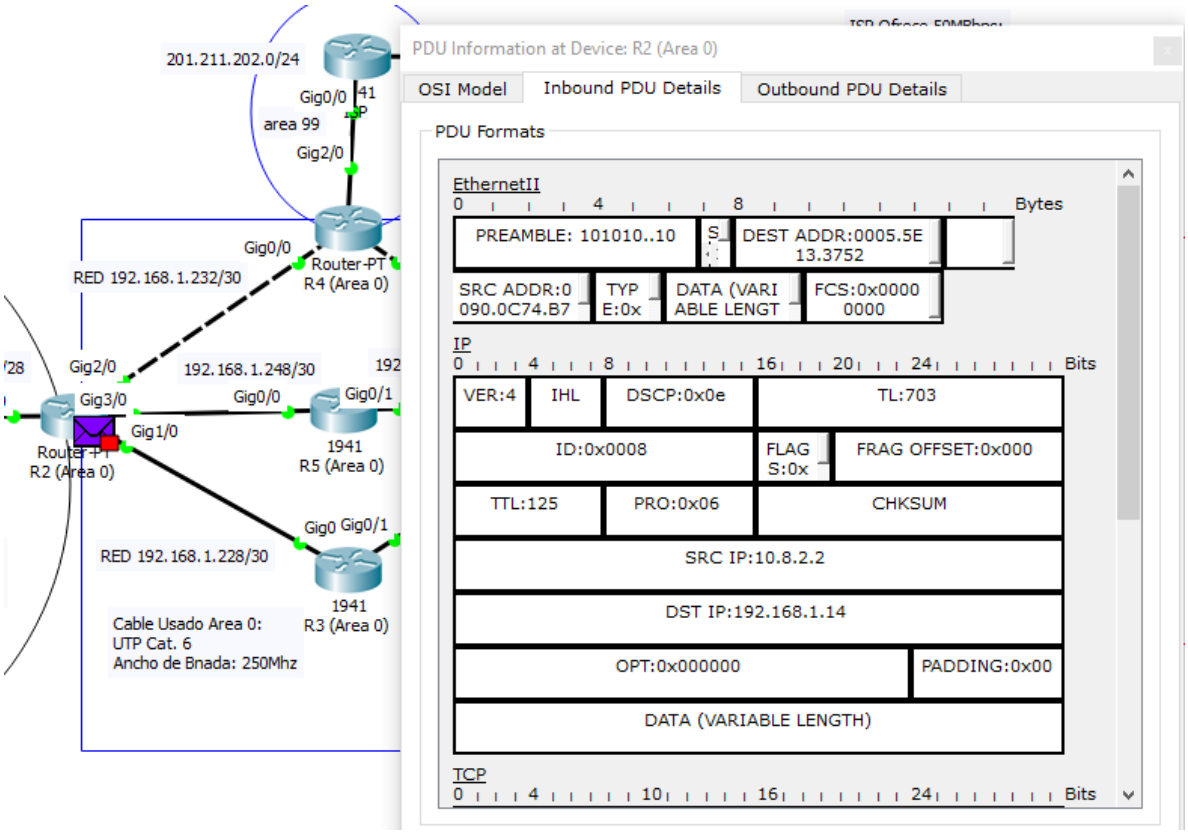


Figura 43:
Fuente: José Escalona

· Ejemplificación de la Política QoS aplicadas al tráfico saliente de cada interfaz.

En la siguiente figura se podrá observar cómo sería las políticas QoS configurada que se basa en una configuración CBWFQ y LLQ. Ver figura 44.

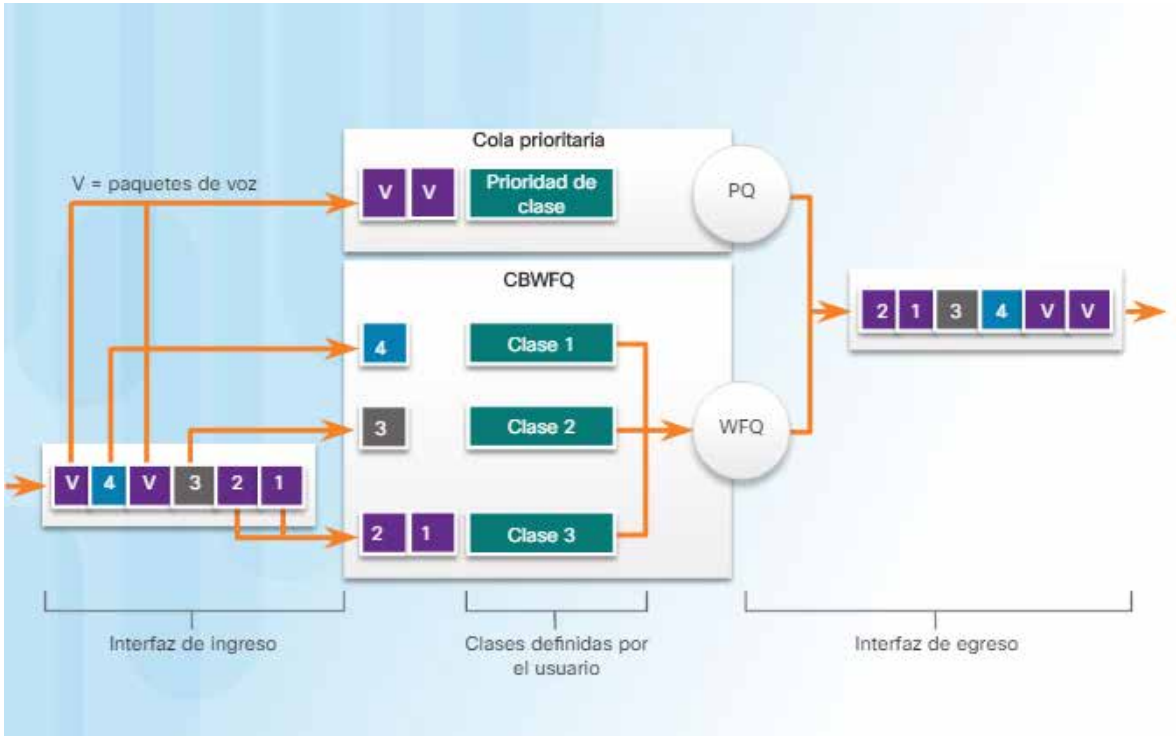


Figura 44
Fuente: José Escalona

Se demostró la verificación y resultados de la configuración de calidad de servicio tanto de marcado como política QoS en toda la red tiene plena funcionalidad, lo pudimos observar con la petición HTTP para ver la página de *google* la cual fue marcada antes de entrar al núcleo de la red área 0 y debidamente tratada con privilegios a lo largo de toda la red hasta llegar al router ISP. Cada clase tiene criterios diferentes por el tipo de protocolo defino en ellas pero funcionara de manera similar al mostrado con la petición HTTP que realizamos.

Con esta configuración se logró aumentar el rendimiento de la red de manera muy satisfactoria ya que nos permite priorizar el tráfico y evitar congestiones en la red. La calidad de servicio en un factor determinante en las redes de hoy en día por las exigencias que debemos cumplir para satisfacer las necesidades de los clientes, las políticas de QoS aplicadas en la red construida en este proyecto de grado pueden ser

ejemplos para ser aplicadas en redes más complejas y con configuraciones más avanzadas.

· Resultados del funcionamiento de MPLS mendiante captura de mensajes de Wireshark.

Vamos a realizar un ping entre la PC-1 y PC-2, para vizualizar el funcioanmiento del protocolo MPLS, debido que los paquetes ICMP tiene que pasar por el area 0 donde se le coloca al encabezado IP una etiqueta para definir la ruta que tomara hasta salir del area 0. Ver figura 45

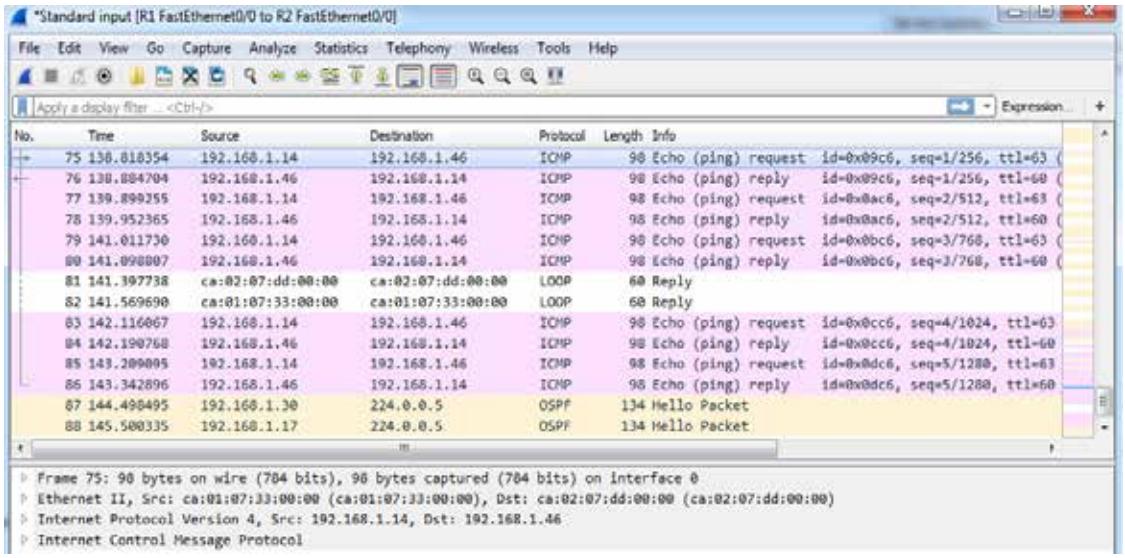


Figura 45:
Fuente: José Escalona

En la figura 45 podemos observar la captura de paquetes de la int. f0/0 del R1, en donde se vizualizan los paquetes ICMP del ping que realizamos entre la PC-1 y PC-2 que fue exitoso, como podemos notar no aparece el procolo MPLS ya que el R1 pertenece al area 1. Ahora ver figura 46

```
R2#sh mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label     3.0.0.0/32       0             Gi1/0       192.168.1.230
17     Pop Label     192.168.1.240/30 0             Gi1/0       192.168.1.230
18     20            6.0.0.2/32       681           Gi1/0       192.168.1.230
       16            6.0.0.2/32       0             Gi2/0       192.168.1.234
       16            6.0.0.2/32       0             Gi3/0       192.168.1.250
19     Pop Label     5.0.0.0/32       0             Gi3/0       192.168.1.250
20     Pop Label     192.168.1.236/30 0             Gi2/0       192.168.1.234
21     Pop Label     192.168.1.252/30 0             Gi3/0       192.168.1.250
22     24            192.168.1.48/28  0             Gi1/0       192.168.1.230
       24            192.168.1.48/28  0             Gi2/0       192.168.1.234
       23            192.168.1.48/28  0             Gi3/0       192.168.1.250
23     No Label      192.168.1.0/28   980           Fa0/0       192.168.1.17
24     Pop Label     4.0.0.0/32       0             Gi2/0       192.168.1.234
25     Pop Label     201.211.202.0/24 0             Gi2/0       192.168.1.234
26     28            192.168.1.32/28  0             Gi1/0       192.168.1.230
       28            192.168.1.32/28  0             Gi2/0       192.168.1.234
       29            192.168.1.32/28  0             Gi3/0       192.168.1.250
R2#
```

Figura 46:
Fuente: José Escalona

En la figura 46 podemos observar la tabla forwarding-table del R2, donde vemos las diferentes etiquetas que pueden ser asignadas a un paquete dependiendo de la dirección IP de destino, también muestra la interfaz de salida de la etiqueta asignada y la dirección IP de siguiente salto. Siguiendo la tabla mostrada al ping realizado entre PC-1 Y PC-2 se le asigno la etiqueta número 28 mediante un proceso Push (empujar) a los paquetes ICMP con interfaz de salida Gi1/0 del R2 con dirección de siguiente salto 192.168.1.230. Ver figura 47

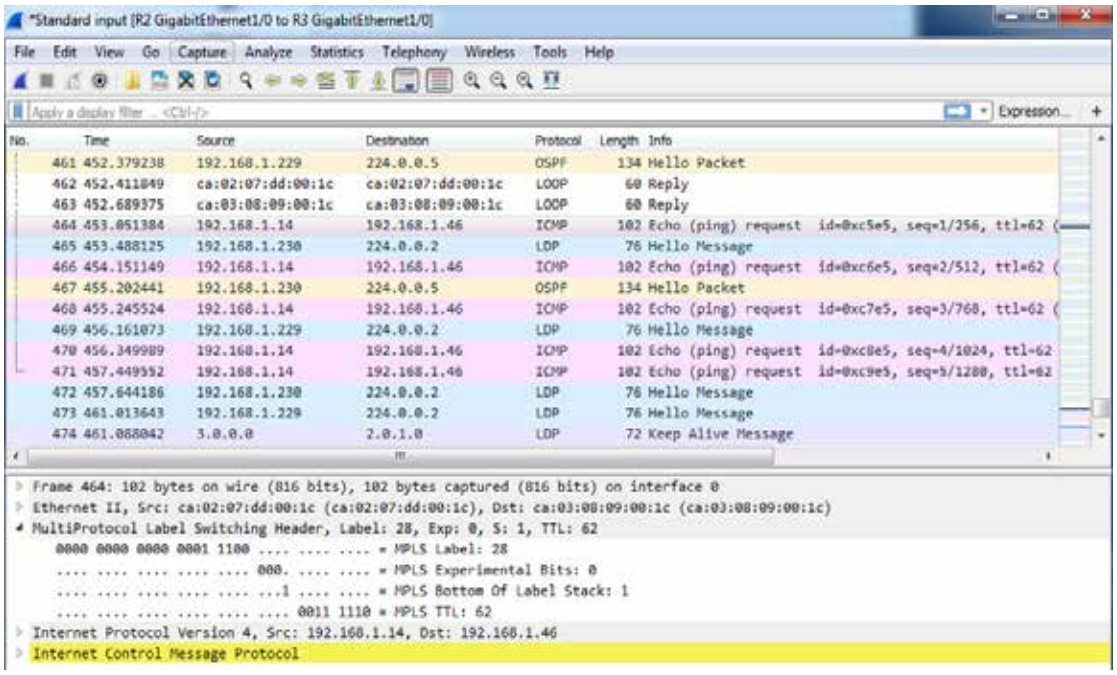


Figura 47:
Fuente: José Escalona

En efecto a lo anterior mencionado podemos observar en la figura 47 que a los paquetes ICMP enviados por la int. Gi1/0 se les asigno la etiqueta número 28 dirigidos al R3, solo se observan los 5 paquetes request (solicitud) del protocolo ICMP debido que OSPF trabaja con balanceo de carga, es decir, que por otra interfaz se mandaron los paquetes reply (respuesta) del protocolo ICMP. Ver figura 48

```
R3#sh mpls forwarding-table
Local  Outgoing      Prefix           Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id     Switched      interface
16     Pop Label     2.0.1.0/32       0             Gi1/0       192.168.1.229
17     Pop Label     192.168.1.248/30 0             Gi1/0       192.168.1.229
18     Pop Label     192.168.1.232/30 0             Gi1/0       192.168.1.229
19     Pop Label     192.168.1.16/28  0             Gi1/0       192.168.1.229
20     Pop Label     6.0.0.2/32       669           Gi2/0       192.168.1.242
21     19            5.0.0.0/32       0             Gi1/0       192.168.1.229
       16            5.0.0.0/32       2418          Gi2/0       192.168.1.242
22     Pop Label     192.168.1.236/30 0             Gi2/0       192.168.1.242
23     Pop Label     192.168.1.252/30 0             Gi2/0       192.168.1.242
24     Pop Label     192.168.1.48/28  0             Gi2/0       192.168.1.242
25     23            192.168.1.0/28   0             Gi1/0       192.168.1.229
26     24            4.0.0.0/32       0             Gi1/0       192.168.1.229
       23            4.0.0.0/32       0             Gi2/0       192.168.1.242
27     25            201.211.202.0/24 0             Gi1/0       192.168.1.229
       24            201.211.202.0/24 0             Gi2/0       192.168.1.242
28     26            192.168.1.32/28  1020          Gi2/0       192.168.1.242
R3#
```

Figura 48:
Fuente: José Escalona

En la figura 49 se observa la tabla forwarding-table del R3, donde se recibirán los paquetes request (solicitud) del ping realizo entre PC-1 y PC-2 con una etiqueta número 28 a la cual se le realizara un proceso Swap (intercambio) y se le coloco la etiqueta número 26 la cual define la red destino por medio de la int. Gi 2/0 con siguiente salto 192.168.1.242. Ver figura 49.

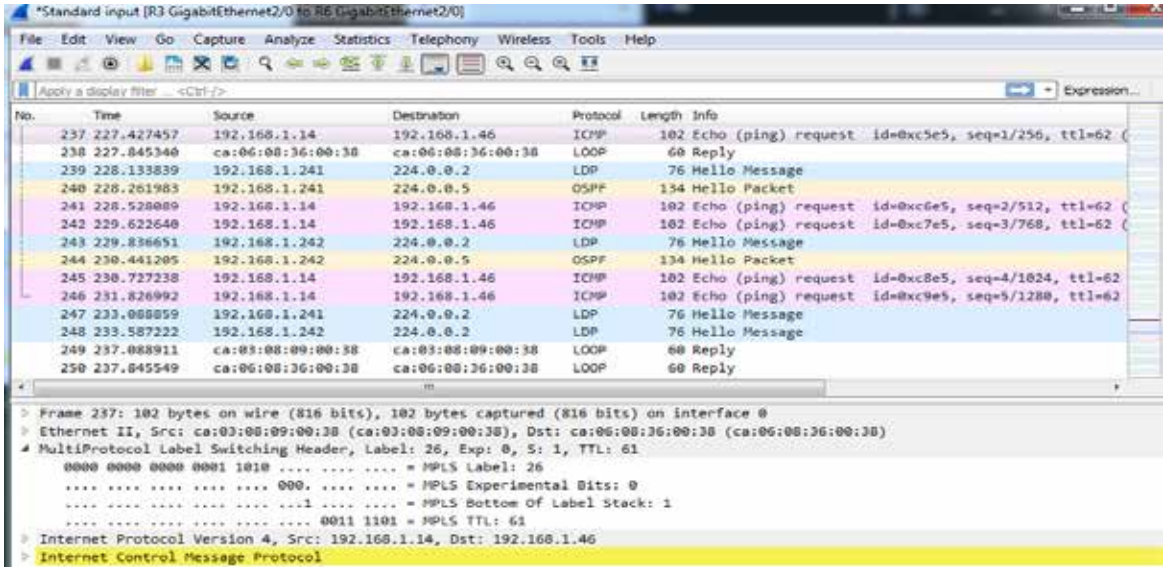
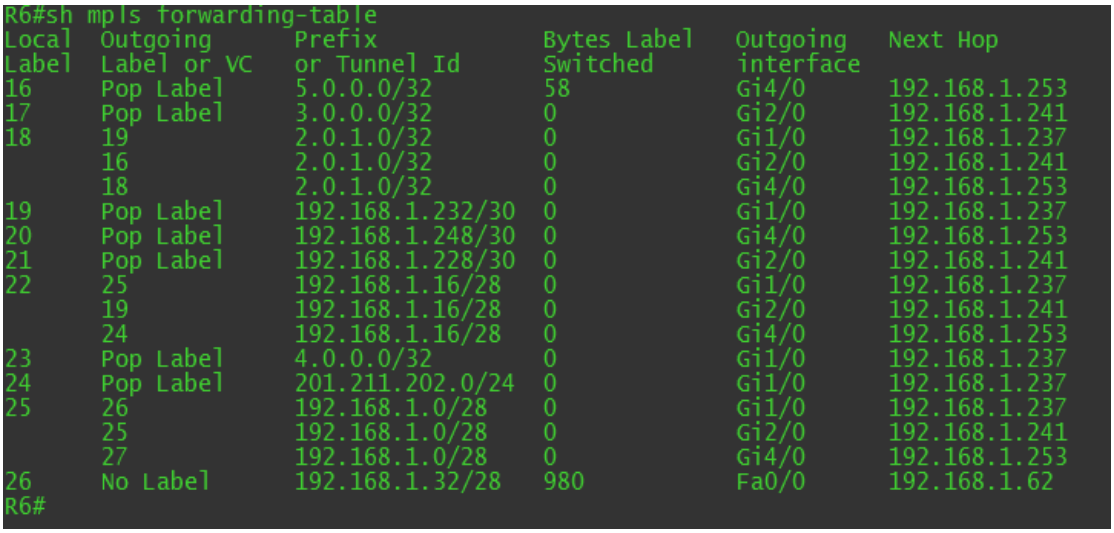


Figura 49:
Fuente: José Escalona

En la imagen 49 podemos ver que se le asignó al paquete ICMP request (solicitud) la etiqueta número 26. Ver imagen 50.



```
R6#sh mpls forwarding-table
Local  Outgoing      Prefix            Bytes Label   Outgoing    Next Hop
Label  Label or VC   or Tunnel Id      Switched      interface
16     Pop Label     5.0.0.0/32        58            Gi4/0       192.168.1.253
17     Pop Label     3.0.0.0/32        0             Gi2/0       192.168.1.241
18     19            2.0.1.0/32        0             Gi1/0       192.168.1.237
       16            2.0.1.0/32        0             Gi2/0       192.168.1.241
       18            2.0.1.0/32        0             Gi4/0       192.168.1.253
19     Pop Label     192.168.1.232/30  0             Gi1/0       192.168.1.237
20     Pop Label     192.168.1.248/30  0             Gi4/0       192.168.1.253
21     Pop Label     192.168.1.228/30  0             Gi2/0       192.168.1.241
22     25            192.168.1.16/28   0             Gi1/0       192.168.1.237
       19            192.168.1.16/28   0             Gi2/0       192.168.1.241
       24            192.168.1.16/28   0             Gi4/0       192.168.1.253
23     Pop Label     4.0.0.0/32        0             Gi1/0       192.168.1.237
24     Pop Label     201.211.202.0/24  0             Gi1/0       192.168.1.237
25     26            192.168.1.0/28    0             Gi1/0       192.168.1.237
       25            192.168.1.0/28    0             Gi2/0       192.168.1.241
       27            192.168.1.0/28    0             Gi4/0       192.168.1.253
26     No Label      192.168.1.32/28   980           Fa0/0       192.168.1.62
R6#
```

Figura 50:
Fuente: José Escalona

La figura 50 muestra la tabla forwarding-table del R6, donde se observa que los paquetes con la etiqueta numero 26 serán enviados por la int. Fa0/0 con siguiente salto 192.168.1.62 sin etiqueta, es decir, los paquetes ICMP request (solicitub) del ping realizado entre PC-1 y PC-2 al llegar al R6 serán enviados sin etiquetas por la int Fa0/0 ya que la red destino se encuentra en el área 1 que no está configurada con MPLS y la int Fa0/0 pertenece a ella. Ver figura 51.

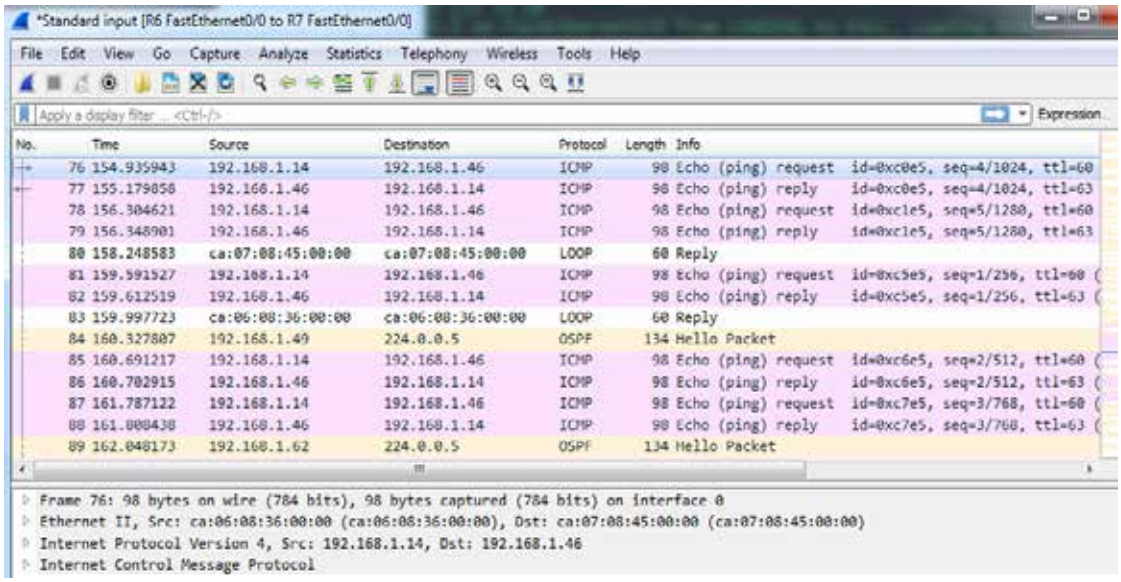


Figura 51:
Fuente: José Escalona

Para culminar podemos ver que en la Figura 52, los paquetes ICMP que llegaron al R7 por medio de la int Fa0/0 no tienen ningún encabezado MPLS por lo mencionado anteriormente y también que el ping realizo entre PC-1 y PC-2 se logró de manera satisfactoria, debido que en la captura de paquetes podemos observar los 5 paquetes resquest (solicitud) y los 5 paquetes reply (respuesta).

Mediante todas las imágenes mostradas anteriormente, se puede demostrar el funcionamiento de MPLS. Siendo MPLS un protocolo que se debe aplicar siempre en el núcleo de la red con base en un protocolo de enrutamiento dinámico que en nuestro caso fue OSPF, de esta manera se puede observar que cuando llega un paquete al router frontera entre la red IP y MPLS el cual recibe el nombre de LER se sabe que ruta debe tomar por los diferentes routers los cuales reciben el nombre de LSR hasta llegar a su destino, esa ruta recibe el nombre LSP lo cual permite un ahorro sustancial del tiempo en que un paquete debe llegar a su destino, de esa forma al ingresar un paquete al dominio MPLS se sabe de antemano que interfaz esta congestionada y cual descongestionada por medio de los mensajes Hello LDP y de esta manera se elegirá el camino más adecuado para que el paquete llegue a su

destino sin problemas y ni retrasos, eso combinado con calidad de servicio nos permite obtener una red totalmente optimizada, lo que nos permite aplicar estos dos protocolos en redes más grandes y complejas permitiendo ofrecer una fiabilidad con la cual nuestro cliente se sienta satisfecho y cómodo con el servicio prestado lo cual es el objetivo que se debe cumplir.

CONCLUSIONES

La evolución imparable de las tecnologías de redes hace extenuante la labor de análisis y recopilación de soluciones para la red. La ingeniería de tráfico en redes MPLS ofrece importantes herramientas de optimización de red que pueden ser utilizadas en situaciones de congestión, mediante el mecanismo de tráfico TE que permiten enviar el tráfico en caminos diferentes al definido por el IGP, obteniendo así mejores niveles de rendimiento de red y optimización en el uso de los recursos disponibles, especialmente el ancho de banda, que constituye uno de los recursos más críticos para los proveedores de servicio

MPLS apareció solventando los problemas y aportando escalabilidad y control sobre la red.

La creatividad de los ingenieros y diseñadores de redes nos ha enseñado que el paradigma de la conmutación aporta mayor escalabilidad de redes, mayor control en la QoS y, lo que más importa a las empresas, mayor control sobre la ingeniería de tráfico (accounting y gestión de recursos). Siendo MPLS, a nuestro parecer, el ejemplo que engloba todas estas características.

La eficiencia para la investigación está enfocada en el tiempo de ejecución del encaminamiento en el plano de control. El enrutador PE anuncia todas las rutas de todos los sitios conectados a él. Dispone de buenas propiedades de escala, ya que ha incorporado en los mecanismos control de flujo para el envío y recepción de mensajes, que permiten el control de error y de flujo, y no requiere de anuncios periódicos de información de enrutamiento, basándose solo en actualizaciones incrementales

RECOMENDACIONES

- Continuar promoviendo proyectos de investigación que estimulen el ingenio y la participación de estudiantes de la UJAP en cuanto al desarrollo tecnológico y diseño de redes.

- Incluir el contenido programático del protocolo MPLS y calidad de servicio en la asignatura de redes de comunicaciones con el fin de impulsar la profundización de la temática iniciada en este trabajo y lograr nuevos conocimientos que permitan investigaciones más avanzadas e innovadoras.

- Impulsar en futuras generaciones de la carrera la implementación del protocolo en una red para generar investigaciones de mayor impacto metodológico que permitan la innovación y puesta en práctica del ingenio propio de nuestra carrera

REFERENCIAS BIBLIOGRÁFICAS

IMPRESAS

Arias, F. (2012). **El proyecto de investigación, Introducción a la metodología científica**. Editorial EPISTEME. Caracas Venezuela.

Borrero. F (2014). **Desarrollo de un manual de prácticas para el laboratorio de transmisión de datos**, tesis de grado, Universidad José Antonio Páez, Valencia edo. Carabobo.

Castro, E. (2015). **Diseño y simulación de una red MPLS para interconectar estaciones remotas utilizando el emulador GNS3** (**trabajo de grado).** Universidad Politécnica Salesiana, Guayaquil. Ecuador

Cerda, H. (1991). **Los elementos de la investigación: como reconocerlos, diseñarlos y construirlos.** Colombia: Editorial El Buho.

Couch, L. (2.008). **Sistemas de comunicación digitales y analógicos.** México: Editorial Pearson Educación.

Crow, W. (2016**). Análisis de calidad de servicio en transferencia de voz y video en una red de tecnología MPLS (Multi-Protocol Label Switching). (Trabajo de grado).** Escuela Superior Politécnica de Chimborazo. Ecuador

Forouzan, B. (2.007). **Transmisión de datos y redes de comunicaciones.** España: Editorial McGraw-Hill.

Freeman, R. (1.999). **Fundamentals of telecommunications.** Estados Unidos: John Wiley & Sons, Inc.

Hernández, S., Fernández, C., Baptista, M. (2014). **Metodología de la investigación**. México: Editorial McGraw-Hill.

Labrador y Otros, (2002). **Metodología**. Valencia: Editorial Clemente.

Magaña, E., Izkue, E., Prieto., Villadangos, J. (2003). **Comunicaciones y redes de computadores problemas y ejercicios resueltos.** España: Editorial Pearson Educación.

Mendez, C. (2011). **Metodología: Diseño y desarrollo del proceso de investigación**. México: Editorial McGraw-Hill.

Moreno y Quispe (2017). **Análisis y mejora de la red de datos de la UNSAAC sobre la plataforma IP-MPLS en un banco de pruebas. (Trabajo de grado).** Universidad nacional de San Antonio Abad del Cusco. Perú

Sabino, C. (1.986). **El proceso de investigación.** Caracas: Panapo.

Stallings, W. (2.008). **Comunicaciones y redes de computadoras.** España: Editorial Pearson Educación.

Tanembaum, A. (2.003). **Redes de computadoras.** México: Editorial Pearson Educación.

Tomasi, W. (2.003). **Sistemas de comunicaciones electrónicas**. México: Editorial Pearson Educación.

ELECTRÓNICAS

Cisco, (2015) **Admin distance,** consultado el 14 de octubre de 2018 desde:https://www.cisco.com/c/es_mx/support/docs/ip/border-gateway-protocol-bgp/15986-admin-distance.html

Cisco, (2015) **QoS policing**, consultado el 20 de octubre de 2018 desde:https://www.cisco.com/c/es_mx/support/docs/quality-of-service-qos/qos-policing/28882-carcounters.html

Cisco, (2015) **QoS packet marking**, consultado el 20 de octubre de 2018 desde:https://www.cisco.com/c/en/us/support/docs/quality-of-service-qos/qos-packet-marking/10103-dscpvalues.html

Frlp. (s/f) **Ruteo OSPF**, consultado el 16 de octubre de 2018 desde:http://www.frlp.utn.edu.ar/materias/internetworking/apuntes/OSPF/Ruteo-OSPF.pdf

Ldc. (s/f) **Funcionamiento de envió**, consultado el 12 de octubre de 2018 desde:https://ldc.usb.ve/~poc/RedesII/Grupos/G5/funcionamiento_envio.htm

Mikroways. (s/f) **Introducción a OSPF,** consultado el 16 de octubre de 2018 desde: https://www.mikroways.net/2009/07/20/introduccion-a-ospf/

Sites Google. (s/f) **Descripcion de diffserv,** consultado el 23 de octubre de 2018 desde: https://sites.google.com/site/redescovergentesingluis/unidad-ii/3---descripcion-de-diffserv

Suryaokhrabo. (s/f) **MPLS Lable**, consultado el 10 de octubre de 2018 desde: https://suryaokhrabo.blogspot.com/2016/07/blog-post.html

Techopedia. (s/f) **Customer edger outer ce router**, consultado el 11 de octubre de 2018 desde: https://www.techopedia.com/definition/16492/customer-edge-router-ce-router

Textos Científicos. (s/f) **Comparación del modelo OSI Y TCP/IP**, consultado el 6 de octubre de 2018desde: https://www.textoscientificos.com/redes/tcp-ip/comparacion-modelo-osi

Wikipedia. (s/f) **Multiprotocol Label Switching**, consultado el 12 de octubre de 2018 desde: https://es.wikipedia.org/wiki/Multiprotocol_Label_Switch

ANEXOS

Anexo A. Configuración OSPF del R1.

```
router ospf 10
 router-id 1.0.0.1
 log-adjacency-changes
 area 1 authentication message-digest
 area 1 stub
 passive-interface FastEthernet3/0
 network 192.168.1.0 0.0.0.15 area 1
 network 192.168.1.16 0.0.0.15 area 1
```

Anexo B. Configuración OSPF R2.

```
router ospf 10
 mpls ldp autoconfig area 0
 router-id 2.0.1.0
 log-adjacency-changes
 auto-cost reference-bandwidth 1000
 area 1 authentication message-digest
 area 1 stub no-summary
 area 2 authentication message-digest
 network 2.0.1.0 0.0.0.0 area 0
 network 192.168.1.16 0.0.0.15 area 1
 network 192.168.1.228 0.0.0.3 area 0
 network 192.168.1.232 0.0.0.3 area 0
 network 192.168.1.248 0.0.0.3 area 0
```

Anexo C. Configuraciones aplicadas a interfaces R6.

```
interface Loopback1
 ip address 6.0.0.2 255.255.255.255
!
interface FastEthernet0/0
 ip address 192.168.1.49 255.255.255.240
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 060C0032491F504051
 ip ospf cost 1
 ip ospf priority 254
 duplex full
 service-policy output POLITICA-QoS
!
interface GigabitEthernet1/0
 ip address 192.168.1.238 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 141D1D180955737270
 ip ospf priority 0
 negotiation auto
 service-policy output POLITICA-QoS
!
interface GigabitEthernet2/0
 ip address 192.168.1.242 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 07052E5F4B58405C43
 ip ospf priority 0
 negotiation auto
 service-policy output POLITICA-QoS
!
interface GigabitEthernet3/0
 no ip address
 shutdown
 negotiation auto
!
interface GigabitEthernet4/0
 ip address 192.168.1.254 255.255.255.252
 ip ospf authentication message-digest
 ip ospf message-digest-key 1 md5 7 045104150A7015175D
 ip ospf priority 0
 negotiation auto
 service-policy output POLITICA-QoS
```

Anexo D. Configuración de política de marcado R1.

```
class-map match-any VOIP
 match access-group 101
class-map match-all VIDEO-STREAMING-DSCP
 match ip dscp ef
class-map match-any TRAFICO-MEDIO-DSCP
 match ip dscp af22
class-map match-all VIDEO-STREAMING
 match access-group 102
class-map match-any TRAFICO-MEDIO
 match protocol ftp
 match protocol tftp
 match protocol imap
 match protocol pop3
 match protocol smtp
policy-map MARCADO-FRON-R1
 class VOIP
  set ip dscp ef
 class VIDEO-STREAMING
  set ip dscp ef
 class TRAFICO-IMPORTANTE
  set ip dscp af13
 class TRAFICO-MEDIO
  set ip dscp af22
 class class-default
```

Anexo E. Configuración de ruta por defecto y ruta estática Router ISP.

```
ip route 0.0.0.0 0.0.0.0 FastEthernet0/0
ip route 172.16.2.1 255.255.255.255 FastEthernet0/0
```

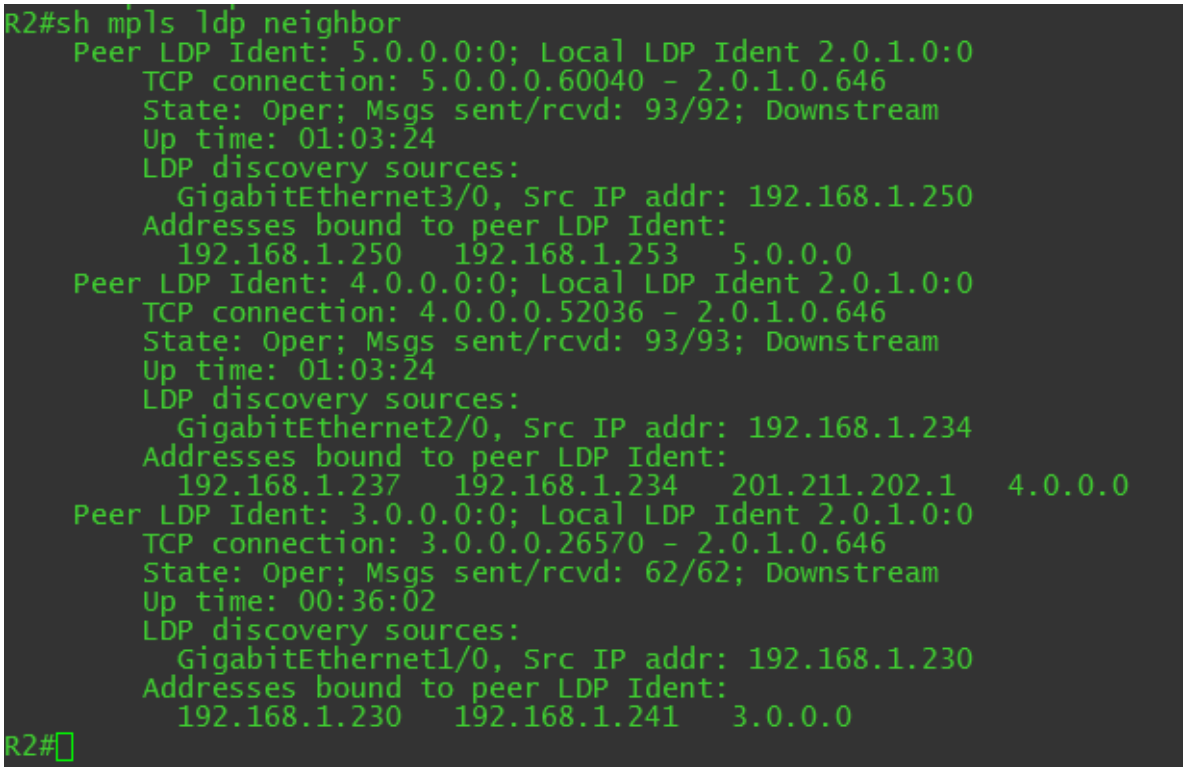
Anexo F. Configuración OSPF Router ISP.

```
router ospf 10
 router-id 8.0.0.0
 log-adjacency-changes
 area 99 authentication message-digest
 redistribute static subnets
 network 201.211.202.0 0.0.0.255 area 99
 default-information originate
!
```

Anexo G. Configuración de política QoS R3.

```
class-map match-all VIDEO-STREAMING-DSCP
 match ip dscp ef
class-map match-any TRAFICO-MEDIO-DSCP
 match ip dscp af22
class-map match-any VOIP-DSCP
 match ip dscp ef
class-map match-any TRAFICO-IMPORTANTE-DSCP
 match ip dscp af13
!
!
policy-map POLITICA-QoS
 class VOIP-DSCP
    priority 400
 class TRAFICO-IMPORTANTE-DSCP
    bandwidth 10000
    shape average 16000000
     random-detect dscp-based
 class TRAFICO-MEDIO-DSCP
    bandwidth 15000
    shape average 20000000
     random-detect dscp-based
 class VIDEO-STREAMING-DSCP
    priority 25000
 class class-default
    fair-queue 16
    queue-limit 25 packets
!
```

Anexo H. Tabla de vecinos MPLS R2.

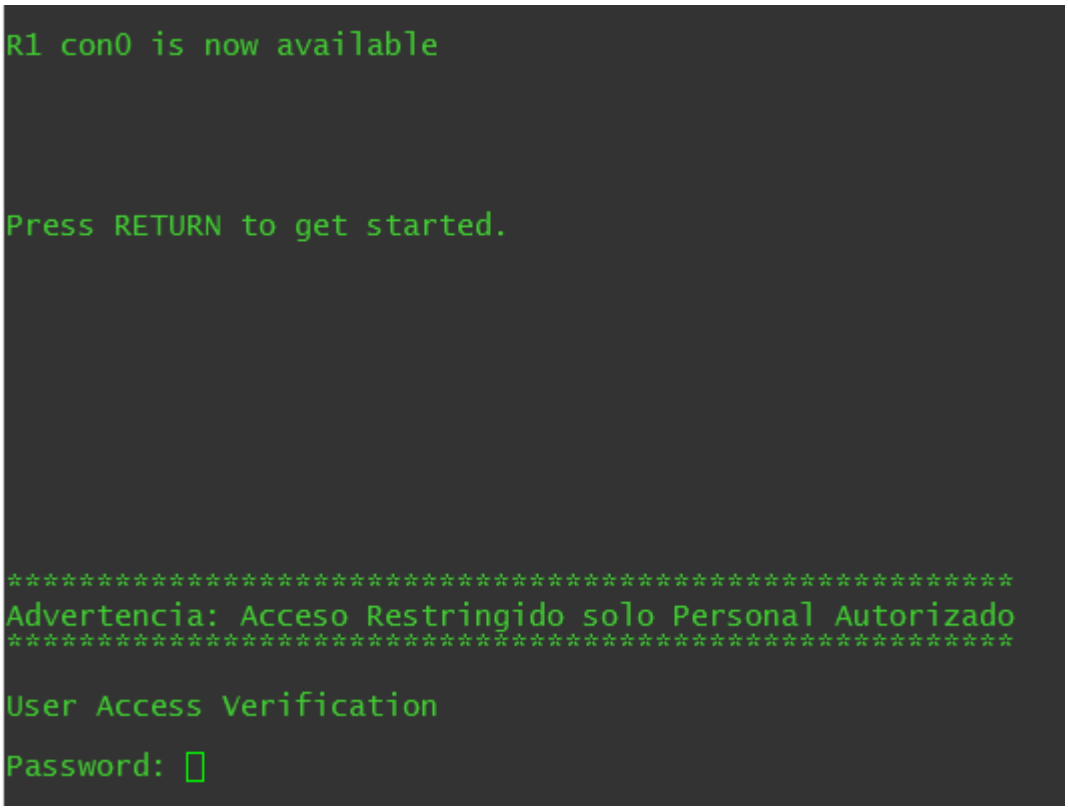


Anexo I. Tabla IP LIB MPLS R6.

```
R6#sh mpls ip binding
  0.0.0.0/0
        in label:      imp-null
        out label:     imp-null  lsr: 3.0.0.0:0
        out label:     imp-null  lsr: 5.0.0.0:0
        out label:     imp-null  lsr: 4.0.0.0:0         inuse
  2.0.1.0/32
        in label:      18
        out label:     18        lsr: 5.0.0.0:0         inuse
        out label:     16        lsr: 3.0.0.0:0         inuse
        out label:     19        lsr: 4.0.0.0:0         inuse
  3.0.0.0/32
        in label:      17
        out label:     17        lsr: 5.0.0.0:0
        out label:     imp-null  lsr: 3.0.0.0:0         inuse
        out label:     18        lsr: 4.0.0.0:0
  4.0.0.0/32
        in label:      23
        out label:     25        lsr: 5.0.0.0:0
        out label:     26        lsr: 3.0.0.0:0
        out label:     imp-null  lsr: 4.0.0.0:0         inuse
  5.0.0.0/32
        in label:      16
        out label:     imp-null  lsr: 5.0.0.0:0         inuse
        out label:     21        lsr: 3.0.0.0:0
        out label:     17        lsr: 4.0.0.0:0
  6.0.0.2/32
        in label:      imp-null
        out label:     16        lsr: 5.0.0.0:0
        out label:     20        lsr: 3.0.0.0:0
        out label:     16        lsr: 4.0.0.0:0
  172.16.2.1/32
        in label:      27
        out label:     28        lsr: 5.0.0.0:0
        out label:     29        lsr: 3.0.0.0:0
        out label:     27        lsr: 4.0.0.0:0         inuse
  192.168.1.0/28
        in label:      25
        out label:     27        lsr: 5.0.0.0:0         inuse
        out label:     25        lsr: 3.0.0.0:0         inuse
        out label:     26        lsr: 4.0.0.0:0         inuse
  192.168.1.16/28
        in label:      22
        out label:     24        lsr: 5.0.0.0:0         inuse
        out label:     19        lsr: 3.0.0.0:0         inuse
        out label:     25        lsr: 4.0.0.0:0         inuse
  192.168.1.32/28
        in label:      26
        out label:     29        lsr: 5.0.0.0:0
        out label:     28        lsr: 3.0.0.0:0
        out label:     28        lsr: 4.0.0.0:0
  192.168.1.48/28
        in label:      imp-null
        out label:     23        lsr: 5.0.0.0:0
        out label:     24        lsr: 3.0.0.0:0
        out label:     24        lsr: 4.0.0.0:0
  192.168.1.228/30
        in label:      21
        out label:     22        lsr: 5.0.0.0:0
        out label:     imp-null  lsr: 3.0.0.0:0         inuse
```

```
  192.168.1.232/30
        in label:     19
        out label:    20         lsr: 5.0.0.0:0
        out label:    18         lsr: 3.0.0.0:0
        out label:    imp-null   lsr: 4.0.0.0:0        inuse
  192.168.1.236/30
        in label:     imp-null
        out label:    19         lsr: 5.0.0.0:0
        out label:    22         lsr: 3.0.0.0:0
        out label:    imp-null   lsr: 4.0.0.0:0
  192.168.1.240/30
        in label:     imp-null
        out label:    21         lsr: 5.0.0.0:0
        out label:    imp-null   lsr: 3.0.0.0:0
        out label:    21         lsr: 4.0.0.0:0
  192.168.1.248/30
        in label:     20
        out label:    imp-null   lsr: 5.0.0.0:0        inuse
        out label:    17         lsr: 3.0.0.0:0
        out label:    23         lsr: 4.0.0.0:0
  192.168.1.252/30
        in label:     imp-null
        out label:    imp-null   lsr: 5.0.0.0:0
        out label:    23         lsr: 3.0.0.0:0
        out label:    20         lsr: 4.0.0.0:0
  201.211.202.0/24
        in label:     24
        out label:    26         lsr: 5.0.0.0:0
        out label:    27         lsr: 3.0.0.0:0
        out label:    imp-null   lsr: 4.0.0.0:0        inuse
R6#
```

Anexo J. Line 0 R1.



Anexo K

Lineas de comando:
R1(Config)#access-list 101 permit udp any any range 16384 32767 (Creando la lista de acceso de nombre 101 para definir el trafico VOIP UDP) R1(Config)#access-list 101 permit tcp any any eq 1720 (Creando la lista de acceso de nombre 101 para definir el trafico VOIP TCP) R1(Config)#access-list 102 permit udp any any eq 554(Creando la lista de acceso de nombre 102 para definir el trafico Video Streaming UDP)

Anexo L. Creación de líneas de acceso

Líneas de comandos
R1(Config)#class-map match-any VOIP (Creación de la clase VOIP) R1(config-cmap)#match access-group 101 (Asignado la lista de acceso a la clase VOIP) R1(config-cmap)#exit (Saliendo de la clase de VOIP) R1(Config)#class-map match-all VIDEO-STREAMING (Creación de la clase Video Streaming) R1(config-cmap)#match access-group 102 (Asignado la lista de acceso a la clase Video Streaming) R1(config-cmap)#exit (Saliendo de la clase de Video Streaming) R1(Config)#class-map match-any TRAFICO-MEDIO (Creación de clase trafico medio) R1(config-cmap)#match protocol ftp (Asignando los protocolos correspondiente a la clase) R1(config-cmap)#match protocol tftp R1(config-cmap)#match protocol imap R1(config-cmap)#match protocol pop3 R1(config-cmap)#match protocol smtp R1(config-cmap)#exit (Saliendo de la clase trafico medio) R1(Config)#class-map match-any TRAFICO-IMPORTANTE (creación de la clase trafico importante) R1(config-cmap)#match protocol http (Asignando los protocolos correspondiente a la clase) R1(config-cmap)#match protocol telnet R1(config-cmap)#match protocol ssh R4(config-cmap)#exit

Anexo M. Creación de clases

Líneas de comando
R1(Config)# policy-map MARCADO-FRON-R1 (Creación de la política de marcado) R1(config-pmap)#class VOIP (Entramos a la clase VOIP) R1(config-pmap-c)#set ip dscp ef (Marcamos la clase) R1(config-pmap-c)#exit (Salimos de la clase) R1(config-pmap)#class VIDEO-STREAMING (Entramos a la clase Video Streaming) R1(config-pmap-c)#set ip dscp ef (Marcamos la clase) R1(config-pmap-c)#exit (Salimos de la clase) R1(config-pmap)#class TRAFICO-IMPORTANTE (Entramos a la clase tráfico importante) R1(config-pmap-c)#set ip dscp af13 R1(config-pmap-c)#exit (Salimos de la clase) R1(config-pmap)#class TRAFICO-MEDIO (Entramos a la clase tráfico medio) R1(config-pmap-c)#set ip dscp af22 (Marcamos la clase) R1(config-pmap-c)#exit (Salimos de la clase) R1(config-pmap)#class class-default (Entramos a la clase default para crearla nada mas)

(Anexo N) Marcado de paquetes

Líneas de comando
Comandos empleados para la configuración del tráfico saliente de cada interfaz. R1(Config)# class-map match-any VOIP-DSCP (Creación de la clase VOIP DSCP) R1(config-cmap)#match ip dscp ef (Asignamos un valor DSCP) R1(config-cmap)#exit (Saliendo de la clase de VOIP DSCP) R1(Config)# class-map VIDEO-STREAMING-DSCP (Creación de la clase Video Streaming DSCP) R1(config-cmap)#match ip dscp ef (Asignamos un valor DSCP a esta clase) R1(config-cmap)#exit (Saliendo de la clase de Video Streaming DSCP) R1(Config)# class-map match-any TRAFICO-IMPORTANTE-DSCP (Creación de la clase trafico importante DSCP R1(config-cmap)#match ip dscp af13 (Asignamos un valor DSCP a esta clase) R1(config-cmap)#exit (Saliendo de la clase trafico importante DSCP) R1(Config)# class-map match-any TRAFICO-MEDIO-DSCP (Creación de la clase trafico medio DSCP) R1(config-cmap)#match ip dscp af22 (Asignamos un valor DSCP a esta clase) R1(config-cmap)#exit (Saliendo de la clase de Video trafico medio) R1(Config)# policy-map POLITICA-QoS (Creamos la política QoS) R1(config-pmap)#class VOIP-DSCP (Entramos a la Clase VOIP DSCP) R1(config-pmap-c)#priority 400 (Definimos criterios) R1(config-pmap-c)#exit (Salimos de la clase) R1(config-pmap)#class VIDEO-STREAMING-DSCP (Entrado a la clase Video Streaming DSCP) R1(config-pmap-c)#priority 25000 (Definimos criterios) R1(config-pmap-c)#exit (Salimos de la clase) R1(config-pmap)#class TRAFICO-IMPORTANTE-DSCP (Entrando a la clase trafico importante DSCP) R1(config-pmap-c)#bandwidth 10000 (Definimos criterios) R1(config-pmap-c)#shape average 16000000 (Definimos criterios) R1(config-pmap-c)#random-detect dscp-based (Definimos criterios) R1(config-pmap-c)#exit (Salimos de la clase) R1(config-pmap)#class TRAFICO-MEDIO-DSCP (Entrando a la clase trafico medio DSCP) R1(config-pmap-c)#bandwidth 15000 (Definimos criterios) R1(config-pmap-c)#shape average 20000000 (Definimos criterios) R1(config-pmap-c)#random-detect dscp-based (Definimos criterios) R1(config-pmap-c)#exit (Salimos de la clase) R1(config-pmap)#class class-default (Entrando a la clase default) R1(config-pmap-c)#fair-queue 16 (Definimos criterios) R1(config-pmap-c)#queue-limit 25 (Definimos criterios)

(Anexo O) Política de tráfico de salida

Lineas de comando
ISP (Config)# class-map match-any TRAFICO-BAJADA (Creamos la clase tráfico de bajada) ISP (config-cmap)# description aseguro trafico http y ftp de un servidor externo (una breve descripccion) ISP (config-cmap)# match protocol http (Asignamos trafico http) ISP (config-cmap)# match protocol ftp (Asignamos trafico ftp) ISP (config-cmap)#exit (salimos de la clase) ISP (Config)# policy-map UP_TRAFICO (Creamos la política de trafico de subida) ISP (config-pmap)#class class-default (Entramos en la clase default) ISP (config-pmap-c)# bandwidth 12500 (Definimos un ancho de banda) ISP (config-pmap-c)#exit (salimos de la clase) ISP (config-pmap)#exit (salimos de la política) ISP (Config)# policy-map DOWN_TRAFICO (Creamos la política de trafico de bajada) ISP (config-pmap)# class TRAFICO-BAJADA (Entramos a la clase tráfico de bajada) ISP (config-pmap-c)# bandwidth 10000 (Definimos un ancho de banda) ISP (config-pmap-c)# shape average 15000000 (Definimos una política shape) ISP (config-pmap-c)#exit (salimos de la clase) ISP (config-pmap)#class class-default (Entramos en la clase default) ISP (config-pmap-c)#bandwidth 15000 (Definimos un ancho de banda) ISP (config-pmap-c)#shape average 22500000 (Definimos una política shape)

Anexo P. Políticas de subida y bajada del ISP

Líneas de comando
R1(Config)# interface g0/0 (entramos en la interfaz) R1(Config-if)# service-policy input MARCADO-FRON-R1(aplicamos la política sea de entrada o salida) R1(Config-if)# service-policy input POLITICA-QoS(aplicamos la política sea de entrada o salida) A continuación los comandos empleados para aplicar las políticas de trafico de subida y bajada. ISP(Config)# interface g0/1 (entramos en la interfaz) ISP(Config-if)# service-policy output UP_TRAFICO (aplicamos la política sea de entrada o salida) ISP(Config-if)# exit (salimos de la interfaz) ISP(Config-if)# interface g0/0 (entramos en la interfaz) ISP(Config-if service-policy output DOWN_TRAFICO (aplicamos la política sea de entrada o salida)

Anexo Q. Aplicar políticas a las interfaces

Líneas de comando
R1(Config)# login block-for 120 attempts 3 within 30 (Prevención contra ataques de fuerza bruta) R1(Config)# enable password cisco1 (Definimos contraseña en modo privilegiado) R1(Config)# no ip domain-lookup (Evitamos la búsqueda DNS en lianas de comandos) R1(Config)# service password-encryption (Activamos encriptación de contraseñas) R1(Config)# banner motd – (Definimos un mensaje de seguridad) ********** Advertencia: Acceso Restringido solo Personal Autorizado **********- R1(Config)# line console 0 (Entramos en la línea 0) R1(Config-line)# password cisco (Definimos la contraseña) R1(Config-line)# exec-timeout 5 (Definimos el tiempo de la sesión sin uso) R1(Config-line)# login R1(Config-line)# exit (salimos) R1(Config)# line vty 0 4 (entramos en las líneas vty que permiten el control a distancia) R1(Config-line)# password jose (Definimos la contraseña) R1(Config-line)# exec-timeout 5 (Definimos el tiempo de la sesión sin uso) R1(Config-line)# login

Anexo R. Configuraciones iniciales de un router y switch

Líneas de comando
ISP (Config)# policy-map UP_TRAFICO (Creamos la política de trafico de subida) ISP (config-pmap)#class class-default (Entramos en la clase default) ISP (config-pmap-c)# police 12500000 156250 312500 (Definimos la política policy con valores CIR, bc y be) ISP (config-pmap-c)#exit (salimos de la clase) ISP (config-pmap)#exit (salimos de la política) ISP (Config)#interface f3/0 R1(Config-if)# service-police input UP_TRAFICO

Anexo S. Políticas de subida en simulador GNS3

Líneas de comando
R5(Config)#ip cef (activamos protocolo cef) R5(Config-if)# interface loopback1 (creamos interfaz loopback) R5(Config-if)# ip address 5.0.0.0 255.255.255.255 (asignamos dirección IP) R5(config-if)# no shutdown (levantaos la interfaz) R5(config-if)#exit (salimos de la interfaz) R5(Config)#mpls label protocol ldp (activamos el protocolo de etiquetas ldp) R5(Config)#mpls ldp router-id loopback1 (asignados interfaz loopback1 a router-id MPLS) R5(Config)#router ospf 10 (entramos en el protocolo OSPF del router) R5(Config)#mpls ldp autoconfig área 0 (activamos cada interfaz del área 0 del R5 con MPLS)

Anexo T, Configuración MPLS en el área 0