PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE INGENIERÍA

MAESTRÍA EN REDES DE COMUNICACIÓN

TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO DE**:**

MASTER EN REDES DE COMUNICACIÓN

TEMA:

EVALUACIÓN DE PARÁMETROS DE CALIDAD DE SERVICIO (QoS) PARA EL DISEÑO DE UNA RED VPN CON MPLS.

MIROSLAVA ARACELY ZAPATA RODRÍGUEZ

DIRECTOR: MsC. Francisco Chafla.

Quito, Marzo 2016

/

Dedicatoria

Este trabajo está dedicado primeramente a Dios quien me ha dado fortaleza, entendimiento para culminar este nuevo reto en mi carrera profesional, en segundo lugar a mi esposo Andrés quién ha sido un apoyo incondicional en todo momento, a mis hijos Stephanie e Ismael que son los luceros de mi corazón, a mis padres quien siempre han sido mi guía en mi camino y a mis hermanos que me han dado siempre su cariño y respaldo.

Agradecimiento

Agradezco a Dios quien me permitió salir adelante en el desarrollo de la tesis, a mi esposo, mis hijos Sthepanie e Ismael que han sido una luz en mi corazón que me impulsan cada día a salir adelante, a mis padres que han sido mi ejemplo y apoyo en mi vida finalmente agradezco al tutor de la tesis por su guía en el desarrollo de la tesis.

ÍNDICE DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

CAPÍTULO I

PERFIL DE TESIS

1 DATOS REFERENCIALES DEL PROYECTO

Tema: Evaluación de parámetros de calidad de servicio (QoS) para el diseño de una red VPN con MPLS.

Alumna Responsable: Ing. Miroslava Zapata Rodríguez.

Orientador: Msc Francisco Chafla.

1.1 ANTECEDENTES

En los últimos años Internet ha ido evolucionando, desarrollándose una gran cantidad de aplicaciones en negocios y mercado de consumo, estas nuevas aplicaciones han llevado al incremento de la demanda de ancho de banda para el área principal de las redes que es el backbone de los proveedores de servicio.

Por el contrario, las demandas de la red en términos de velocidad y ancho de banda de los nuevos servicios y aplicaciones han ido disminuyendo abruptamente los recursos existentes en la Infraestructura de Internet, añadiéndose al problema el crecimiento exponencial en el número de usuarios, el volumen de tráfico y el transporte de bits sobre un backbone.

Adicionalmente en esquemas de redes convencionales IP que son los IP forwarding packet se utiliza ruteo convencional donde los routers analizan la dirección IP destino contenido en el encabezado de red de cada paquete, a medida que el mismo atraviesa la red desde su origen a su destino, donde se configuran los protocolos de enrutamiento estático ó dinámico dentro de los routers creando la tabla de ruteo o “routing table” que permite determinar la dirección destino, este proceso es el ruteo unicast, salto por salto basado en el destino (hop-by-hop detination-based unicast routing).

A pesar de ser un esquema exitoso y desarrollado ampliamente se han detectados problemas como es la disminución en la flexibilidad y velocidad de la red, por lo que nuevas técnicas han sido requeridas para contrarrestar los inconvenientes presentados y al mismo tiempo expandir las funcionalidades de la infraestructura de una red basado en protocolo IP.

Para afrontar los aspectos anteriormente mencionados se han desarrollado nuevas tecnologías emergentes en redes actuales bajo técnicas de packet forwarding como es el MPLS (Multiprotocol Label Switching) o conmutación de etiquetas de múltiples protocolos que dan solución a las limitaciones de velocidad, escalabilidad, manejo de calidad de servicio (QoS) y manejo de tráfico incrementando el rendimiento de la red.

Con esta tecnología se proporciona manejo del ancho de banda y servicios requeridos para las futuras redes “backbone” basados en protocolo IP, permitiendo a la red escalabilidad, ruteo basado en QoS y métricas de calidad de servicio, soportando redes de enlaces existentes de capa 2 como son ATM (Asynchronous Transfer Mode) y Frame Relay, permitiendo a una empresa u organización trabajar con esta tecnología permitiendo una reducción en costos de infraestructura.

En oficinas remotas que cuenta con empresas u organizaciones se ha visto la necesidad de una comunicación segura, fiable y efectiva en costos, encontrando una solución en las redes privadas virtuales con MPLS (VPN MPLS).

Estas redes permiten comunicaciones seguras al intercambiar información entre los diferentes sitios que pertenecen una VPN común con lo que permite a los proveedores de servicio construir intranet y extranets a través de una red pública, adicionalmente una de la principales ventajas de las VPNs son los beneficios que se brinda a las empresas como la conectividad “any-to-any” y la escalabilidad entre los diferentes sitios de una empresa (Rodríguez, 2008).

La tendencia actual en las redes es la convergencia de las comunicaciones en sistemas integrados que permitan transmitir simultáneamente voz, video y datos en una red única dando beneficios de conectividad a las empresas y a sus usuarios. (Trujillo Machado, 2006)

1.2 JUSTIFICACIÓN E IMPORTANCIA

Para el funcionamiento óptimo de una empresa u organización se busca integrar en la red servicios de voz, video y datos ya que se tendrá beneficios como compartición de información sin necesidad de ir a un lugar remoto con lo que se agilitan las tareas que esto involucre, generándose una reducción de costes de administración y mantenimiento e incrementando su cobertura.

Con la tecnología VPN MPLS permite a una empresa u organización integrar voz, video y datos en una plataforma común con garantía de calidad de servicio que es necesario en la actualidad ya que el tráfico de red es muy diverso y cada tipo de tráfico tiene diferentes requerimientos como ancho de banda, jitter, latencia y disponibilidad. Adicionalmente brinda seguridad y permite que estas redes sean escalables y de bajo costo al interconectar subredes privadas de cualquier empresa u organización en una sola red lógica como es el internet. (Pincay Espinoza, 2015).

Existen variados paper, foros, revistas técnicas que discuten las diferentes tecnologías e inducen el uso de la tecnología VPN MPLS, por lo que es necesario realizar el estudio de esta tecnología, ver sus ventajas, sus desventajas y el impacto de su implementación. El desarrollo de este modelo de red VPN MPLS se realizará en base de pruebas a través de un simulador GNS3 que permite diseñar topologías de redes complejas y ponerlos en marcha en tiempo real.

Adicionalmente a nivel de la seguridad a través de una red en el Ecuador, tanto para empresas e instituciones públicas y privadas están dando gran importancia a la fiabilidad de datos como El Plan Integral de Seguridad Nacional, donde las redes VPN MPLS entran a dar solución a esta necesidad.

Debido a la generalidad del diseño de redes orientadas al soporte de voz, video y datos no se contemplan requerimientos de parámetros de calidad de servicio en el diseño de una red, por lo que en el presente trabajo toma en cuenta el estudio de estos requerimientos.

1.3 ALCANCE

El presente trabajo tiene la finalidad de diseñar e implementar una red VPN/MPLS para tres nodos en ambiente de laboratorio (Simulación) con calidad de servicio (QoS), realizando el análisis de las Redes Virtuales Privadas con MPLS para establecer condiciones y requerimientos mínimos de la red, donde se evaluará los parámetros de calidad de servicio (throughput, porcentaje de pérdidas de paquetes, jitter y latencia).

1.4 OBJETIVOS

1.4.1 OBJETIVO GENERAL

Diseñar una red VPN/MPLS en ambiente de laboratorio (Simulación) mediante la evaluación de parámetros de QoS para garantizar la disponibilidad y escalabilidad de la red.

1.4.2 OBJETIVOS ESPECÍFICOS

- Estudiar el estado del Arte de las Redes Virtuales Privadas con MPLS y sus ventajas sobre otras tecnologías de VPN.
- Establecer las condiciones y requerimientos de la red que se va a diseñar para interconectar tres nodos.
- Diseñar la Red VPN-MPLS de tres nodos en ambiente de laboratorio (simulación) y mínimos requerimientos.
- Evaluar los parámetros de calidad de servicio (throughput, porcentaje de pérdidas de paquetes, jitter y latencia) de la red diseñada.
- Realizar las pruebas del correcto funcionamiento de la red implementada en el ambiente de laboratorio (simulación).

1.5 METODOLOGÍA

La metodología para el desarrollo del presente proyecto será mediante procedimiento inductivo y experimental que permitirán la recolección de la información para hacer la estimación de tráfico y variables relacionadas entre los enlaces de la red, ver el comportamiento estadístico para definir los parámetros de QoS críticos en el diseño y evaluación.

Una vez determinados los parámetros críticos en la evaluación de la calidad de servicio de la red, se realizará la simulación de dicho esquema utilizando el paquete de software GNS3 que permite simular redes complejas.

Con la herramienta D-ITG se inyectará tráfico de Voz, Datos y Streaming en la red emulada dependiendo del protocolo de la capa de transporte (TCP o UDP).

Los escenarios de prueba son implementados de la siguiente manera: Primero la red VPN MPLS sin mecanismos de QoS y segundo la red VPN MPLS con mecanismos de QoS, los cuáles serán comparados y analizados mediante los indicadores ó parámetros de QoS (Latencia, Jitter y Pérdida de paquetes).

CAPÍTULO 2

2 ESTADO DE ARTE

2.1 REDES PRIVADAS VIRTUALES (VPN)

2.1.1 INTRODUCCIÓN

Las redes privadas virtuales son redes que usan una infraestructura pública compartida, para poder simular una red dedicada (privada), las redes VPN generalmente pertenecen a una compañía que le permite acceder de forma segura a diferentes sedes interconectados con la infraestructura de un proveedor de servicios.

En si la red VPN es una red pública en un entorno privado y confidencial que permite que el usuario trabaje en una sede distante como si estuviera en una red local, una de las desventajas de estas redes es el ancho de banda insuficiente, mientras más usuarios hayan en la conexión VPN menos ancho de banda quedarán para usuarios individuales.

Muchos de los proveedores de internet proporcionan un ancho de banda garantizado con un gran aumento en el costo, adicionalmente el hecho de transmitir información por una red pública, los datos son vulnerables a intrusión con diferentes técnicas que aparecen en el mercado, adicionalmente la gestión de claves de acceso y autenticación es delicada y laboriosa. (Orozco Lara, 2014).

2.1.2 COMPONENTES DE UNA RED VPN

Los componentes básicos que tiene una red VPN son los siguientes(Fernández Muñoz, 2007):

- Cliente VPN
- Servidor VPN
- Túnel
- Conexión VPN
- Red pública de tránsito

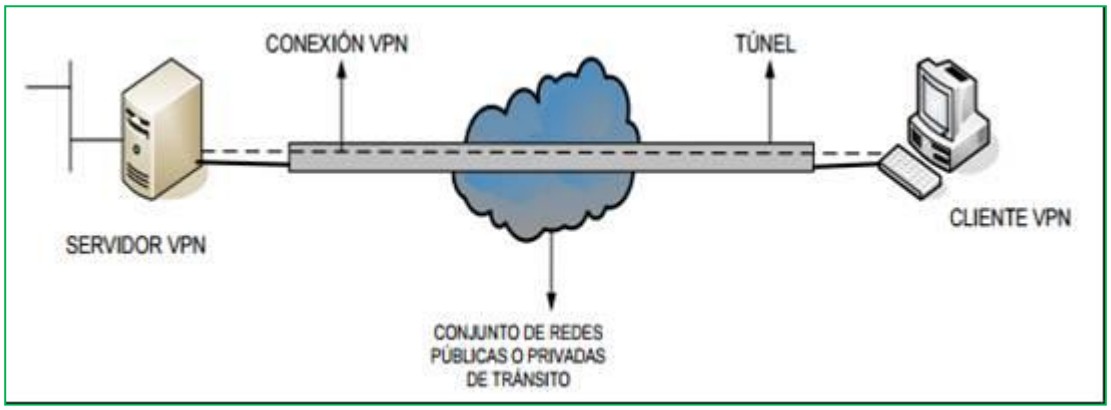


Figura 1: Componentes de una red VPN[1]

Cliente VPN Los clientes VPN pueden ser un enrutador que inicia la conexión VPN también conocido como enrutador de llamada.

Servidor VPN El servidor VPN es el enrutador que acepta las conexiones desde el cliente VPN, también conocido como enrutador de respuesta.

Túnel Se lo conoce a la parte de la conexión en la que se encapsula los datos, que no necesariamente deberán estar cifrados.

- Protocolos de túnel Son los protocolos utilizados para administrar los túneles y encapsular los datos privados, los mismos que deben estar cifrados para establecer una conexión VPN.
- Datos en túnel Son los datos que normalmente se envían a través de un vínculo punto a punto privado.

Conexión VPN Es la parte de la conexión donde se cifran los datos, para las conexiones VPN seguras, los datos se cifran y encapsulan en la misma parte de la conexión.

Red pública de tránsito Es la red compartida o privada que atraviesa los datos encapsulados.

[1] Figura tomada de Sandra Daniela Fernanda, Muñoz, Tesis Diseño de un canal Privado de comunicaciones entre dos puntos utilizando la infraestructura de Internet y Análisis del Canal VPN de la Universidad Politécnica Salesiana.

http://www.dspace.ups.edu.ec/bitstream/123456789/754/12/Tesis.pdf

2.1.3 REQUERIMIENTOS BÁSICOS DE UNA VPN

Una red VPN necesita los siguientes requerimientos (Fernández Muñoz, 2007):

- Identificación de usuario
- Cifrado de Datos
- Administración de Claves

Identificación de usuario Es donde una VPN debe verificar la identidad del usuario y restringir su acceso a personas no autorizadas.

Cifrado de Datos: Son los datos que se van a transmitir por una red pública deben ser cifrados para que no puedan ser leídos, teniendo varios estándares como son DES, 3 DES como se ve a continuación (Fernández Muñoz, 2007):

- DES: Es conocido como un estándar de cifrado de datos, que es un algoritmo de bloque que utiliza una clave de 56 bits para cifrar bloques de 64 bits, el mismo que está orientado a hardware.
- 3DES: Es conocido como Triple DES que es un estándar que utiliza dos claves y tres ejecuciones de algoritmo DES, con la ventaja de permitir a los usuarios descifrar datos de usuarios DES.

Administración de Claves Esta administración es para garantizar que la información sea segura, debido a que al usar la misma clave de cifrado a través de la red permite que sea vulnerable a un tercero y robar la información que es confidencial para una empresa (Fernández Muñoz, 2007).

2.2 TIPOS DE VPN

Entre los tipos de VPN que se encuentran están:

- Sistemas basados en Hardware
- Sistemas basados en Firewall
- Sistemas basados en Software

Sistemas basados en Hardware: Son aquellos routers que se encriptan y son seguros de usar ya que ofrecen gran rendimiento con un hardware dedicado, muy rápido y fácil de instalar (Trujillo Machado, 2006).

Entre las principales ventajas están:

- La capacidad de asegurar el flujo de paquetes entre dos redes, a través de una red púbica.
- La capacidad de autenticar y autorizar a los usuarios el acceso sobre redes privadas.

Sistemas basados en Firewall Estos sistemas se implementan con software de cortafuegos o llamado firewall con las siguientes ventajas (Trujillo Machado, 2006):

- Tiene mecanismos de seguridad que incluyen acceso restringido a la red interna.
- Realizan un NAT que es un traductor de direcciones para satisfacer los requerimientos de autenticación fuerte.
- Muchos de estos firewall comerciales aumentan la protección al retirar el sistema operativo.

Sistemas basados en software: Estos sistemas son útiles en situaciones en donde los 2 puntos de conexión no están controlados por la misma empresa u organización o cuando los firewall no están implementadas en la misma organización. Con este sistema permite un método más flexible en el manejo del tráfico, el mismo que puede ser enviado a través de un túnel en función de las direcciones o protocolos (Trujillo Machado, 2006).

2.3 TIPOS DE TOPOLOGÍAS VPN

Dentro de las topologías de las VPNs están las topologías Hub and Spoke, topología Full mesh y topología híbrida.

Topología Hub and Spoke: Es conocida como topología radial en el que el número de sitios remotos (Spokes) se conectan a un sitio central (Hub), los sitios remotos no tienen conectividad directa entre sí, como se puede observar en la figura (Cosios Castillo, 2004).

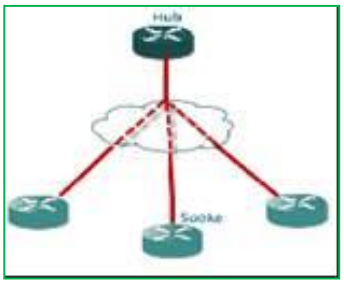


Figura 2: Topología Hub and Spoke[2]

Topología Fush Mesh: Es una topología completamente mallada que proporciona mucha redundancia permitiendo el intercambio constante de datos entre los sitios remotos, dependiendo de su necesidad la empresa puede utilizar una topología malla completa o malla parcial, por lo general las empresas usan malla parcial, la conectividad es a través de un circuito físico o virtual con cada uno de los otros nodos (González Morales, 2006) como se muestra en figura.

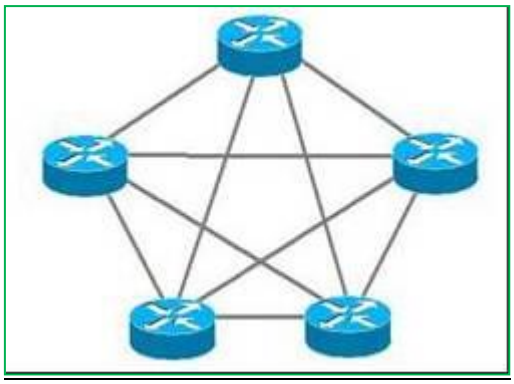


Figura 3: Topología Fush Mesh[3]

[2] Tomado: http://www.w7cloud.com/what-is-frame-relay-hub-and-spoke-topology/

[3] Tomado de Cisco Network Router Symbol Clipart

Topología Híbrida: Es cuando las redes VPN grandes combinan topología Hub and Spoke con topología malla parcial, como por ejemplo una empresa multinacional podría tener acceso a redes implementadas en cada país con una topología radial, mientras que la red principal internacional estaría implementada con una topología malla parcial (González Morales, 2006).

2.4 ARQUITECTURAS DE LA VPN

Dentro de las redes privadas virtuales existen varios tipos, las más comunes son:

- VPN de Acceso Remoto
- VPN Sitio a Sitio
- VPN Interna

VPN de Acceso Remoto: Este modelo es el más usado donde acceden los usuarios con la empresa desde sitios remotos utilizando como medio el servicio internet (Humans, 2013).

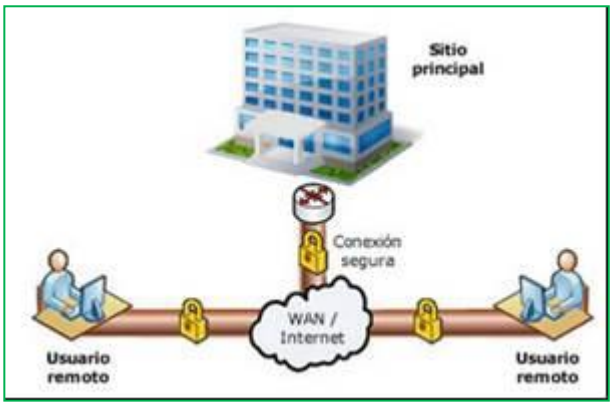


Figura 4: VPN de Acceso[4]

[4] Referencia de la empresa tecnología net-Humans

https://www.nethumans.com/solutions/itSecurity/VPN.aspx

VPN Sitio a Sitio: Este modelo permite acceder a oficinas o sucursales remotas con la sede principal, utilizando como medio el servicio de internet (Humans, 2013).

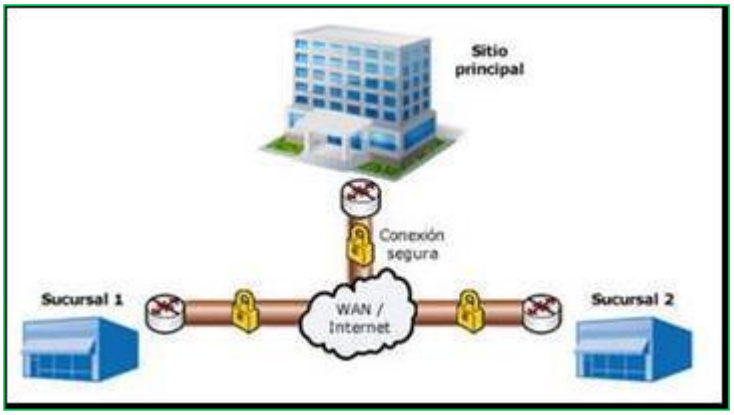


Figura 5: VPN Sitio a Sitio[5]

VPN Interna: Es semejante al de Acceso remoto con la diferencia de que se establece redes privadas virtuales dentro de una misma red local, es un modelo muy útil y potente que ayuda aumentar la seguridad de acceso inalámbrico (Humans, 2013).

2.5 TECNOLOGÍAS VPN

Las tecnologías VPN hacen referencia al modelo OSI, se pueden crear VPN usando tecnologías de Tunneling de capa 2 (Enlace de Datos) y de capa 3 (Red).

VPN capa 2: Es la tecnología de tunneling, donde se establece un túnel VPN que permite mayor seguridad de las sedes remotas con la sede principal, el tunneling consiste en abrir conexiones entre dos máquinas con un protocolo seguro SSH (Secure Shell), la información estará cifrada bajo este protocolo y se descifra con este protocolo en el destino, permitiendo una transmisión segura (Humans, 2013).

[5] (Humans, 2013)

Las tecnologías de Tunneling son: (Trujillo Machado, 2006)

- DSLW (Data Link Switching)
- IPX for Novell Netware over IP
- ATMP (Ascend Tunnel Management Protocol)
- Mobile IP (For mobile users)
- PPTP (Point-to-Point Tunneling Protocol)
- L2F (Layer 2 Forwarding)
- L2TP (Layer 2 Tunneling Protocol)

VPN capa 3 Es la tecnología tunneling que transmiten paquetes. Dentro de los protocolos de tunneling tenemos los siguientes:

- GRE (Generic Routing Encapsulation): Es donde se puede encapsular un protocolo de red con otros protocolos de red (Chiqui Guachiullca, 2015).
- IPSec (Internet Protocol Security Tunnel Mode): Es un conjunto de sistemas de seguridad de datos en redes IP, incluye protocolos como cabecera de autenticación (AH), carga de seguridad encapsulada (ESP) e internet key Exchange (IKE) (Chiqui Guachiullca, 2015).

Tanto GRE e IPSec se utilizan para servicios VPN de línea privada.

2.6 PROTOCOLOS USADOS EN LAS REDES VPN

Dentro de las redes privadas virtuales existen varios protocolos, entre los principales tenemos:

PPTP: Point-to-Point Tunneling Protocol, que fue desarrollado por un grupo de ingenieros de Ascend Communcations: U.S. Robotics, 3Com Corporation, Microsoft y ECI Telematics, este protocolo permite el intercambio seguro de datos de un cliente a un servidor formando una Red Privada Virtual (VPN) basado en una red de trabajo vía TCP/IP (Alvarez Gonzaga).

IPSec: Protocolo de seguridad de internet que permite varios servicios de seguridad para el protocolo de internet (IP) tanto para IPv4 como para IPv6, este protocolo fue diseñado para soportar dos modos de cifrado.

El modo de transporte que protege sólo la parte de carga útil de cada paquete, y el modo de túnel que es el más seguro ya que protege la identidad del remitente y del receptor así como oculta otros campos de IP, para que funcione IPSec, todos los dispositivos deben compartir una clave común (Menéndez Avila, 2012).

L2TP: Llamado también Layer 2 Tunneling Protocol, es un protocolo de estándar aprobado por el IETF, creado para corregir las deficiencias de los protocolos PPTP y L2F, utiliza PPP para proporcionar acceso telefónico que puede ser dirigido a través de un túnel por Internet hasta un punto determinado, L2TP, es una variación de un protocolo de encapsulamiento IP que incluye mecanismos de autenticación PPP, PAP y CHAP (RFC 2661).

2.7 BENEFICIOS DE LA VPN

Reducción en Costos

Cuando una empresa está alejada geográficamente, se puede acceder de manera transparente y confidencial a sus sucursales y adicionalmente compartir accesorios como impresoras, scanner y demás, asegurando integridad, confidencialidad y seguridad de datos a través de la VPN que es la red privada dentro de una red pública, donde los usuarios ahorran costos por movilidad de personas o llamadas telefónicas (Menéndez Avila, 2012).

Alta Seguridad

Las redes VPN utilizan altos estándares de seguridad como 3 DES, utiliza protocolos como IPSec para manejo de túneles mediante software, emplea varios niveles de autenticación para el acceso a la red mediante llaves de acceso que validan la identidad del usuario (Menéndez Avila, 2012)

Escalabilidad

No es necesario realizar inversiones adicionales para añadir usuarios a la red, la provisión de servicios se realiza con dispositivos y equipos fácil de configurar y manejar, utiliza infraestructura de alto nivel que los

proveedores lo tienen, y no a través de un enlace físico que puede significar tiempo y dinero (Menéndez Avila, 2012).

Compatibilidad con tecnologías de banda ancha.

Las redes VPN tienen gran flexibilidad y reducción de costos al aprovechar infraestructura existente de banda ancha inalámbrica, TV cable o conexiones de alta velocidad del tipo ISDN o ADSL, es factible usar voz sobre IP permitiendo significativo ahorro en telefonía de larga distancia (Menéndez Avila, 2012).

Mayor Productividad

Se puede probar que se obtiene mayor productividad de los usuarios debido al mejor nivel de acceso, fomentando el teletrabajo con la respectiva reducción en las necesidades de espacio físico (Menéndez Avila, 2012).

2.8 REDES MULTIPROTOCOL LABEL SWITCHING (MPLS)

2.8.1 INTRODUCCIÓN

MPLS es una tecnología de alto rendimiento para transmitir paquetes que permite mayor escalabilidad, alto rendimiento de la capa de red, eficiencia, flexibilidad en transferir datos a través de cualquier combinación de tecnología de capa de enlace como ATM, Frame Relay, líneas dedicadas, LANS , brinda apoyo a todos los protocolos de nivel tres.

Las principales motivaciones para su desarrollo son la ingeniería de tráfico (diferentes funciones necesarias para planificar, diseñar, proyectar, dimensionar y supervisar redes en condiciones óptimas independiente del protocolo), la diferenciación de clase de servicio (QoS) y las redes privadas virtuales (Orozco Lara, 2014).

MPLS en la capa OSI está entre la capa 2 y la capa 3 como se muestra en la figura:

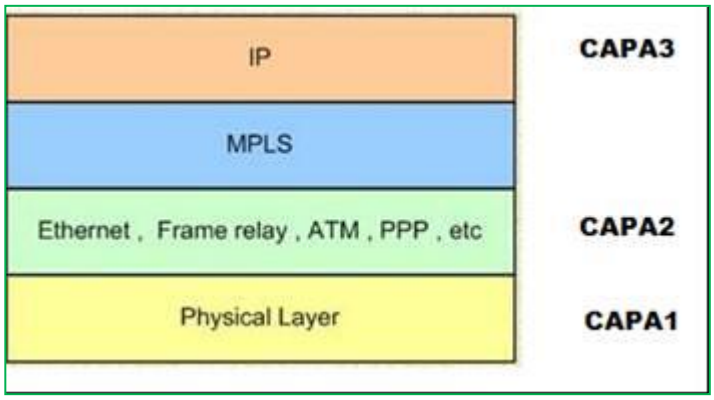


Figura 6: Capa de MPLS[6]

2.8.2 FUNCIONAMIENTO DE LA RED MPLS

La red MPLS trabaja cambiando las etiquetas de un paquete ya etiquetado, las etiquetas de MPLS se anuncian a todos los routers para construir un mapeo de etiquetas que están asociadas a los paquetes IP, para enviar los paquetes solo se envía mirando la etiqueta (label) en base a criterios de prioridad y/o calidad de servicio (QoS), ofreciendo servicios multiprotocolo sobre varias tecnologías (Orozco Lara, 2014).

Es decir en forma más detallada el objetivo de MPLS es separar la parte de encaminamiento de la parte de conmutación en el reenvío de los paquetes, de forma que mientras la parte de encaminamiento es compleja y lenta (tiempo de convergencia, cálculo de rutas) que se realiza independientemente, la parte de conmutación es rápida y simple (Orozco Lara, 2014).

En forma general, se puede decir que los router inicialmente calculan todas las rutas (usando protocolos de routing) a los destinos y luego intercambiando etiquetas se establecen los circuitos virtuales entre cualquier origen y cualquier destino para empezar a conmutar (Lab-MPLS).

[6] Fuente: Práctica de redes de comunicaciones:

http://arantxa.ii.uam.es/~apacheco/redesiii/pract3.html

Las etiquetas que se añaden solo tienen significado local al nodo MPLS (El router) y van cambiando salto a salto, de esta manera el paquete entra en la red (a través de los routers MPLS de frontera) y se le añade una etiqueta según el circuito virtual para su destino, el paquete es conmutado dentro de la red (a través de los routers MPLS internos) cambiando en cada salto la etiqueta y finalmente sale de la red MPLS (a través de los routers de frontera) próximo al destino quitándole la etiqueta (Lab-MPLS).

CABECERA DE UNA RED MPLS

Los campos de la cabecera MPLS son los siguientes: Etiqueta (Label), Exp, S, TTL (Orozco Lara, 2014).

Etiqueta: Este campo tiene 20 bits que se asigna a un prefijo de destino en un router y determina el próximo salto del paquete.

Exp: Bits para uso experimental, también aparece como QoS que identifica la clase de servicio.

S: Indicador de fondo de pila, es la primera etiqueta introducida.

Cuando S=0 Indica que hay más etiquetas añadidas al paquete.

Cuando S=1 Indica que se está en fondo de la pila de 1 bit.

Siendo una pila de etiquetas un conjunto ordenado de etiquetas.

TTL: Tiempo de vida del paquete, hay un decremento en cada enrutador permitiendo ser el contador del número de saltos (Orozco Lara, 2014).

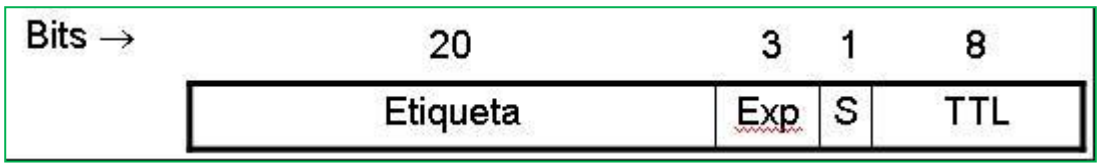


Figura 7: Cabecera de la red MPLS[7]

[7] (Orozco Lara, 2014)

Los paquetes MPLS son enviados después de una búsqueda por etiquetas en vez de una búsqueda dentro de una tabla IP (Orozco Lara, 2014).

2.8.3 ARQUITECTURA DE UNA RED MPLS

La red MPLS está formado por los bloques que son:

Plano de control: Es aquella que lleva las tareas destinadas a determinar la disponibilidad del acceso hacia una red destino, el plano de control contiene toda la información de direccionamiento de la capa 3, por ejemplo una función del plano de control es cuando se hace el intercambio de información por parte de dos protocolos de enrutamiento como OSPF y BGP, adicionalmente se encarga del valor que llevan las etiquetas (Orozco Lara, 2014).

Plano de Datos: Es aquella que está relacionada con el forwarding (envío de paquetes), los mismo que pueden ser paquetes IP o paquetes IP etiquetados (Orozco Lara, 2014).

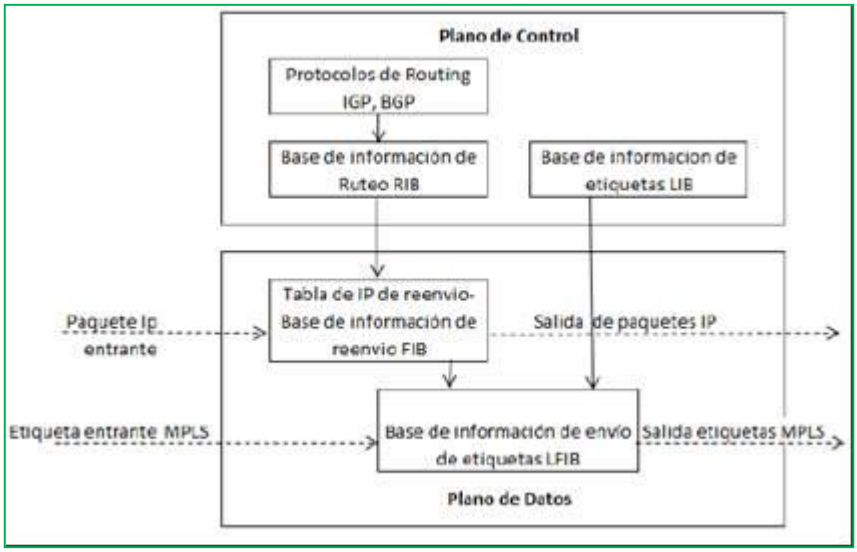


Figura 8: Bloques de la red MPLS[8]

[8] (Orozco Lara, 2014)

2.9 TÉRMINOS UTILIZADOS EN UNA RED MPLS

MPLS tiene los siguientes elementos:

LER: (Label Edge Enrutador) Es un enrutador que pone y quita etiquetas, que se encuentran en los extremos de la red MPLS (Orozco Lara, 2014).

LSR: (Label Switching Router) Es un enrutador de alta velocidad que conmuta etiquetas utilizando el protocolo de señalización de etiquetas adecuado, los mismos que se clasifican en base a la dirección del flujo de datos, como enrutadores ascendentes (upstream, origen) o descendente (downstream, destino) (Orozco Lara, 2014).

LSP: (Label Switched Path) Es el nombre de un camino MPLS para cierto tráfico, es similar a un canal virtual que puede ser punto a punto, punto a multipunto, multipunto a punto, multipunto a multipunto (Orozco Lara, 2014).

LDP: (Label Distribution Protocol) Es un protocolo para la distribución de etiquetas MPLS entre equipos de la red (Orozco Lara, 2014).

LIB: (Label Information Base) o TIB (Tag Information Base), es la tabla de etiquetas que manejan los LSR (Orozco Lara, 2014).

LFIB: (Label Forwarding Information Base) Es la tabla que asocia las etiquetas con los destinos o rutas de capa 3 y la interfaz de salida en el router, indicándole al router si tiene que poner o quitar etiquetas (Orozco Lara, 2014).

FEC: (Forwarding Equivalence Class) Es el nombre que se le da al tráfico que se encamina bajo una etiqueta (Orozco Lara, 2014)

PHP: (Penultimate Hop Popping) Es una alternativa de entrega de trama MPLS al final del circuito virtual que mejora las prestaciones y consumo de la CPU.

Consiste en quitar la etiqueta MPLS cuando se sabe que el siguiente router no necesita la etiqueta MPLS por estar directamente conectada a el o ser el final del circuito virtual (Orozco Lara, 2014).

Dominio MPLS: Es la porción de la red donde los procedimientos de enrutamiento y envío están acorde al protocolo MPLS (Orozco Lara, 2014).

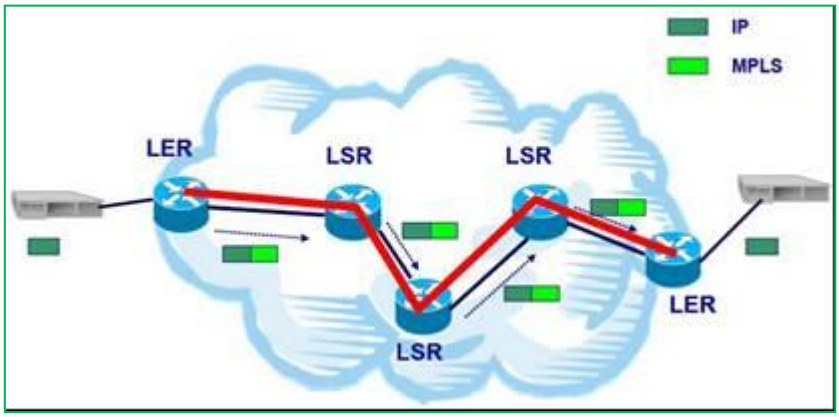


Figura 9: Componentes de la red MPLS[9]

2.10 OPERACIÓN DE UNA RED MPLS

La operación de MPLS involucra a los enrutadores de etiquetas (LER) realizando el proceso siguiente:

- LSR asigna etiquetas MPLS
- Se establece una sesión LDP o TDP de MPLS.
- Se realiza la distribución de etiquetas MPLS.
- Retención de etiquetas.

En forma detallada las redes MPLS usan al router LER para colocar una etiqueta simple a todos los paquetes que entran a la red, sea cual sea su procedencia (paquetes IP, paquetes Frame Relay, paquetes X-25, etc.), esta etiqueta contiene el destino dentro de la red MPLS y la ruta a través de la misma. En el interior de la red MPLS está el router de conmutación de alta velocidad LSR que examina la etiqueta colocada y enruta dichos paquetes al destino, lo cual hace que el proceso sea muy rápido.

[9] Tomado de Proyecto de innovación sobre fibras y redes Erandio Bizkaia: http://fibraoptica.blog.tartanga.net/

Al abandonar el paquete de la red MPLS la etiqueta es retirada por el router de borde LER y el paquete es entregado al destino con el formato original (Orozco Lara, 2014).

2.11 PROTOCOLOS DE DISTRIBUCIÓN DE ETIQUETAS

Es un conjunto de procedimientos y mensajes a través de los cuáles los router de conmutación de etiquetas LSRs pueden localizar a sus homólogos y establecer asociaciones (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

Los protocolos de distribución de etiquetas se pueden clasificar en:

Protocolos de enrutamiento implícitos: Que son aquellos que permiten el establecimiento de LSPs pero no ofrece ingeniería de tráfico por ejemplo:

- Label Distribution Protocol (LDP).
- Border Gateway Protocol (BGP).
- Intermediate System to Intermediate System (IS-IS).

Protocolos de enrutamiento explícitos: Son aquellos que son idóneos para ofrecer ingeniería de tráfico y permitir la creación de túneles por ejemplo:

- Costraint-Based Routing LDP (CR-LDP).
- Resource Reservation Protocol – Traffic Engineering (RSVP-TE) (MPLS-UMBC).

2.11.1 PROTOCOLOS DE ENRUTAMIENTO IMPLÍCITO

Label Distribution Protocol (LDP)

Es un protocolo para la distribución de etiquetas hacia los LSRs, son usadas para mapear FECs (Forwarding Equivalence Class) a etiquetas, las cuáles a su vez crean LSPs.

Las sesiones LDP son establecidas entre LDP pares en la red MLS (No necesariamente adyacentes), algunas veces emplean OSPF o BGP.

Tipos de mensajes LDP:

- *Discovery message:* Son aquellos que anuncian y mantienen la presencia de un LSR en la red.
- *Session messages:* Son aquellos que establecen, mantinen y terminan la sesión entre LDP pares.
- *Advertisement message:* Son aquellos que crean, cambian y borran el mapeo de labels para las FECs,
- *Notification messages:* Son aquellos que proveen información de avisos y señalización de errores (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

Border Gateway Protocol (BGP)

BGP es un protocolo de borde que brinda gran escalabilidad a las redes MPLS, jugando un papel importante para la separación entre el plano de control y el plano de reenvío, este protocolo lleva la información de enrutamiento externo por ejemplo la información de enrutamiento de internet, es así que se utiliza para proporcionar servicios de internet y servicios L3 VPN BGP (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

El protocolo BGP se utiliza para llevar la siguiente información:

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

BGP permite que las diferentes partes de la cadena transmitan únicamente la información requerida para llevar a cabo su función específica, por ejemplo: La información VPN se entregará sólo a routers LERs que tienen conocimiento de las redes privadas virtuales y no a todos los routers de borde.

El túnel MPLS es un mecanismo que permite a los enrutadores LSRs el envío de paquetes utilizando etiquetas sin tener que buscar sus destinos en la tabla de enrutamiento IP (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

Intermediate System to Intermediate System (IS-IS)

Es un protocolo desarrollado por la Digital Equipment Corporation y estandarizado por la ISO en 1992 como ISO 10589 que permite la comunicación entre dispositivos de red que son llamados los sistemas intermedios por la ISO, el objetivo de este protocolo es hacer posible el encaminamiento de datagramas usando ISO (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

Este protocolo se desarrolló en paralelo a un protocolo similar que es OSPF y se extiendo más adelante al encaminamiento de datagramas usando protocolo IP, esta versión se la llamo IS-IS integrado.

Una de las ventajas de OSPF es su rápida convergencia y escalabilidad en redes mucho mayores, donde cada router posee una imagen completa y sincronizada de la red con la característica que moderan el tráfico, mientras que IS-IS converge rápidamente y es muy escalable, flexible (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

Dentro de las características de IS-IS están:

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

2.11.2 PROTOCOLOS DE ENRUTAMIENTO EXPLICITO

Constraint Based Routing LDP (CR-LDP)

Es un protocolo de distribución de etiquetas basado en restricciones, es una extensión del LDP que se basa en el cálculo de trayectos que están sujetas a ciertas restricciones como ancho de banda, requisitos de calidad de servicio, retardo (delay), variación de demora (jitter), entre otras que se asocian al trayecto que define el operador de la red (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

Es una herramienta útil que sirve para controlar el dimensionado del tráfico y la calidad de servicio (QoS) en la red que se ofrece a los clientes y/o usuarios.

Con Constraint Routing se puede seleccionar la trayectoria más larga (en términos de costo), pero con menos carga de tráfico se puede usar un enrutamiento convencional. (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

Resource Reservation Protocol-Traffic Engineering (RSVP-TE)

Es un protocolo de señalización para reserva de recursos, para tener una sesión con mayor flexibilidad se combina MPLS y RSVP. El protocolo RSVP requiere que el dominio MPLS soporte enrutamiento explicito para facilitar la gestión de tráfico.

El protocolo RSVP-TE es una extensión del protocolo RSVP que fue diseñado para la distribución de etiquetas sobre MPLS, permite la creación de rutas explícitas con reserva o sin reserva de recursos, este protocolo permite un re-enrutamiento de los túneles LSP dando solución a caídas de red, congestión y cuellos de botella (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

2.12 VENTAJAS DE LA RED MPLS SOBRE OTRAS TECNOLOGÍAS

La arquitectura MPLS soporta diferentes aplicaciones (España, 2008) como:

- Calidad de Servicio “QoS”
- Ingeniería de tráfico.
- Redes privadas virtuales.
- Soporte Multiprotocolo.

Esta arquitectura permite una tecnología abierta apta para que soporte otras tecnologías, entre las principales ventajas de MPLS son:

Ahorro de coste: Dependiendo de la combinación de aplicaciones y configuración de la red, las redes basadas en MPLS pueden reducir costes entre un 10 y 25% frente a otras tecnologías como Frame Relay o ATM (España, 2008).

Rendimiento Mejorado: Por la naturaleza de la tecnología MPLS, se reduce enormemente el número de saltos entre puntos, lo que se traduce directamente en una mejora de tiempos de respuesta y rendimiento de la red

Soporte de QoS: Es uno de los principales beneficios de la red MPLS, es la capacidad de aplicar calidad de servicio mediante priorización de tráfico en tiempo real, siendo una prestación clave cuando se introduce voz y video en las redes de datos (España, 2008).

Recuperación entre desastres: Esta tecnología permite mayor flexibilidad y facilidad en reconexiones, por ejemplo en caso de obtener un backup.

Preparación para el futuro: MPLS representa el camino del futuro, una de las principales ventajas son los servicios basados en MPLS (España, 2008).

Nivel 3	Border Gateway Protocol (BGP)/VPN MPLS basado en RFC2547
Nivel 2	Ethernet: Servicios de LAN Privada Virtual (VPLS): Transport-MPLS (T-MPLS): Provider Backbone Transport (PBT). ATM / Frame: Emulación Pseudowire de extremo a extremo
Nivel 1	Generalized MPLS (GMPLS)

Tabla 1: Servicios basados en MPLS[10]

[10] Tomado de (España, 2008)

2.13 REDES PRIVADAS VIRTUALES BASADOS EN LA TECNOLOGÍA MULTIPROTOCOL LABEL SWITCHING

2.13.1 INTRODUCCIÓN

Las Redes privadas virtuales basados en la tecnología Multiprotocol Label switching (VPN MPLS) es una familia de métodos para aprovechar el poder de MPLS y crear redes privadas virtuales eficientes, fiables, escalables para la interconexión de las distintas sedes de una empresa en diferentes localizaciones, estableciendo una plataforma WAN completamente gestionada y con un bajo costo al no tener que comprar un circuito Frame Relay o ATM o arriendo de una línea para que una empresa siga creciendo (Onestopclick, 2015)

2.13.2 ARQUITECTURA VPN MPLS

Existen dos tipos de VPN que pueden ser implementadas a través de MPLS:

- VPN MPLS de capa 2 (MPLS L2 VPN)
- VPN MPLS de capa 3 (MPLS L3 VPN)

MPLS VPN LAYER 2

La tecnología MPLS VPN Layer 2 se usa para proporcionar VPN's encapsulando la trama completa VPN no los paquetes de capa 3 con el uso de las etiquetas MPLS.

Las MPLS VPN L2 son usadas para enviar tramas a través del backbone MPLS, Las mismas que son implementadas en escenarios punto a punto y soportan una propagación transparente del protocolo de capa 2, como pueden ser: ATM, Frame Relay, HDLC y Ethernet.

Conexiones multipunto de capa 2 pueden ser establecidas para crear VLAN a través de backbone MPLS.

A continuación se muestra el Backbone MPLS de capa 2 (Morales Santiago, Gilberto Nuñez Trejo, Jonathan Patiño Toribio, Pedro Porras Flores, Benjamin Alejandro, Presbitero Pacheco, 2007).

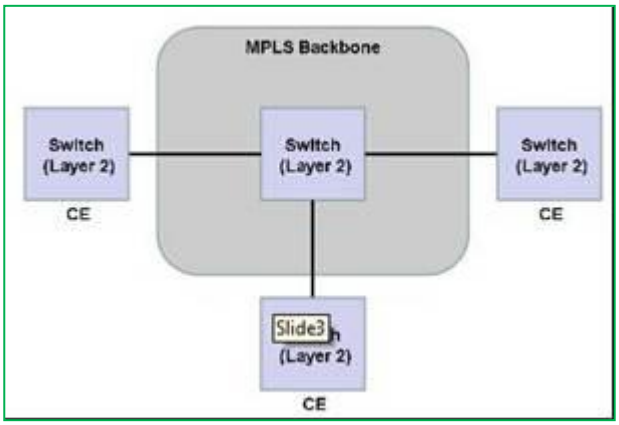


Figura 10: MPLS VPN Layer 2[11]

MPLS VPN LAYER 3

La tecnología MPLS VPN de capa 3 provee la funcionalidad de VPN Multipunto con el direccionamiento directo entre dispositivos del cliente y equipos del proveedor. La privacidad es implementada usando las tablas de ruteo para cada VPN que evita que diferentes VPN puedan comunicarse entre sí.

MPLS VPN de capa 3 provee un óptimo envío dentro del backbone MPLS. Las VPN tradicionales requieren una conectividad Fush Mesh para proporcionar el mismo servicio. MPLS VPN de capa 3 proporciona soporte para IPV4, los equipos del cliente (CE) pueden usar algún protocolo de ruteo o usar un ruteo estático para intercambiar información con el equipo del proveedor (PE) (Morales Santiago, Gilberto Nuñez Trejo, Jonathan Patiño Toribio, Pedro Porras Flores, Benjamin Alejandro, Presbitero Pacheco, 2007).

Multiprotocol BGP es usado dentro del Backbone MPLS para transportar información de ruteo de las VPN's de los clientes a lo largo de la red (Morales Santiago, Gilberto Nuñez Trejo, Jonathan Patiño Toribio, Pedro Porras Flores, Benjamin Alejandro, Presbitero Pacheco, 2007)

[11] Tomado de: http://blog.globalknowledge.com/technology/cisco/routing-switching/mpls-part-12/

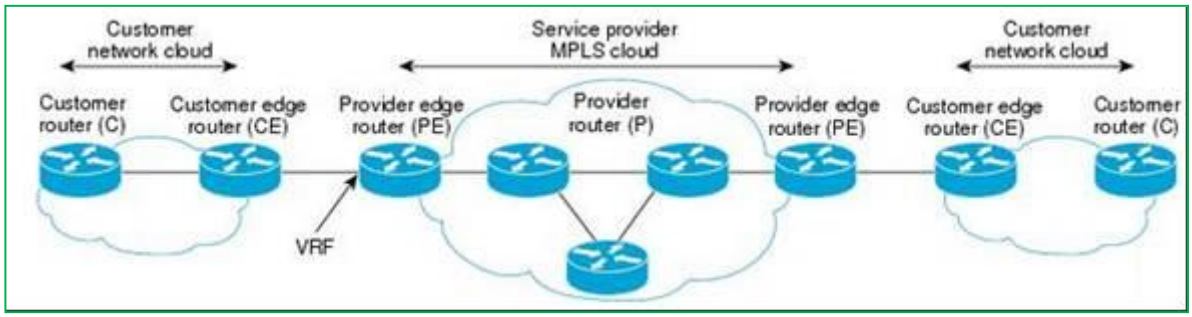


Figura 11: MPLS VPN Layer 3[12]

Para explicar más detalladamente la arquitectura de la red VPN MPLS Layer 3 se utilizará un caso de estudio de Cisco que tiene una empresa proveedora de servicios VPN llamada InterCom con dos puntos de presencia (POP), uno en Arequipa y otro en Chiclayo, los mismos que están enlazados por un router en Lima (Menéndez Avila, 2012).

CASO DEL ESTUDIO

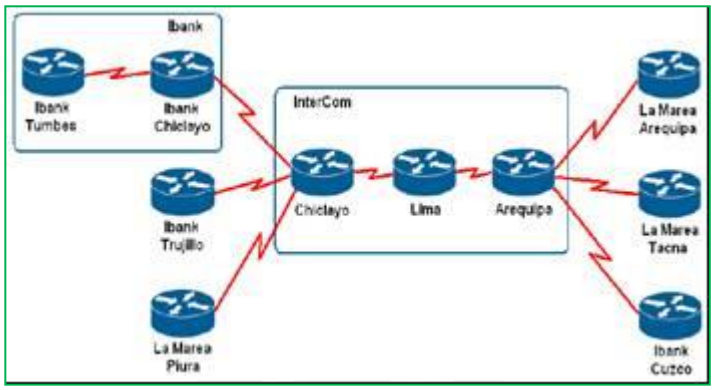


Figura 12: Red de InterCom y sus clientes[13]

La descripción de la red es:

- PE: Los routers de Arequipa y Chiclayo.
- P: El router de Lima.
- CE: Los router Ibank Chiclayo, Cuzco y Trujillo,

[12] Fuente: http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/L3VPNCon.html

[13] Tomado : http://www.ciscopress.com/articles/article.asp?p=28259

- Marea Arequipa, Tacna y Cuzco serán los router CE (Customer Edge)
- El router de la oficina Ibank en Tumbes será el router C (Customer).
- El proveedor será InterCom (Menéndez Avila, 2012).

Enrutamiento VPN y Tablas de Reenvió

Los clientes pueden usar direcciones IP privadas en sus redes lo que podría generar problemas al implementar VPN peer to peer.
Las redes VPN MPLS fue la solución dando a cada VPN su propia tabla de enrutamiento y reenvío en el router, creándose de esta forma routers virtuales en un router físico.

Estos routers virtuales permiten que el cliente utilice direcciones privadas o públicas, las direcciones deben ser únicas dentro de la VPN.
La combinación de la tabla de enrutamiento VPN IP con la tabla de reenvío VPN IP asociada se llama *Virtual Routing and Forwarding* ó *VPN Routing. and Forwarding (VRF)*. Para el caso de estudio tiene 3 VRF (Menéndez Avila, 2012)

Router targets

El router targets es una forma para saber que ruta se inserta en cada VRF, cada ruta VPN es etiquetada con uno o más router targets cuando es exportado a una VRF para ser ofrecidas a otras VRFs. (Menéndez Avila, 2012)

Propagación de Rutas en la Red del Proveedor

Para realizar el intercambio de rutas VPN entre routers PE se lo realiza de dos formas diferentes:

- Los routers PE ejecutan un protocolo de enrutamiento para cada VPN (OSPF ó EIGRP) que es ideal en redes pequeñas que sean menores de 100VPN.
- Los routers PE ejecutan un protocolo de enrutamiento para intercambiar todos los prefijos VPN.

Para redes MPLS-VPN se usa el segundo método, donde a las subredes que los router CE anuncian a los router PE se les agrega un prefijo de 64 bits llamado *route distinguisher.*

El resultado es una dirección de 96 bits que se intercambia dentro de la red a través de una extensión del protocolo BGP denominado Multi Protocolo BGP (MP-BGP) (Menéndez Avila, 2012).

Multi Protocol BGP (MP-BGP)

Este protocolo permite anunciar rutas VPN de clientes entre los routers PE, que aprendieron de los routers CE directamente conectados. Estas rutas pueden ser aprendidas con protocolos como BGP-4, RIP v2, rutas estáticas, OSPF. MP-BGP hay que considerar que es necesario únicamente en el backbone del proveedor (Menéndez Avila, 2012).

Entre las razones para escoger el protocolo BGP están:

- BGP es el único protocolo de enrutamiento que soporta un gran número de rutas.
- BGP, EIGRP, IS-IS son los únicos protocolos de enrutamiento diseñados para ser multiprotocolo (Llevar información de diferentes familias de direcciones), los protocolos IS-IS y EIGRP no son tan escalables como el protocolo BGP.
- BGP puede llevar información adjunta a una ruta como atributo adicional.

La redistribución en MP-BGP no es automática, se configura manualmente en cada router de la VRF (Menéndez Avila, 2012).

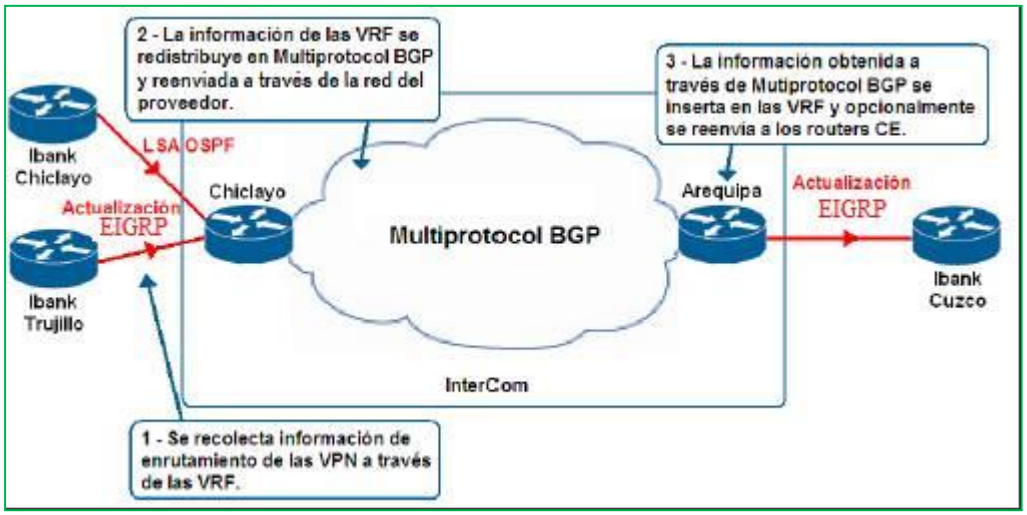


Figura 13: Protocolo de Enrutamiento en la Red de InterCom y sus clientes[14]

Reenvío de Paquetes VPN

Las direcciones IP usadas dentro de una VPN se les agrega un route distinguisher para que sean únicas, igualmente los paquetes originados en la VPN que se envían por la red backbone se les agrega información que sea reconocida por los router (Menéndez Avila, 2012).

Cada paquete VPN es etiquetado en el router PE de ingreso con una etiqueta que solo puede ser identificada por el router PE de salida y se envía dentro de la red. Los demás routers cambian las etiquetas sin tomar en cuenta el contenido del paquete.

Se examina la VRF cuando el paquete VPN llega al router PE de ingreso y busca la etiqueta asociada con la dirección del router PE de salida. Todos los router P envían el paquete basándose únicamente en la primera etiqueta, no analizan la segunda etiqueta por lo que se desconoce que se trata de un paquete VPN (Menéndez Avila, 2012).

El router PE de salida remueve la primera etiqueta y analiza la segunda donde identifica la VRF y algunas veces a la interfaz de salida en el router PE (Menéndez Avila, 2012).

[14] Tomado : http//:www.ciscopress.com/articles/article.asp?p=28259

2.14 TOPOLOGÍAS VPN MPLS

Se tiene varios tipos de VPN basados en la arquitectura MPLS, son varias topologías VPN que se pueden crear con la configuración VRF's, entre las principales tenemos: VPN Full mesh, Hub and spoke, VPN traslapadas y VPN centralizada (Hernández, 2008).

VPN full mesh: Es una topología donde todos los sitios tienen conexión directa con los demás a través de una red común, siendo la más sencilla de implementar, aquí todas las VRF's que se utilicen en esa topología se configuran con las mismas rutas de destino tanto importación como exportación, el ruteo es óptimo dentro del backbone (Hernández, 2008).

Topología hub and spoke: En esta topología los sitios solo se pueden comunicar con el Hub que es el punto de tránsito (Hernández, 2008).

VPN Traslapadas: En esta topología un sitio puede pertenecer a múltiples VPN's, se utiliza esta topología para implementar una Extranet o servicios centrales, aquí se necesita una dirección IP única entre las VPNs traslapadas (Hernández, 2008).

VPN Centralizada: En esta topología la conectividad IP de las VPNs centralizadas debe comunicarse con cualquier enrutador CE pero los enrutadores CE no se pueden comunicar entre sí (Hernández, 2008).

2.15 ESTRUCTURA DE LA VPN MPLS

La estructura básica de una red VPN MPLS es la siguiente:

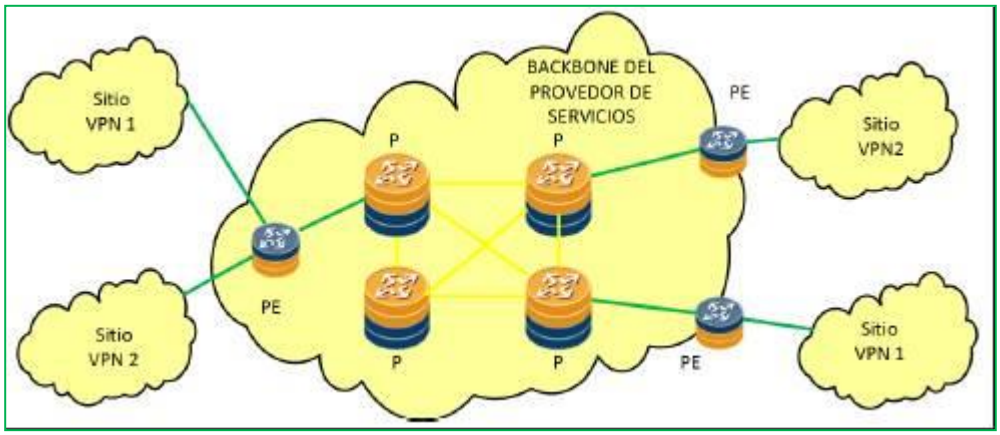


Figura 14: Estructura de la VPN MPLS[15]

Este modelo consta de las siguientes partes:

Cliente Edge (CE): Es un dispositivo de borde en una red cliente el mismo que puede ser un router, un switch o un host teniendo una o más interfaces conectadas a un proveedor de servicios.

Un CE puede acceder a varios PEs desde el mismo o desde un diferente proveedor de servicio (Chiqui Guachiullca, 2015).

Proveedor Edge (PE): Es un dispositivo de borde en la red del proveedor de servicios. Se encuentra conectado directamente al CE donde se realiza el procesamiento de la VPN, dando mayores prioridades para los PEs, hay que tomar en cuenta que un PE puede proporcionar el servicio de acceso para múltiples CEs (Chiqui Guachiullca, 2015).

[15] Tomado de (Chiqui Guachiullca, 2015)

Proveedor (P): Es un dispositivo de Core en un Proveedor de servicios, no están directamente conectados a los CE y no mantiene la información VPN. Tanto los PE's y P's son gestionados por el proveedor de servicios, mientras que los CEs son gestionados por los usuarios, a menos que los usuarios brinden el derecho de gestión al SP (Chiqui Guachiullca, 2015).

2.16 BENEFICIOS DE LA IMPLEMENTACIÓN VPN MPLS

Dentro de los beneficios o Ventajas de las VPN MPLS están:

- La escalabilidad.
- La seguridad.
- La facilidad de aprovisionar.
- Un direccionamiento de cliente flexible.
- Esta basado en estándares.
- Tiene servicios con prioridades de extremo a extremo.
- La consolidación.
- La ingeniería de tráfico.
- Un servicio centralizado (Rodríguez, 2008).

Escalabilidad: El protocolo MPLS se lo diseño para dar soluciones altamente escalables permitiendo gran cantidad de VPNs sobre una misma red, el modelo de vecindad (peer model) permite agregar un nuevo CPE de forma sencilla con un router PE (Rodríguez, 2008).

Seguridad: Las VPNs MPLS tienen el mismo nivel de seguridad que las VPNs orientadas a conexión, los datos de las VPN_A no ingresan a una VPN_B ya que la seguridad es provista en el borde del proveedor, el tráfico VPN se mantiene separado por medio de los niveles de etiquetas (Rodríguez, 2008).

Fácil aprovisionar: Las redes VPN MPLS no necesitan mapeo de conexión punto a punto, por lo que se puede agregar a un sitio múltiples VPNs maximizando la flexibilidad para construir intranet y extranets (Rodríguez, 2008).

Direccionamiento Flexible: Las VPNs MPLS permite a los clientes conservar sus direcciones sin necesidad de utilizar NAT, solo lo requerirán en caso de que dos VPNs con solapamiento de direcciones deseen interconectarse, esta característica de las VPN MPLS permite que los clientes empleen las direcciones privadas y se comuniquen entre sí a través de una red pública (Rodríguez, 2008).

Basada en estándares: El protocolo MPLS se encuentra disponible para todos los fabricantes de equipo de comunicaciones, asegurando la interoperabilidad entre distintas marcas (Rodríguez, 2008).

Servicios con prioridad de extremo a extremo: Con los mecanismos de calidad de servicio presentes en la industria de extremo a extremo se garantiza compatibilidad con los SLA (Servicie level agreements) (Rodríguez, 2008).

Consolidación: Permite la consolidación de los tráficos de voz, datos y video permitiendo a los proveedores reducir los costos operativos y grandes inversiones (Rodríguez, 2008).

Ingeniería de tráfico: El empleo de ruteo con funcionalidad de reserva de recursos (RRR: Routing with Resource Reservation) con utilización de extensiones al protocolo RSVP que provee a los carriers máximo aprovechamiento de los recursos de la red, la funcionalidad de RRR permite a los operadores de red aplicar y forzar ruteo explicito, técnicas de ruteo convencional, rápida convergencia, mecanismos de protecciones para determinadas situaciones (Rodríguez, 2008).

Servicio centralizado: Como las VPNs MPLS son vistas como intranets privadas, es posible agregar nuevos servicios como Multicast, QoS, VoIP, Data Center (contenidos de almacenado), conectividad múltiple (Rodríguez, 2008).

Mecanismos de migración hacia MPLS: La migración de un cliente que posee otras tecnologías hacia el empleo de las VPNs MPLS para el desarrollo de su intranet o extranet resulta mínima, ya que el cliente no se ve involucrado en la necesidad de implementar MPLS en sus routers de borde (CE) y no necesita hacer ninguna modificación a su intranet. (Rodríguez, 2008).

2.17 SEGURIDAD EN LA RED

En las redes actuales uno de los problemas principales es la seguridad de la información, tomando en cuenta que la seguridad está asociada a la confiabilidad, integridad, autenticación y no repudio de los datos transmitidos.

Los elementos asociados pueden ser implementados por varios mecanismos que son de naturaleza criptográficos, la confidencialidad de los datos que se transmiten en una red se puede realizar con mecanismos de cifrado entre los elementos que lo componen, el mismo puede ser end – to – end o punto multipunto.

Los tipos de autenticación disponible dependerán del protocolo de seguridad utilizado.

Por ejemplos para VPN seguras están los protocolos:

- IPSec: Internet Security Protocol
- Transport Layer Security (TLS)
- Secure Socket Layer (SSL)
- Datagram Transport Layer Security (DTLS)
- Secure Socket Tunneling Protocol (SSTP)
- Microsoft P-P Encryption (MPPE)
- Secure Shell (SSH)

Gracias al surgimiento de nuevas tecnologías en el mundo de las redes se han abierto muchas posibilidades para el intercambio de la información

como es el aparecimiento de la tecnología criptográfica para mitigar la inseguridad existente y es así que a partir de la capa física del modelo OSI a la capa de aplicación la criptografía es el primer paso para proporcionar solución al intercambio de información segura (Ramiro, 2014).

2.17.1 SEGURIDAD EN LOS DATOS

2.17.1.1 SISTEMA CRIPTOGRÁFICO Y CRIPTO ANÁLISIS

Este sistema es una estructura que consiste en la aplicación de la criptografía para la seguridad en la transmisión de la información.

El sistema de cifrado es un conjunto de protocolos, procedimientos y algoritmos para implementar un sistema de codificación y decodificación utilizando tecnología criptográfica.

Con este sistema criptográfico la confidencialidad e integridad de la información se logra usando diferentes métodos como técnicas de cifrado, descifrado, funciones hash, firmas digitales y técnicas de gestión de claves.

A continuación se presenta el proceso de criptografía:

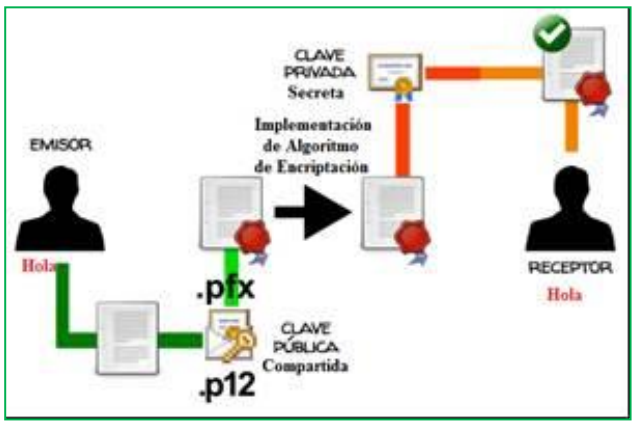


Figura 15: Proceso de Criptográfico[16]

[16] Tomado: https://www.google.com.ec/search?q=proceso+criptografico&espv=2&biw=1242&bih=581&source=lnms&tbm=isch&sa=X&ved=0ahUKEwiCw_vr_fLMAhXIqh4KHbbTAGEQ_AUIBigB#imgrc=VCnesxTZfj3hfM%3A

2.17.1.2 ALGORITMOS CRIPTOGRÁFICOS

Dentro de los algoritmos criptográficos están:

- ✓ Criptografía Simétrica o de clave privada: En este algoritmo utilizan la misma clave para el proceso de cifrar y descifrar un documento.

  Esta criptografía de clave simétrica se utiliza típicamente para el cifrado de los datos que proporcionan la confidencialidad.

- ✓ Criptografía Asimétrica o de clave pública: Se utilizan un par de dos claves, una clave para el cifrado y la otra clave para el proceso de descifrado.

  Esta criptografía de clave asimétrica se utiliza principalmente en el intercambio de claves y el no repudio proporcionando de este modo la confidencialidad y la autenticación.

- ✓ Función de dispersión (Hash): Se llama también algoritmo Hash donde se utiliza una función matemática para producir un valor hash único que es algorítmicamente aleatorio para identificar los datos uno de otro.

  Este algoritmo de hash (noncryptic) no proporciona confidencialidad, pero si proporciona la integridad del mensaje y la identidad de los puntos involucrados durante el transporte por canales de comunicación inseguros.

  Las funciones de dispersión unidireccionales (one-way hash function), se usan para la autenticación de datos y creación de firmas digitales.

  Una función de dispersión tiene las siguientes propiedades:

  - ✓ La función puede ser aplicada a un bloque de datos de cualquier tamaño.
  - ✓ La función produce una salida de longitud fija.
  - ✓ Para cualquier valor dado es relativamente fácil calcular su función.

- ✓ Con la función es imposible crear un mensaje a partir de un código, manteniéndose secreto el mensaje.

Las funciones de dispersión más importantes son MD5 y SHA-1 (González Morales, 2006)

MD-5 (Message Digest versión 5) es un algoritmo que autentica los datos de los paquetes, las versiones anteriores MD2, MD4, este algoritmo tiene un mensaje de longitud variable y produce un mensaje de 128bits que es usado por IPSec.

SHA-1 (Algoritmo de dispersión segura) este algoritmo se lo público en 1995, toma como entrada un mensaje de longitud máxima de 2^{64} bits y produce un resumen del mensaje hash de 160 bits, lPSec y los certificados utilizan ampliamente SHA-1 para la autenticación y firmas digitales.

- ✓ Firmas digitales: Son utilizadas con las claves públicas y se trata de un medio por el que los autores de un mensaje, archivo u otro tipo de información codificada digitalmente enlazan su identidad a la información, este proceso de firmar información digitalmente implica la transformación de la misma y de algunos datos secretos que guarda el remitente en una etiqueta denominada firma (Morales, 2006).

La firma digital es el equivalente electrónico de una firma manuscrita y tiene el mismo propósito, estas firmas no deben ser falsificables, los receptores deben ser capaces de verificarles y los firmantes no deben poder negarlas después, como se muestra en la figura:

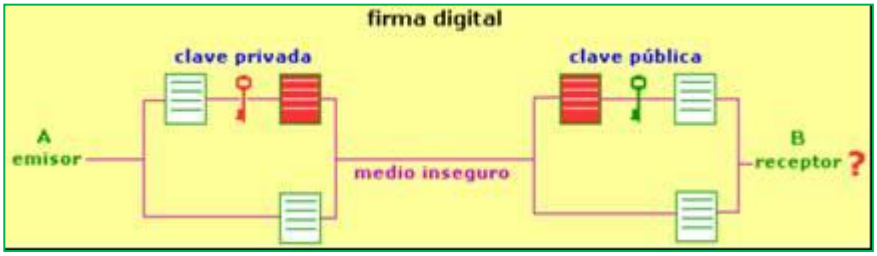


Figura 16: Firma digital[17]

[17] Tomado de https://www. (Morales, 2006)google.com.ec/search?q=firma+digital+creacion+y+validacion&biw=1242&bih=581&source=ln

2.18 SEGURIDAD EN LAS REDES MPLS VPN

Hay que considerar que cuando se habla de los servicios VPN la Autenticación, Autorización y Autoría (AAA) son importantes para que las diversas tecnologías VPN se adapten eficazmente al acceso de banda ancha (Catarina), a continuación se realizara una breve explicacion de los mismos.

Autenticación: Se conoce así cuando en una conexión VPN el usuario pide entrada a la red.

Autorización: Es importante que dentro de la VPN estén controlados con contraseñas para evitar problemas de spoofing, sniffing o usuarios maliciosos, aquí los usuarios piden permiso para realizar acciones específicas en diferentes secciones de la red (Catarina).

Autoría: El servicio VPN tiene un costo por lo que es importante que el cliente y el proveedor intercambien información de costos (Catarina).

Las redes MPLS VPN crea una ruta de datos privados a través de la red central proporcionando rutas de datos más seguros y más rápidos sin carga de red

Sin embargo estas redes MPLS VPN no profundiza en funciones de confidencialidad, datos criptográficos, por lo que estos datos podrían ser interceptados durante la transmisión sin conocimiento del emisor o del receptor.

Las redes MPLS/VPN no cumplen con los requisitos de confidencialidad y no repudio que muchos de los estándares de la industria lo requieren, la solución al mismo es usar el protocolo IPSec VPN que se puede implementar como una superposición a la red MPLS.

---

ms&tbm=isch&sa=X&ved=0ahUKEwisvNLM4PbMAhVKziYKHc_JDlsQ_AUIBigB#imgrc=dTqkBPz6dgxayM%3A

El protocolo IPSec actúa en la capa de red 3 el mismo que evita riesgos en la transmisión de información, a nivel de capa 4 que es la capa de transporte también existen otros protocolos como SSL, TLS y SSH que ayudan al usuario en los problemas de seguridad.

A continuación se hace una tabla comparativa de VPN MPLS e IPSec VPN

PARÁMETRO	MPLS VPN	IPSec VPN
Ubicación	Implementado en la red de CORE (reside en el ISP)	Implementado en el local loop, edge (borde) y fuera de la red (reside en la red del cliente)
Escalabilidad	Es altamente escalable, no se requiere conexiones sitio a sitio, apoya a decenas de miles de conexiones VPN a través de la misma red.	La escalabilidad es un desafio cuando es aplicada a gran escala. IPSec VPN requiere una cuidadosa planificación y coordinación para asignación y gestión de claves.
Equipamiento	Para permitir una conexión MPLS VPN se requiere de un solo aprovisionamiento de equipamiento (routers) a nivel de CE como de PE.	IPSec VPN utiliza el equipamiento de una red central IP ofreciendo servicios con reducción de gastos de operación centralizado a través de la misma infraestructura.
Despliegue	Se necesita de una red MPLS con capacidad de infraestructura tanto en el CORE como en el EDGE del proveedor.	No depende del proveedor y puede ser desplegado en cualquier red existente.

Autenticación	Las conexiones se autentican a través de las membrecías de VPN lógicas, basados en puerto lógico y el descriptor de ruta única	Las conexiones se autentican a través de certificados digitales o claves previamente compartidas.
Confidencialidad	Los circuitos lógicos punto a punto se separan proporcionando una sensación de seguridad y privacidad de los datos.	Set de cifrado estándar y mecanismo de túnel se utilizan en la capa de red IP para proteger los datos.
Calidad de Servicio QoS y SLA	Proporciona QoS y SLA con capacidades de ingeniería de tráfico robusto.	No trata directamente la QoS y SLA.

Tabla 2: Tabla comparativa de VPN MPLS e IPSecVPN [18]

[18] (Ramiro, 2014)

CAPÍTULO 3

3 CALIDAD DE SERVICIO QoS

3.1 INTRODUCCIÓN

En los últimos años ante el alto grado de difusión de las redes IP ha ido tomando gran importancia la convergencia de todos los servicios de telecomunicaciones surgiendo el internet que en un inicio no se necesitaba gran demanda de velocidad, ingeniería de tráfico, prioridades entre otros; solo se requería aplicaciones en las que solo importaba la información que iba en forma de paquetes y llegue a su destino de manera segura y fiable (Doménico Luna).

Las nuevas aplicaciones que aparecieron no requerían solamente que el tráfico llegue a su destino, sino que dependiendo de la aplicación se necesita un ancho de banda asegurado con un jitter mínimo, una probabilidad de pérdida determinada entre otros, que son parámetros que maneja la calidad de servicio, debido a que los protocolos de enrutamiento como RIP, OSPFv2, IS-IS no son capaces de detectar los picos de tráfico que se dan en las redes hay que tomar en cuenta que la gestión de colas no benefician a los tráficos sensibles a retados y su variabilidad (Doménico Luna).

Se conoce como calidad de servicio (QoS) a los efectos colectivos y/o globales de las prestaciones de uno o más servicios, aplicaciones diversas los que determinan el grado de satisfacción de un usuario con respecto al servicio o servicios contratados por una entidad (Doménico Luna).

3.2 PARÁMETROS DE QoS

La ITU-T define diferentes parámetros de calidad de servicio que son la base para definir los requerimientos de las distintas aplicaciones, 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 y/o evaluaciones de calidad de servicio (Doménico Luna).

- Retardo de transferencia de paquetes: Es el retardo o latencia que sufre un paquete IP cuando es transmitido entre dos puntos de referencia que pueden estar en la misma red o en puntos de extremo a extremo, la dependencia de este parámetro incluye el número de nodos, el protocolo de enrutamiento usado, el tráfico de la red, entre otros. (Doménico Luna).

  Los servicios que se transmiten en tiempo real y multimedia son sensibles a retardos, por lo que en aplicaciones como videoconferencia se necesita que este parámetro se reduzca al mínimo (Cevallos Romero, 2015).

- Ancho de Banda: Es un factor importante, ya que a medida que se aumenta el ancho de banda es posible transmitir más datos por unidad de tiempo lo que resulta muchas veces en incremento de costo ya que en ocasiones resulta imposible su ampliación sin que implique cambiar la tecnología de red. La reserva de ancho de banda debe garantizar la transmisión de cierta cantidad de datos en un tiempo determinado (Cevallos Romero, 2015).

- Varianza de retardo de los paquetes de información: Este parámetro se refiere al jitter o variación de retardo, difícilmente se le puede predecir es aleatorio y se lo obtiene de muestra en muestra, de este parámetro depende mucho para el funcionamiento de la red (Doménico Luna).

  Es producida por la congestión en la red, pérdida de paquetes de sincronización o por las diferentes rutas que los paquetes deben tomar para llegar a su destino. La principal desventaja de este efecto se presenta en las aplicaciones multimedia y en tiempo real como telefonía IP radio, puesto que hace que algunos paquetes lleguen demasiado rápido o tarde para entregarlos a tiempo (Cevallos Romero, 2015).

- Tasa de errores en los paquetes IP: (IPER) Este parámetro se refiere a los paquetes erróneos que se obtienen en una transmisión total de paquetes, las fuentes de error pueden ser desde la codificación en el transmisor o en la decodificación del receptor (Doménico Luna).

- Tasa de pérdida del paquete IP: (IPLR) Porcentaje de paquetes descartados de un total que han sido transmitidos, estás pérdidas se pueden dar por diversos motivos como congestión en las colas de los nodos, tiempo de vida (TTL en IPv4) o (HL en IPv6) (Doménico Luna).

Existen varios motivos para perder paquetes como colisiones, enlace saturado, pérdida del enlace entre otros (Cevallos Romero, 2015).
La ecuación está dada por:

P pérdidos= [(**P**tx-**P**rx)*100] / **P**tx[19]

A continuación se da un breve resumen de los parámetros de calidad se servicio.

Parámetro	Unidades	Significado
Ancho de Banda	Kb/s	Indica el caudal máximo que se puede transmitir
Retardo	ms	El tiempo medio que tardan en llegar los paquetes
Jitter	ms	La fluctuación que se puede producir en el retardo
Pérdida de paquetes	%	Proporción de paquetes pérdidos respecto de los enviados

Tabla 3: Parámetros de calidad de servicio[20]

[19] Tomado de (Cevallos Romero, 2015)

[20] Tomada de: José Antonio Rodríguez López, Diseño y Evaluación de Algoritmos para la selección de redes de comunicaciones móviles según la calidad de Servicio, Universidad (Cevallos Romero, 2015) Politécnica de Catalunya

3.3 REQUERIMIENTOS DE QoS

Los requerimientos de QoS están dependiendo del tipo de aplicación que se esté trabajando, a continuación se da una tabla de los requerimientos de calidad de servicio en ciertas aplicaciones (Cevallos Romero, 2015).

Aplicación	Pérdida de paquetes	Retardo	Jitter	Ancho de Banda
Correo electrónico	Baja	Alto	Alto	Bajo
Transferencia de ficheros	Baja	Alto	Alto	Medio
Acceso Web	Baja	Medio	Alto	Medio
Loggin remoto	Baja	Medio	Medio	Bajo
Audio bajo demanda	Media	Medio	Medio	Medio
Televisión	Media	Bajo	Medio	Alto
Telefonía	Media	Bajo	Bajo	Bajo
Videoconferencia	Media	Bajo	Bajo	Alto

Tabla 4: Requerimientos de calidad de servicio en ciertas aplicaciones[21]

3.4 MECANISMOS DE QoS

El modelo IntServ, Precedencia IP y Diffserv definen el uso de campos y un tratamiento básico de los paquetes dentro de la red, porque existen una variedad de colas, políticas, métricas y técnicas de catalogación de tráfico que pueden usarse para afectar y condicionar el tráfico. Dentro de los algoritmos que existen (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011) están:

[21] Tomado de (Cevallos Romero, 2015)

TRAFFIC POLICING*:* Que es un mecanismo que permite controlar la tasa de envío o recepción de una interfaz para los diferentes niveles de servicio que se tengan.

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

Los paquetes son medidos y se puede tomar diferentes acciones dependiendo si el paquete está de acuerdo o viola o excede la tasa promedio configurada para lo que se usa la ráfaga comprometida (commited burst Bc) y la ráfaga de exceso (excess burst Be) (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

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

Este método implementa funciones que permite limitar el tráfico entrante en un dispositivo, hace un análisis de los paquetes para realizar una adecuada clasificación de los mismos (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

El CAR se encarga de vigilar el ancho de banda de acceso a la red, con lo que asegura que el tráfico que se encuentra dentro de los parámetros sea enviado, y los que no cumplan sean descartados o transmitidos a una prioridad más baja. Dentro de las funciones de limitación del CAR están:

- Controlar la máxima tasa de tráfico enviado o recibido por una red.
- Realizar agregación o granulidad de capa 3 para limitar el ancho de banda de ingreso o egreso.
- El CAR se configura en los bordes de la red para limitar el tráfico entrante y saliente de la red.
- En su funcionamiento el CAR examina el tráfico recibido por un interfaz o un conjunto de criterios de selección de tráfico como la dirección IP, MAC, Precedencia, etc, después compara la tasa de

tráfico con lo configurado en token bucket y toma la acción basándose en el resultado (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

Token Bucket: Es la definición de tasa de transferencia que tiene la ecuación: (Committed information rate) CIR = Bc / Tc
CIR=> Tasa de información media comprometida (bps)
Bc => Committed Burst – Tamaño de la ráfaga
Tc =>Intervalo de tiempo en segundos para la ráfaga.

Cada token es un permiso para el envío de cierta cantidad de bits a la red, cuando es enviado un paquete el dispositivo regulador retira un número de tokens que representa el tamaño del paquete, de no existir el número adecuado de tokens se puede descartar el paquete (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).
Leaky Bucket: Este mecanismo permite regular el tráfico de un flujo a una determinada tasa de transmisión prefijada, pero no resulta ser eficiente si la tasa de los flujos son demasiados bajos.

CBWFQ: (Class Based Weighted Fair Queue)**,** este mecanismo se aplica sobre interfaces de salida de los routers, donde se divide todo el ancho de banda disponible entre las clases de servicio, asignando diferentes pesos a diferentes clases de servicio donde cada router puede manejar el buffer y el ancho de banda para cada clase de servicio (Cosios Castillo, 2004).

WRED: (Weighted Random Early Detection) Por medio de este mecanismo se descartan paquetes basados en la precedencia IP o el valor del campo experimental del paquete MPLS de las interfaces próximas al nivel de congestión para:

- Favorecer las clases de mayor prioridad en situaciones de carga de la red.
- Para no realizar un descarte sistemático de paquetes que por los mecanismos de retransmisión de TCP/IP llevarían a situaciones de mayor congestión (Cosios Castillo, 2004).

TRAFFIC SHAPPING: Este mecanismo permite controlar el tráfico que sale de una interfaz para controlar el flujo de manera que coincida con la velocidad de la interfaz remota, para asegurar que el tráfico este conforme a las políticas contratadas, eliminando así los cuellos de botella en topologías donde la tasa de transmisión sufre variaciones. Una de las razones que se lo utiliza es para controlar el acceso al ancho de banda disponible, regula el flujo de tráfico para prevenir la congestión previniendo la pérdida de paquetes (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

Generic Traffic Shaping (GTS): Este mecanismo permite realizar traffic shaping, reduciendo el flujo de tráfico de salida y previniendo un evento de congestión al restringir la tasa de bits de salida usando token bucket, se aplica a cada interfaz y puede usar listas de control de acceso para controlar el tráfico (Hidalgo Llumiquinga & Laguapillo Muñoz, 2011).

3.5 MODELOS DE CALIDAD DE SERVICIO

Durante la última década se ha realizado investigaciones con los modelos propuestos con la IETF, donde se han plasmado las características de cada uno de estos modelos, tratando de encontrar alguno que cumpla con todas las expectativas de QoS en redes IP, todavía no se ha logrado uno que sea totalmente aceptado.

La IETF ha propuesto modelos que ofrecen QoS en diferentes modalidades como el modelo IntServ que pretendía ampliar la arquitectura IP existente para soportar actividades en tiempo real, manteniendo el servicio Best-Effort que existía hasta el momento y el modelo Diffserv que es una de las propuestas más alentadoras para redes grandes como por ejemplo el Internet (Reyes, 2007)

3.5.1 MODELO BEST EFFORT

Este modelo es también conocido como QoS deficiente debido a que designa un tipo de servicio de red en el que la red no puede garantizar que los datos lleguen a su destino, ni ofrecer al usuario una determinada calidad de servicio en sus comunicaciones, está caracterizado por colas tipo FIFO

(First Input First Output) los que no presentan diferenciación entre flujos (Reyes, 2007).

En este tipo de redes todos los usuarios reciben el mejor servicio que se le pueda dar en ese momento, por lo que tendrá distintos anchos de banda y tiempos de respuesta de acuerdo al volumen de tráfico que tenga en la red. Para redes telemáticas de correo electrónico, páginas web, entre otros se provee una corrección de errores básica, pero no se garantiza entrega efectiva de datos (Alvarez, 2007).

3.5.2 MODELO INT-SERV

En este modelo el flujo se define como un tráfico continúo de datagramas relacionadas entre sí que se produce por una acción del usuario y que requiere una misma QoS, el flujo es unidireccional y definen tres tipos de servicio (Reyes, 2007):

Servicio Garantizado: Es aquel que garantiza un caudal mínimo con un retardo máximo, cada router que se encuentra en la red debe ofrecer las garantías solicitadas (Reyes, 2007).

Servicio de carga controlada: En este servicio se debe ofrecer una calidad comparable a la de una red poco cargada de datagramas, deben proporcionar un buen tiempo de respuesta, aunque eventualmente puede producir retardos grandes (Reyes, 2007).

Servicio de Mejor Esfuerzo: En este servicio no se tiene ninguna garantía, no ofrece QoS. Este modelo dispone de un protocolo RSVP (Resource Reservation Protocol) es decir un Protocolo de Reservación de Recursos, basándose en el mismo para señalizar y reservar la QoS deseada para cada flujo de datos en la red.

Int-Serv da a las aplicaciones un nivel garantizado de servicio, donde negocia parámetros de red de punto a punto. La aplicación solicita el nivel de servicio necesario basandose en la QoS para que se reserven los recursos de red antes de que la aplicación comience a operar, está reserva se encuentra activa hasta que la aplicación termine o el ancho de banda requerido sobrepase el límite deseado (Reyes, 2007).

3.6 COMPONENTES BÁSICOS

El control de admisión: Es aquel que comprueba si hay recursos suficientes para soportar el servicio pedido.
Clasificación de Paquetes: Es aquel que analiza los campos de dirección y puertos para determinar la clase a la que pertenece el paquete.
Planificador de paquete: Es aquel que aplica algoritmos de encolado que gestionan la transmisión de los paquetes por un enlace de salida (Reyes, 2007).
Protocolo RSVP: Se utiliza cuando la aplicación pide un determinado servicio a la red, este protocolo entrega la petición al control de tráfico de cada router comprobando si es viable o no (Reyes, 2007).

PROTOCOLO RSVP

Para implementar RSVP los routers deben incorporar cuatro elementos que son:
Control de Admisión: Donde se comprueba si la red tiene recursos suficientes para proveer la petición.

Política de Control: Es aquel que determina si el usuario tiene los permisos correctos para la petición realizada, que se lo puede hacer consultando una base de datos con el protocolo COPS (Política de servicio comúnmente abierto).

Clasificador de Paquetes: Es donde se clasifica los paquetes en categorías de acuerdo con la QoS a la que pertenece, cada categoría tendrá una cola y un espacio propio para buffer en el router.

Planificador de Paquetes: Es aquel que organiza el envío de los paquetes dentro de cada categoría (Reyes, 2007).

3.7 VENTAJAS Y DESVENTAJAS DE LOS INT-SERV

Ventajas (Reyes, 2007):

- Es la simplicidad conceptual que facilita la integración con la administración de las políticas de red.
- Arquitecturalmente QoS discreta por flujo es conveniente para el control de admisión de las llamadas de voz.

Desventajas (Reyes, 2007):

- Falta de escalabilidad: El costo de la implementación crece linealmente de acuerdo a la complejidad de la red.
- El protocolo RSVP esta orientado a conexión, lo que implica que los routers guardan información de los estados de los flujos activos que atraviesan por ellos.
- La información de los estados pueden ser aceptados, pero es complicado y costoso soportarlos en los routers del centro de la red porque soportan miles de conexiones activas.
- En las versiones actuales no hay implementados mecanismos de seguridad para evitar robos de servicios, ni políticas de control para autenticar, autorizar las aplicaciones y a los usuarios.
- No existe un protocolo que sirva para hallar una ruta que soporte QoS solicitado por el protocolo RSVP.
- Todos los elementos de la red deben mantener e intercambiar mensajes de estado y señalización por cada flujo, lo que puede requerir un ancho de banda significativo en redes grandes.
- Se utiliza mensajes para refresco periódicos lo que puede requerir protección frente a pérdida de paquetes para mantener la sesión inalterable.

3.8 MODELO DIFF-SERV

Este modelo es uno de los más alentadores para proporcionar QoS en redes grandes como el internet, añadiendo facilidad de implementación y bajo costo porque no hay necesidad de implementar grandes cambios en las estructuras de las redes actuales (Reyes, 2007).

Los Diff-Serv son un conjunto de tecnologías donde los proveedores de servicios de red pueden ofrecer distintos niveles de QoS para diferentes clientes y tráfico, sigue una estrategia que facilita la estabilidad y despliegue en las redes, ya que no se necesita que este implementado en todos los nodos.

La diferenciación de servicios se lleva a cabo mediante la definición de comportamientos específicos para cada clase de tráfico entre dispositivos de interconexión, lo que se conoce como PHB (Per Hop Behavior – Comportamiento por Salto) *que define cuánto tráfico le corresponde a un paquete en particular, se manejan mediante los valores del campo DSCP* (Punto de Codificación de Servicios Diferenciados).

El PHB especifica la prioridad de encaminamiento de paquetes en los routers teniendo los valores estándares que son BE (Best Efort-Mejor Esfuerzo), CS (Selector de clase), EF (Expedite Forwarding-Encaminamiento Expedito), AF (Assured Forwarding- Encaminamiento Asegurado).

3.8.1 CARACTERÍSTICAS DEL DIFF-SERV

En este modelo cada router debe analizar y dar tratamiento diferencial a cada uno de los paquetes que son enviados en la red y no necesita establecer ningún proceso de señalización por lo que ofrece mayor escalabilidad.

Diff-Serv permite ofrecer servicios de red basados en un conjunto de reglas de salto definidas en los routers que componen la red, que se pueden aplicar a flujos agregados de tráfico mediante la asignación del código DSCP (Reyes, 2007).

3.8.2 ELEMENTOS DE LA ARQUITECTURA DIFF-SERV

Clasificador: Cuya función es de guiar a los paquetes con características similares hacia los procedimientos de condicionamiento de tráfico y se los puede configurar por medio de un procedimiento de administración.

Medidor: Tiene la función de pasar su información hacia las funciones de acondicionamiento para determinar una acción en particular para cada paquete.

Marcador: Tiene la función de marcar los paquetes con un código DS para seleccionar un PHB dentro de un grupo de PHB's.
Acondicionador: Tiene la función de acondicionador poseendo un tamaño de cola finito, descartando el paquete cuando no existe suficiente espacio dentro de la cola.
Descartador: Tiene la función de descartar paquetes pertenecientes a un flujo de tráfico para evitar congestionamiento y cumplir con los requisitos del perfil del tráfico (Reyes, 2007).

3.8.3 VENTAJAS Y DESVENTAJAS DE LOS DIFF-SERV

Ventajas (Reyes, 2007):

- Escalabilidad: Proporciona soporte escalable para voz y datos sobre una misma infraestructura, adicionalmente mejora la complejidad de mantener información de estado de muchos circuitos virtuales.
- Funcionamiento: Permite que el contenido de los paquetes se inspeccione una vez para clasificarlo, en ese instante se marca el paquete y todas las decisiones de QoS se hacen de acuerdo al valor de un campo fijo de la cabecera, con lo que se reduce los requerimientos en el procesamiento.
- Flexibilidad: DiffServ define muchos tipos de tráfico.
- Sencillez de señalización: Es más sencillo que en el protocolo RSVP.
- Costo: Tiene costo de gestión reducidos.

La forma que maneja los campos de las cabeceras de los protocolos IPv4 e IPV6, hace que sea una de las mejores soluciones que se propone hoy en día en asignación de QoS (Reyes, 2007).

Desventajas :(Reyes, 2007)

- No se encuentra reservación de ancho de banda extremo a extremo, por lo que al no ser implementado correctamente los PHB's sobre los enlaces congestionados o no está correctamente diseñado para el volumen de tráfico esperado de una clase específica, las garantías de servicio pueden ser imparciales en los nodos de la red.

- Es la ausencia de control de admisión por flujo que hace posible que las aplicaciones se congestionen unas con otras (Reyes, 2007).

Una vez determinado las ventajas y desventajas de modelos Int-Serv y Diff-Serv se concluye que Diff-Serv ofrece ventajas como flexibilidad, escalabilidad, distinción de diferentes clases de servicio mediante marcado de paquetes entre otras, sobre lo que ofrece Int-Serv.

3.9 CALIDAD DE SERVICIO EN LAS REDES VPN MPLS

Es importante la calidad de servicio en una red porque permite controlar características de la red como es el ancho de banda, el jitter, el retardo, las pérdidas de paquetes entre otros. En la actualidad es un factor crítico a la hora de diseñar una red en una empresa o institución, de acuerdo a la aplicación a trabajar será necesario un criterio u otro para un determinado tipo de aplicación.

En la cabecera del paquete IP está el campo Type of Service (ToS) que es de 8 bits que indica la importancia del paquete, como se puede observar:

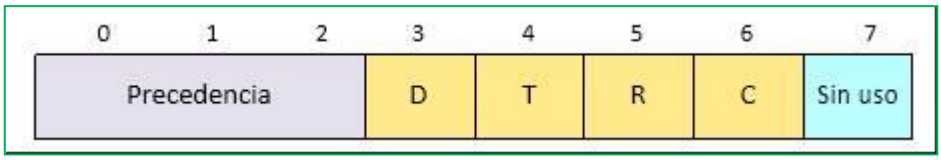


Figura 17: Estructura del campo ToS[22]

Las características del servicio los determinan los siguientes bits:
Los 3 primeros bits asignan la prioridad del datagrama IP (Precedence.)
Los bits D es el delay (Retardo)
Los bits T es el thoughput (Rendimiento)
Los bits R es el reability (Fiabilidad)
Los bits C es el cost (Costo)

[22] Tomado de Sandra Pupiales Backbone MPLS 3Play

3.9.1 CONFIGURACIÓN DE LAS CLASES DE TRÁFICO

En la red VPN MPLS se debe crear una clase de tráfico que consiste en agrupar un tipo de tráfico bajo un mismo dominio, para que los mismos puedan tener el mismo tratamiento.

Dependiendo al valor Precedence del paquete IP al ingreso de los router's LER's se clasifican en AF11, AF12, AF21 (Aplicaciones empresariales VIP), AF22 (Aplicaciones empresariales corporativos), AF31, AF32 como se muestra a continuación:

CLASES	DIFFSERV	TRAFICO	TIPO	EXP
Best Effort	AF11	Aplicaciones que no reciben ninguna garantía de QoS	ICMP	0
Bronce	AF12	Protocolos y aplicaciones para administrar la red.	SNMP, TELNET	1
Plata	AF21-AF22	Aplicaciones empresariales.	Bases de datos transacciones Web	2,3
Oro	AF31	Videoconferencia y Streaming	HTTP	4
Premium	AF32	VoIP	TCP, UDP	5

Tabla 5: Clasificación de tráfico en Servicios Diferenciados[23]

3.10 ARQUITECTURA DE VPN MPLS CON QoS

La arquitectura MPLS ofrece un circuito virtual o LSP, permitiendo un trato igualitario a los diferentes tráficos que se envían bajo un mismo túnel LSP bajo una etiqueta FEC en particular, estudios relacionados a la calidad

[23] Tomado de Sandra Narvaez Pupiales

de servicios en diferentes escenarios son de interés actual dado que a comparación con las demás arquitecturas VPN MPLS ofrece seguridad escalabilidad, simplicidad, velocidad entre otros. Las facilidades que ofrece esta arquitectura para la implementación de calidad de servicio son los que se dan a continuación (Doménico Luna):

Velocidad frente al esquema de enrutamiento IP: La conmutación de etiquetas es más rápida y eficiente ya que se produce en la capa de enlace. El envío o forwarding se hace en base a un campo específico de la cabecera de la tecnología de conmutación (Doménico Luna).

Procesamiento más rápido de la cabecera MPLS: Es debido a que MPLS solo necesita los campos Label, TTL para el envío de tráfico, el stacking para envío interdominio y el EXP para implementar prioridades (Doménico Luna).

Facilidad de implementación: La arquitectura MPLS requiere de poca señalización entre los nodos, cualquier cambio en cualquier capa de esta arquitectura se amolda a los cambios sin la intervención del administrador de la red MPLS (Doménico Luna).

Adaptabilidad frente a la capa de red como a la capa de enlace: La arquitectura MPLS está entre la capa de red y la de enlace, utiliza la capa superior inmediata e inferior, pero su funcionamiento no depende de ellas. MPLS se adapta perfectamente a las tecnologías de capa de enlace (ATM, Frame Relay, PPP, Familia Ethernet) como cualquier tecnología de la capa de red (IPv4, IPv6) (Doménico Luna).

El cambio se da en el software y no en el Hardware: Los nodos de la red MPLS solo necesitan los procesos, para equipos actuales solo necesitan actualización del sistema operativo de los routers que conforman el backbone (Doménico Luna).

Se acomoda a los modelos de calidad de servicio: Con el campo experimental EXP que cuenta con 3 bits se puede priorizar diferentes tipos de tráfico, tomando en cuenta que la calidad de servicio puede ser implementado bajo una reserva de recursos que se lo aprovecha ya que MPLS es capaz de reservar recursos a través de un dominio o de diferentes dominios (Doménico Luna).

Permite la implementación de Ingeniería de tráfico: Con los nuevos protocolos de enrutamientos MPLS tiene la capacidad de cambiar dinámicamente la ruta, estas rutas pueden ser generadas por protocolos de capa de red bajo ciertas métricas, así como la aplicación de ciertas políticas en estos mismos protocolos para una mejor evaluación de los recursos de red, con protocolos RSVP – TE RSVP Traffic Engienering permite alternativas para un mayor impacto en la calidad de servicio (Doménico Luna).

Reserva de Recursos Intradominios MPLS: Con el uso de algoritmos de enrutamiento como de protocolos de reserva de recursos RSVP, se puede asegurar una correcta asignación de recursos a los tráficos según dirección destino, origen, puertos entre otros (Doménico Luna).

Garantía de calidad de servicio sobre el esquema IP: En una red MPLS los recursos que se destinan para tráfico FEC serán destinados para este tráfico exclusivamente hasta que el tráfico acabe y se liberen los recursos asignados y sean tomados por otro requerimiento, con MPLS los mismos recursos pueden ser usados en diferentes tráficos según los requerimientos especificados en el LSA (Doménico Luna).

Permite implementación de Balanceo de Carga: MPLS permite el balanceo de carga que se puede proporcionar a la red usando protocolos de capa superiores en los nodos que maneja MPLS, esta funcionalidad se puede combinar con otras características de MPLS como ingeniería de tráfico (Doménico Luna).

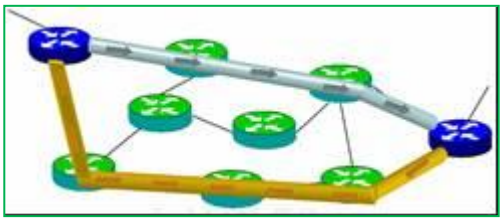


Figura 18: Balanceo de carga en MPLS, envío de tráfico por diferentes caminos[24]

3.11 CLASIFICACIÓN Y MARCAJE DE TRÁFICO

La clasificación es el proceso o mecanismo que identifica el tráfico y lo categoriza dentro de clases de marcaje que es de acuerdo al comportamiento y a las políticas empresariales.

Entre las herramientas para clasificación y marcado estan: NBAR, PBR, ACL/Route Map, CAR, MQC (Moodular Quality of Service command-line interfaz).

3.11.1 CLASIFICACIÓN DE TRÁFICO

En la clasificación de tráfico los más comunes son las ACL (Listas de control de acceso) y NBAR (reconocimiento de aplicaciones basadas en red).

LISTAS DE CONTROL DE ACCESO ACL

Las ACL se utilizan para cuestiones de seguridad, sin embargo se puede utilizar para clasificar el tráfico que entra o sale de una interfaz de un router o switch, el cual permite a cada clase de tráfico recibir un trato diferente y dar lugar a la QoS.

Cuando un paquete entra a una interfaz el router verifica sus cabeceras para ver donde debe ser entregado, previamente verificando si cumple o no las condiciones de la lista de acceso permitiéndole o negándole el siguiente salto. Las ACL actúan en orden secuencial, verifica la primera condición y luego continúa con la siguiente.

[24] Tomado de (Doménico Luna)

Para la implementación de QoS se realizarán sentencias solo de tipo permisivo (dando la prioridad a un determinado tipo de tráfico), aunque debido a la sentencia implícita se denegará todo tipo de tráfico que no cumpla con la sentencia (Quevedo Bravo & Vaca Nuñez, 2011).

RECONOCIMIENTO DE APLICACIONES BASADAS EN RED

Es un método de clasificación de tráfico que reconoce una amplia variedad de aplicaciones incluyendo TCP o UDP, decide buscando los paquetes de control para determinar que puertos se usaran para pasar la aplicación.

Entre las características se tiene la capacidad de descubrimiento del protocolo, que permite definir una referencia para pasar los protocolos en una interfaz determinada, se tiene el PDLM (Módulo de descripción de lenguaje) que permite que protocolos adicionales puedan ser agregados fácilmente a la lista de protocolos identificables, estos módulos se cargan en una memoria no volátil de router y cuando se reinicializa no se pierden, con este módulo se pueden agregar protocolos adicionales a la lista sin reiniciar el router (Quevedo Bravo & Vaca Nuñez, 2011).

3.11.2 MARCAJE DE TRÁFICO

Marcado y clasificación de paquetes.

Al proporcionar prioridad a diferentes flujos, se identifica primeramente el flujo que va a ser marcado, usándose descriptores de tráfico y categorizando el paquete que pertenezca a un grupo específico, determinando que paquetes es accesible a la manipulación de QoS.

Para categorizar los paquetes existen técnicas, métodos que seleccionan los paquetes que atraviesan un elemento o una interfaz en particular para los diferentes tipos de QoS (Paspuel Fraga, 2014).

Los métodos actuales de marcación de paquetes con su clasificación permiten poner información en las cabeceras de capa 2, 3 o 4 para el establecimiento de información dentro de la carga útil del paquete (Paspuel Fraga, 2014).

Dentro de los métodos para la marcación y clasificación de paquetes para obtener calidad de servicio están los descriptores de tráfico que son:

- Interfaz de entrada.
- Valor de CoS.
- Direcciones IP de origen o destino.
- Valor IP Precedence o DSCP en la cabecera IP.
- Valor EXP en la cabecera MPLS.
- Tipo de aplicación.

Capa de enlace

- CoS: A nivel de capa de enlace en Ethernet 802.1p y los marcos ISL, es posible incrustar información de calidad de servicio CoS (class of service) mediante 3bits que ingresan en un campo adicional de 4 Bytes (etiqueta denominada Tag o Label), dentro del protocolo MAC.
  Estos 3 bits permiten definir prioridades desde 0(máxima) a 7 (mínima) y ajustar un umbral en el buffer de entrada y salida del switch LAN para la descarga de paquetes, los 7 niveles de diferenciación permiten dar preferencia en el proceso de conmutación de paquetes (Moraga, 2004) por ejemplo:

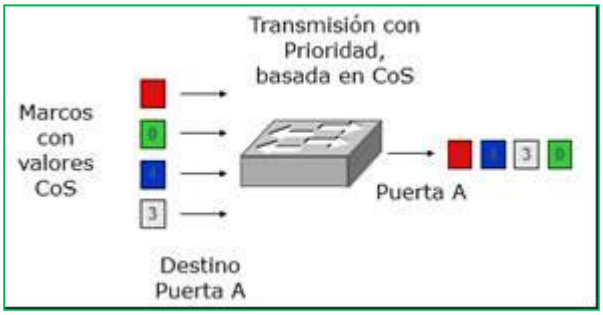


Figura 19: Marcado con valores CoS

- EXP: A nivel de capa de enlace se utilizó este campo EXP (experimental) que cuenta con tres bits para poder priorizar diferentes tipos de tráfico, que permite que la calidad de servicio pueda ser implementado bajo una reserva de recursos (Doménico Luna).

3.12 QoS EN MPLS Y EL MODELO DIFF-SERV

3.12.1 Arquitectura de Servicios Diferenciados

Para entender este modelo se analizará la arquitectura Diff-Serv que está basado en un modelo simple de tratamiento de tráfico, utilizado para grandes redes enrutadas, la clasificación, marcado de paquetes, política y operaciones son implementadas en los bordes de la red o en los host, el marcado se lo realiza mediante la asignación de un código específico (DSCP-DiffServ Code Point) que es lo que se necesita para identificar a cada clase de tráfico.

Se logra la escalabilidad cuando se implementa complejas funciones de clasificación y condicionamiento en los nodos de borde y aplicando conductas por salto a los agregados del tráfico que han sido apropiadamente marcados usando el campo DS en las cabeceras IPv4 ó IPv6 (Buñay Guisñay, 2013).

Separación de control y envío**:** En el envío IP la conectividad es lograda por la interacción de la parte del envío del paquete que usa la cabecera del paquete para encontrar una tabla de ruteo.

Primitivas del camino de envío

La clasificación: Aquí se saca la información de los paquetes que ingresan al dominio, la política se encarga de asegurar que el comportamiento se cumpla con las reglas que gobiernan la información de los paquetes.

Marcado DiffServ: Cada paquete IP lleva 1byte llamado octeto de Tipo de Servicio (TOS).

El ToS (Tipo de Servicio) reserva ancho de banda con anticipación y después se lo asigna al tráfico que tenga preferencias, como el de voz o un CoS con prioridad de modo que este tráfico pueda utilizar el ancho de banda reservado (Buñay Guisñay, 2013).

El campo ToS consta de 8 bits en la cabecera IPv4, donde los 6 primeros bits se definen como campo DSCP, está incluido como uno de los campos en la tecnología QoS denominado DiffServ, como se observa:

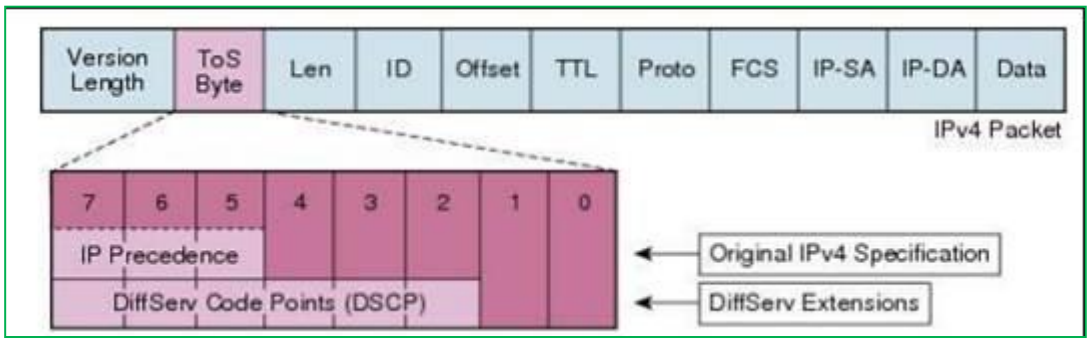


Figura 20: Campo ToS en IPv4: DSCP e IP Precedence[25]

El campo ToS es una característica poco utilizada de IP, hay un byte equivalente llamado octeto de Clase de Servicio.

A continuación se muestra el campo DS más detalladamente.

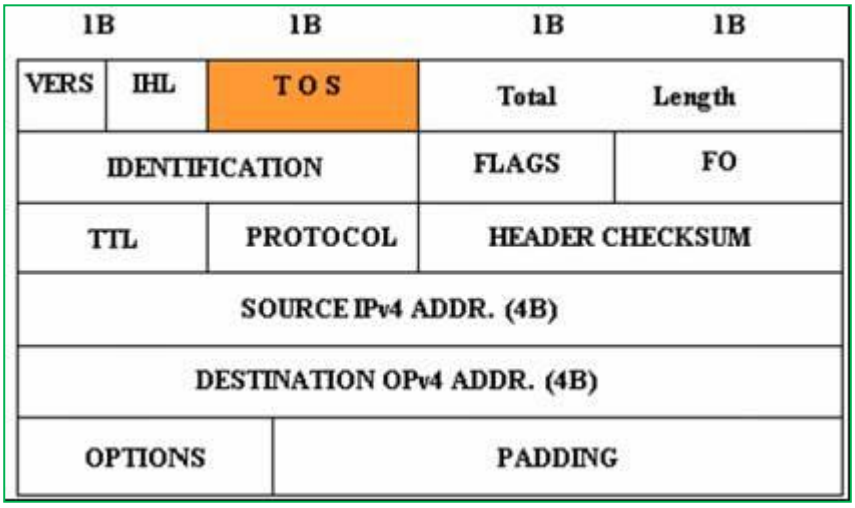


Figura 21: Campo DS – Campo TOS de IPv4[26]

[25] Tomado de (Buñay Guisñay, 2013)

[26] Tomado de (Buñay Guisñay, 2013)

Políticas de control

Clasificación y condicionamiento de tráfico: El SLA puede especificar la clasificación del tráfico y las reglas de re-marcado, la política de clasificación de paquetes identifica el subconjunto de tráfico que puede llegar a recibir un servicio diferenciado, el clasificador de tráfico identifica que flujo de tráfico llega al dominio DS.

Perfil de tráfico: Da las reglas para determinar si un paquete está dentro o fuera del perfil, los paquetes dentro del perfil pueden ser mandados sin ningún otro procesamiento o marcado, los paquetes fuera del perfil pueden ser encolados hasta que estén dentro del perfil (Buñay Guisñay, 2013).

3.12.2 Modelo Arquitectónico de los Servicios Diferenciados

El modelo Diff-Serv está formado por formado por un conjunto de nodos DS operando bajo una política de servicio común que es suministrada por el proveedor de servicio y un conjunto de grupos per-hop behavoir (PHB) implementado en cada nodo.

El PHB es una descripción de un conjunto de paquetes BA (Behavoir Aggregate) que permite la construcción de servicios predecibles.

El dominio DS está formado por los nodos de borde y los nodos interiores, los de borde permiten clasificar y acondicionar el tráfico de entrada, mientras que los interiores que se encuentran en el núcleo, permiten conectar el interior con la periferia, adicionalmente son responsables de garantizar que el tráfico entrante se comporte conforme a un determinado TCA (Traffic Conditionating Agreement) acordado entre dominios.

El PHB está dividido en tres clases de servicio Expedite Forwarding (EF), Assured Forwarding (AF) y Best-Effort (BE) representadas en Internet por los servicios Premium, Assured y Best-Effort.

Expedited Forwarding (EF) (DSCP=101110) proporciona el mayor nivel de QoS al tráfico agregado, se utiliza para implementar un servicio extremo a

extremo de bajas pérdidas, baja latencia y baja variación de retardo, dominado servicio Premium es solo un nivel de calidad (Buñay Guisñay, 2013).

El comportamiento EF puede implementarse por diversos mecanismos de colas como:

Cola con prioridad simple: Se aplica si una cola de mayor prioridad no desaloja el tráfico EF por un tiempo mayor que la transmisión del paquete.

Cola en un grupo de colas servidas por un planificador WRR: Aquí el porcentaje de ancho de banda de salida asignado al tráfico EF es igual a la velocidad configurada.

Planificador CBQ (Class Based Queue): Da la prioridad al tráfico EF hasta la velocidad configurada.

El Servicio Asegurado AF (Assured Service) define cuatro clases de servicio AF1, AF2, AF3 y AF4, cada clase asigna una cantidad específica del espacio del buffer y ancho de banda de la interfaz garantizando una mayor fiabilidad y seguridad para los paquetes con alta prioridad frente a los de baja prioridad.

Los usuarios que controlan el servicio AF tienen un acuerdo de Nivel de Servicio (SLA) con el proveedor.

Las implementaciones de AF deben detectar y responder a las congestiones a largo plazo con descarte de paquetes y manejar las de corto plazo mediante mecanismos de colas (Buñay Guisñay, 2013).

A continuación se definen las clases de servicio de DiffServ:

	Clase1	Clase 2	Clase 3	Clase 4
Descarte bajo	001010	010-	011010	100010
Descarte Medio	001100	010100	011100	100100
Descarte Alto	001110	010110	011110	100110

Tabla 6: Clases de Servicio DiffServ [27]

3.13 ENCOLAMIENTO Y CONTROL DE CONGESTIÓN

La congestión en una red es cuando hay demasiadas fuentes enviando demasiados datos a la red para lo cual existen mecanismos de control de congestión como los sistemas de encolamiento que se utiliza para manejar situaciones donde la demanda de ancho de banda solicitada por las aplicaciones excede el ancho de banda total de la red, controlando la inyección de tráfico a la red para que ciertos flujos tengan prioridad sobre otros. Estos sistemas de encolamiento tienen un impacto en el ancho de banda, retardo, jitter y pérdida de paquetes. (Quevedo Bravo & Vaca Nuñez, 2011).

Encolamiento FIFO (First in first out): Es el más simple y consiste en el que el primer paquete que entra a la interfaz es el primer paquete en salir, es utilizado para interfaces de alta velocidad y no para bajas porque maneja cantidades limitadas de ráfagas de datos (Quevedo Bravo & Vaca Nuñez, 2011).

En algunos casos los routers implementan dos colas, una cola de alta prioridad que está dedicada a servir el tráfico de control de la red y una cola FIFO que sirven a los demás tipos de tráfico.

[27] Tomado de (Buñay Guisñay, 2013)

A continuación se muestra la gráfica de encolamiento FIFO:

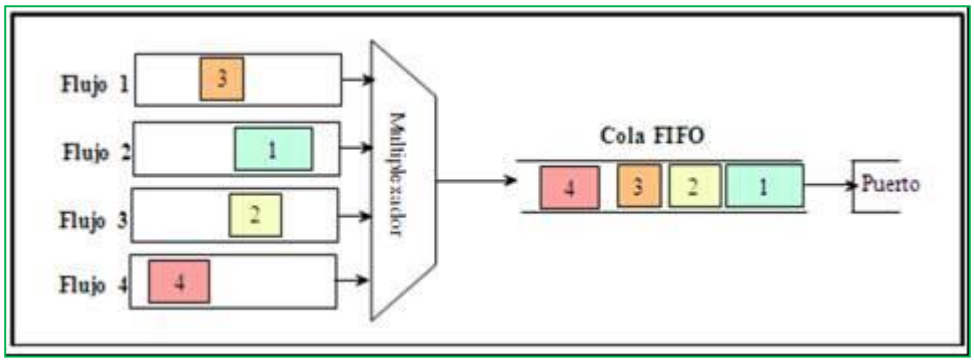


Figura 22: Encolamiento FIFO[28]

Encolamiento de Prioridad PQ (Priority Queueing): Es un conjunto de colas clasificadas desde alta a baja prioridad que luego los coloca en 4 colas de espera que son alta, media, normal y baja que son servidas en estricto orden de prioridad, los paquetes que no se puedan clasificar bajo este mecanismo es considerado como tráfico normal (Quevedo Bravo & Vaca Nuñez, 2011).

Si una cola de menor prioridad está siendo atendida y en ese momento se integra una cola de mayor prioridad ésta es atendida inmediatamente, este mecanismo se ajusta a condiciones donde existe un tráfico importante.

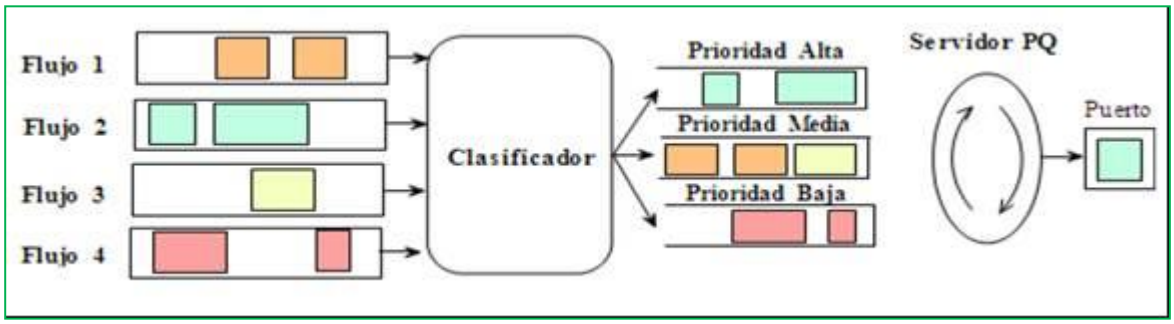


Figura 23: Encolamiento PQ

[28] Tomado de (Quevedo Bravo & Vaca Nuñez, 2011)-Cap 3

Encolamiento FQ (Fair Queuing): Se denomina también per-flow o flow based queueing, está diseñado para asegurar que cada flujo tenga un acceso justo a los recursos de la red evitando que un flujo de ráfagas consuma más ancho de banda de lo que le corresponde.

En este encolamiento primero el sistema clasifica los paquetes en flujo y los asigna a una cola dedicada para este flujo, las colas se sirven siguiendo un tiempo en orden round robin (orden secuencial circular).

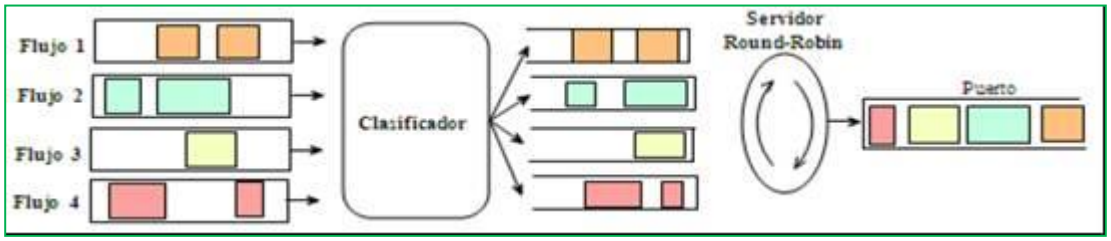


Figura 24: Encolamiento FQ[29]

Encolamiento WFQ (Weighted Fair Queuing): Este encolamiento es a través de un algoritmo que ordena el tráfico en flujos, utilizando una combinación de parámetros, así para una conversación TCP/IP se utiliza como filtro el protocolo IP, dirección IP fuente, dirección IP destino, puerto origen, etc. Una vez distinguidos estos flujos el router determina cuáles son de uso intensivo o sensible al retardo, priorizándolos y asegurándose que el flujo de alto volumen sea empujado al final de cola y los volúmenes bajos sensibles al retardo sean empujados al principio de la cola (Quevedo Bravo & Vaca Nuñez, 2011).

Cada paquete se clasifica y el servidor de la cola calcula, asigna un tiempo de fin de cada paquete. Este encolamiento es apropiado en situaciones donde se desea proveer un tiempo de respuesta consistente ante usuarios que generan altas y bajas cargas en la red, ya que se adapta a las condiciones cambiantes del tráfico.

[29] (Paspuel Fraga, 2014)

La desventaja es la carga para el procesador en los equipos de enrutamiento que hace a esta metodología poco escalable porque requiere recursos adicionales en la clasificación y manipulación dinámica de las colas.

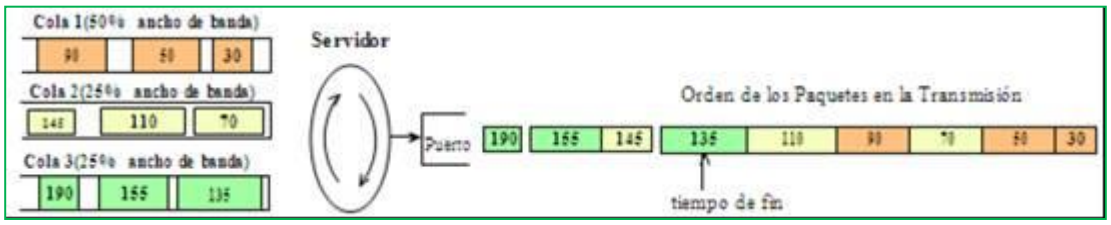


Figura 25: Encolamiento WFQ[30]

Encolamiento por espera equitativa ponderada basado en clases (CBWFQ):

Está basada en clases, desarrollada para evitar limitantes y extender la funcionalidad del algoritmo WFQ permitiendo la incorporación de clases definidas por el usuario permitiendo un mayor control sobre las colas de tráfico y asignación de ancho de banda (Quevedo Bravo & Vaca Nuñez, 2011).

En este encolamiento se define las clases de tráfico sobre la base de criterios de coincidencia con inclusión de protocolos, listas de control de acceso (ACL) y las interfaces de entrada, siendo de gran utilidad en proceso de implementación de calidad de servicio porque es necesario garantizar una determinada tasa de transmisión para cierto tipo de tráfico que lo permite CBWQ y no lo hace WFQ, adicionalmente las clases que son posible implementar pueden ser determinadas según las ACLs, valor DSCP o interfaz de ingreso, cada clase posee una cola separada y todos los paquetes que cumplen con el criterio definido para una clase particular son asignados a dicha cola.

Una vez que se establecen los criterios para las clases es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados (Quevedo Bravo & Vaca Nuñez, 2011).

[30] (Paspuel Fraga, 2014)

Las clases utilizadas en CBWQ se puedes asociar a:

- Flujos (direcciones origen-destino, protocolo, puertos)
- Prioridades (Campo DS differentiated service, otras etiquetas)
- Interfaces de entrada/salida
- VLAN

En función de esta clasificación se crean política de servicio para luego aplicarla a una interfaz, este método es aplicable a paquetes que no son susceptibles a retardo.

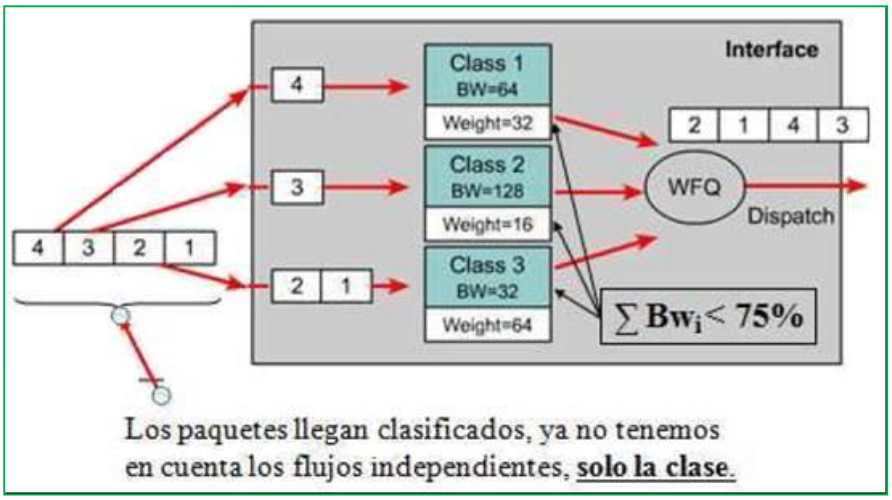


Figura 26: Encolamiento CBWFQ[31]

Encolamiento de baja latencia LLQ (Low Latency Queueing): Este encolamiento es una mezcla entre PQ y CBWFQ, es el método más recomendado para voz sobre ip y para telefonía IP, trabajando adecuadamente con videoconferencias.

Consta de dos colas de prioridad personalizadas, basándose en las clases de tráficos en conjunto con una cola de prioridad la cual tiene preferencia absoluta sobre las otras colas, este tipo de tráfico es susceptible al retardo y al descarte de paquetes por trabajar en aplicaciones en tiempo real, cuando hay tráfico en la cola de prioridad esta es atendida primero que las de prioridad personalizada.

[31] (Paspuel Fraga, 2014)

Si la cola de prioridad no está encolando los paquetes se procede a atender a otras colas según su prioridad funcionando el método CBWQ, es importante configurar el ancho de banda límite reservado para la cola de prioridad, la misma que provee un máximo de retardo garantizado para los paquetes entrantes para esta cola.

LLQ se recomienda para tráfico multimedia que requiere de unas características muy especiales como bajo retardo y jitter además se complementa usando CBWQ para el resto de colas como una cola más asociada a una clase determinada.

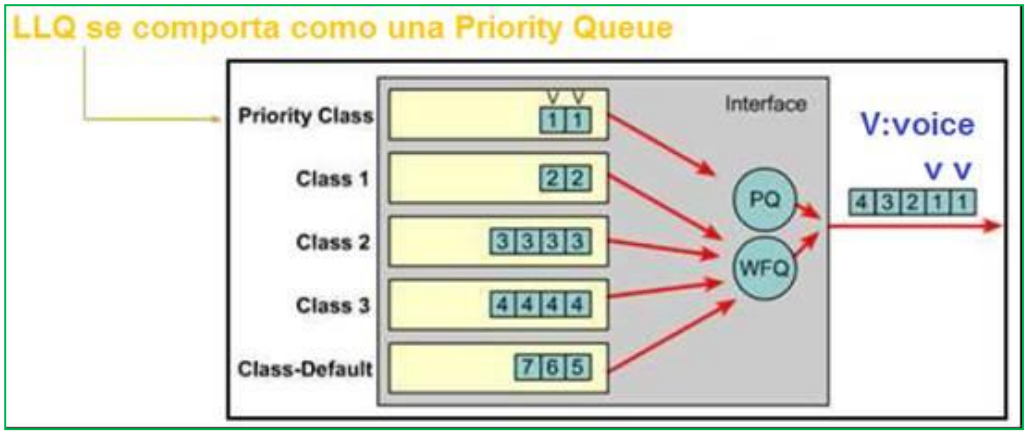


Figura 27: Encolamiento LLQ [32]

3.14 PREVENCIÓN DE CONGESTIÓN

Se utilizan técnicas como RED (Random Early Detection) y WRED (Weighted Random Early Detection) que evitan el efecto conocido como sincronización global, si no se configura ninguno de los dos el router usa el mecanismo de descarte de paquetes por defecto que es conocido como tail drop (Quevedo Bravo & Vaca Nuñez, 2011).

La sincronización global se refiere que al existir múltiples conexiones TCP que operen sobre un enlace común pueden incrementar el tamaño de la ventana deslizante sin embargo consume el ancho de banda, experimentando errores de transmisión, disminuyendo la calidad del enlace.

[32] (Paspuel Fraga, 2014)

Los métodos de control de congestión tratan este problema descartando paquetes de manera aleatoria. A medida que se llega el estado de congestión de la red, más paquetes que ingresan son descartados para no llegar al punto de congestión en el enlace, con la desventaja que solo sirve para el tráfico basado en TCP, ya los otros protocolos no usan ventana deslizante.

Tail drop: Es una manera sencilla de gestionar la memoria de la cola ya que trata todo el tráfico de igual forma y no hace diferencias entre clases de servicio, cuando hay una situación de congestión las colas se llenan, cuando la cola de salida está llena y entra a ejecutar este mecanismo los paquetes que llegan son descartados hasta que la congestión es eliminada y la cola no está muy llena así:

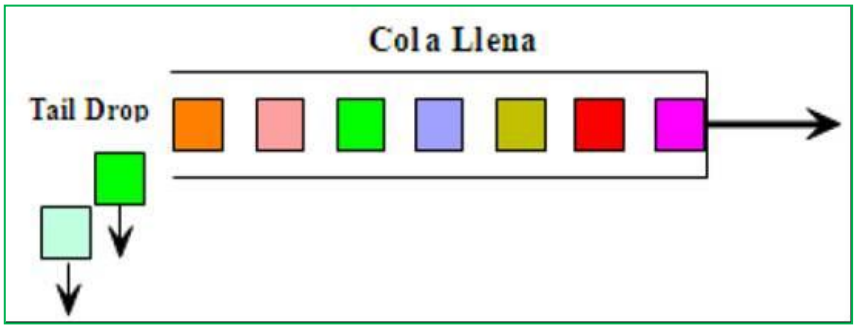


Figura 28: Tail Drop[33]

Random Early Detection (RED)

Esta forma obliga a que el flujo de datos reduzca el tamaño de la ventana de transmisión bajando la cantidad de información enviada, controla el tráfico de la red evitando que la congestión se produzca. Este sistema emplea un perfil de descarte drop profile del paquete para controlar el proceso de descarte de paquetes, adicionalmente define un rango de probabilidad de descarte mediante un rango de estados de ocupación de la cola, si el mismo permanece por debajo del umbral mínimo configurado por el usuario, un paquete nunca se descarta de la cola.

[33] (Paspuel Fraga, 2014)

- Si el nivel ocupacional excede un umbral máximo la cola funcionará como si estuviera configurado Tail Drop.
- Si el nivel ocupacional permanece entre el min y el max un paquete se tirará de acuerdo a una probabilidad definida por el usuario.

Weighted Random Early Detection (WRED): Este método combina el potencial del algoritmo RED con la posibilidad de usar precedencia IP, proveyendo características de rendimiento diferenciado para diferentes clases de servicio, puede usarse con RSVP y proveer QoS con carga controlada (Quevedo Bravo & Vaca Nuñez, 2011).

WRED hace dos proximidades para dar solución a problemas de descartar paquetes linealmente:

- Clasifica el tráfico que ingresa en flujos basados en parámetros teniendo la dirección de entrada y salida de los puertos.
- Mantiene el estado de flujos activos, conservando los paquetes en las filas de espera de la salida.

WRED usa esta clasificación para asegurar que cada flujo no consuma más de lo que tiene permitido en los buffer de salida.

3.15 CODECS PARA EL ANÁLISIS DE VoIP

Según la ITU-T G (Serier: Transmission system and media, digital system and network) se tiene los siguientes codecs:

G.711: Es el estándar de compresión de audio de la ITU-T que es usado principalmente en telefonía empezando a usarse 1972, representa señales de audio con frecuencia de voz humana.

G723.1: Es el estándar de códec de voz de banda ancha de la ITU-T, es una extensión de la recomendación G721 de 24 y 40 kbits/s.

G729: Es un algoritmo que comprime la voz en trozos de 10 milisegundos, permitiendo la compresión de datos de audio para voz, se lo usa en aplicaciones de Voz sobre IP por sus bajos requerimientos en ancho de banda, opera a una tasa de 8kbits/s, existiendo tasas de 6.4 kbit/s y de 11.8 kbits/s para menor o mayor calidad en la conversación.

CAPÍTULO 4

4 EVALUACIÓN DE LOS PARÁMETROS DE QoS PARA EL DISEÑO DE UNA RED VPN CON MPLS.

4.1 DISEÑO DE LA RED VPN MPLS CAPA 3

4.1.1 INTRODUCCIÓN

Muchas de las empresas, centros educativos entre otros tienen sucursales en diferentes sitios remotos, por lo que se busca la concentración de sus servicios como son voz, video y datos para que se distribuya eficientemente la información. Las redes VPN MPLS permiten garantizar la información interconectando diferentes sitios remotos con una mayor flexibilidad, eficiencia, seguridad y bajo costo que son ventajas significativas de la tecnología MPLS, adicionalmente la tendencia del mundo actual es migrar las antiguas tecnologías como ATM, Frame Relay a las redes de nueva generación como son las VPN MPLS.

Para el diseño se considera que se tiene una empresa matriz que se va a comunicar con una sucursal, consideremos que la empresa tiene al menos un tiempo de vida de 5 a 10 años y que será una empresa consolidada para que tenga una matriz y una sucursal.

Primeramente nos enfocaremos para el diseño de la red en analizar los requerimientos que se debe considerar:

4.2 REQUERIMIENTOS

Una empresa actualmente busca que se integre seguridad, rendimiento, disponibilidad, productividad llamándolo convergencia de redes, tomando en cuenta estos elementos analizaremos:

- Requerimientos de usuario
- Requerimientos para Servicios.

4.2.1 REQUERIMIENTOS DE USUARIO

En este requerimiento la red que se diseña debe cumplir la tarea que le fue asignada necesitando para esto cumplir con:

Tiempo de respuesta: Que sea el adecuado de acuerdo al servicio, para servicios de video y audio necesitando un tiempo moderado.

Confiabilidad: A través de la topología que se diseña se genera un método de redundancia permitiendo que la red sea confiable en sus diferentes servicios como son descargas de archivos, navegación en la internet, videoconferencia.

Adaptabilidad: El diseño de la red se adapte a las necesidades de una empresa sin que tenga que rediseñarse totalmente la red, permitiéndose fácilmente añadirse o retirarse dispositivos de la red y pueda expandirse.

Seguridad: Una red debe cumplir con políticas de acceso a la configuración de los dispositivos, para evitar daños a la red y garantizar la información al usuario.

4.2.2 REQUERIMIENTOS PARA SERVICIOS

Entre los servicios más usados en la institución se tiene:

Servicio de Videoconferencia: Para este servicio se necesita de un retardo mínimo del origen al destino para mantener interactividad al momento de la conversación.

Navegación Web y correo electrónico: Para la navegación Web el tiempo de acceso debe ser mínimo mientras que para el correo electrónico el tiempo de respuesta no necesariamente será inmediata, puede llegar a tardar algunos minutos.

Servicios de Voz: Hay que tomar en cuenta que la voz es digitalizada y transmitida como datos al destino por lo que dependerá el tiempo de respuesta de las terminales telefónicas.

Tomando estas consideraciones se trabajara en el diseño los siguientes tipos de tráfico:

- Voz
- Datos críticos
- Datos de administración
- Datos generales como ping, Best effort.

Después de haber analizado los requerimientos procederemos a detallar el desarrollo de la Red VPN MPLS.

4.3 SELECCIÓN DE LA TOPOLOGÍA DEL BACKBONE

Tradicionalmente las redes VPN MPLS tienen las siguientes topologías tipicamente que son Hub and Spoke y Full Mesh como lo analizaremos.

Hub and Spoke VPN

En esta topología todos los sitios están conectados y administrados en un router central o Hub Site, como se muestra en la figura:

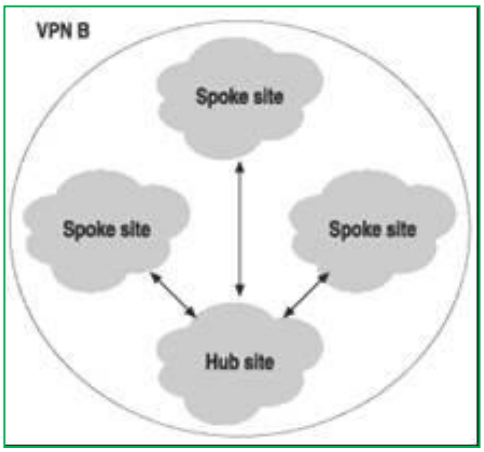


Figura 29: Conectividad de Sitio en un Hub and Spok VPN[34]

[34] Tomado de: https://www.juniper.net/techpubs/en_US/junose10.3/information-products/topic-collections/swconfig-bgp-mpls/id-49476a.html

Esta topología tiene como ventaja una mayor seguridad entre la matriz y sus filiales dando acceso restringido a las mismas, como desventaja al ser un único router de enlace, si el mismo se daña pierden la conectividad con el resto de enlaces de sus filiales.

Full Mesh

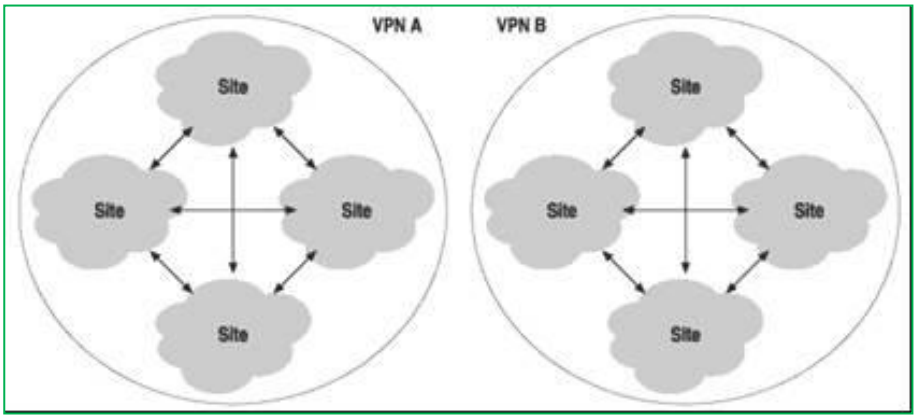


Figura 30: Conectividad Full Mesh VPN [35]

Como se puede apreciar principalmente esta topología maneja redundancia evitando la caída del enlace de red en caso de existir algún problema en uno de sus caminos además cada VPN A se enlaza con su VPN A en diferentes sitios remotos y no se comunica con sitios VPN B permitiendo una mejor administración de la red.

De lo anteriormente analizado se observa que la topología Full mesh es la más adecuada por conectividad de redundancia que es característica de las VPN MPLS adicionalmente se busca que cada ruta en el núcleo tenga un next-hop más cercano hacia el destino para poder tener entre los equipos alta disponibilidad, redundancia y tolerancia a las fallas.

[35] Tomado de: https://www.juniper.net/techpubs/en_US/junose10.3/information-products/topic-collections/swconfig-bgp-mpls/id-49476a.html

A continuación se presenta el diseño de la Topología Full Mesh en el backbone de la VPN MPLS de la red:

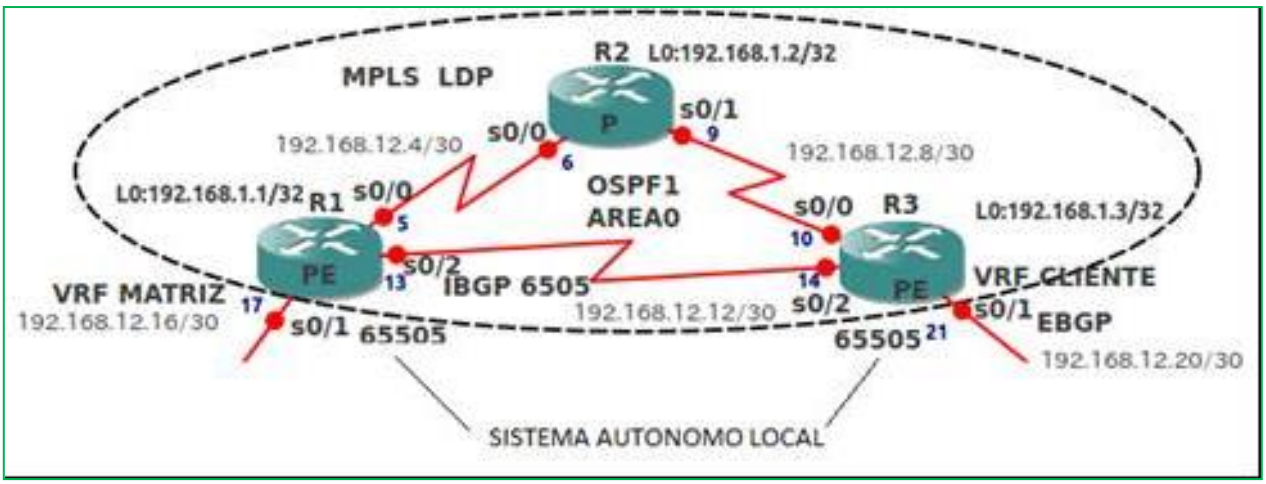


Figura 31: Modelo del Diseño del Backbone de la red VPNMPLS[36]

Como se puede observar el backbone MPLS esta formado por los dos routers R1 y R3 que son los provider-edge (PE) que es el límite del proveedor y el router provider (P) que es proveedor.

MPLS (Multiprotocol label switching) necesita internamente un protocolo IGP para intercambiar los LDP´s (label distribution protocol) utilizándose OSPF por sus bondades que al ser un protocolo de enrutamiento dinámico en caso de caída de algún enlace se recalcula automáticamente su nueva ruta, otra bondad que tiene son sus interfaces lógicas Loopback.

[36] Fuente propia

4.4 TOPOLOGÍA COMPLETA DE LA RED

Como se menciono anteriormente se realizara el diseño para una empresa que tiene una Nube Matriz y una Nube Sucursal como se muestra en la figura:

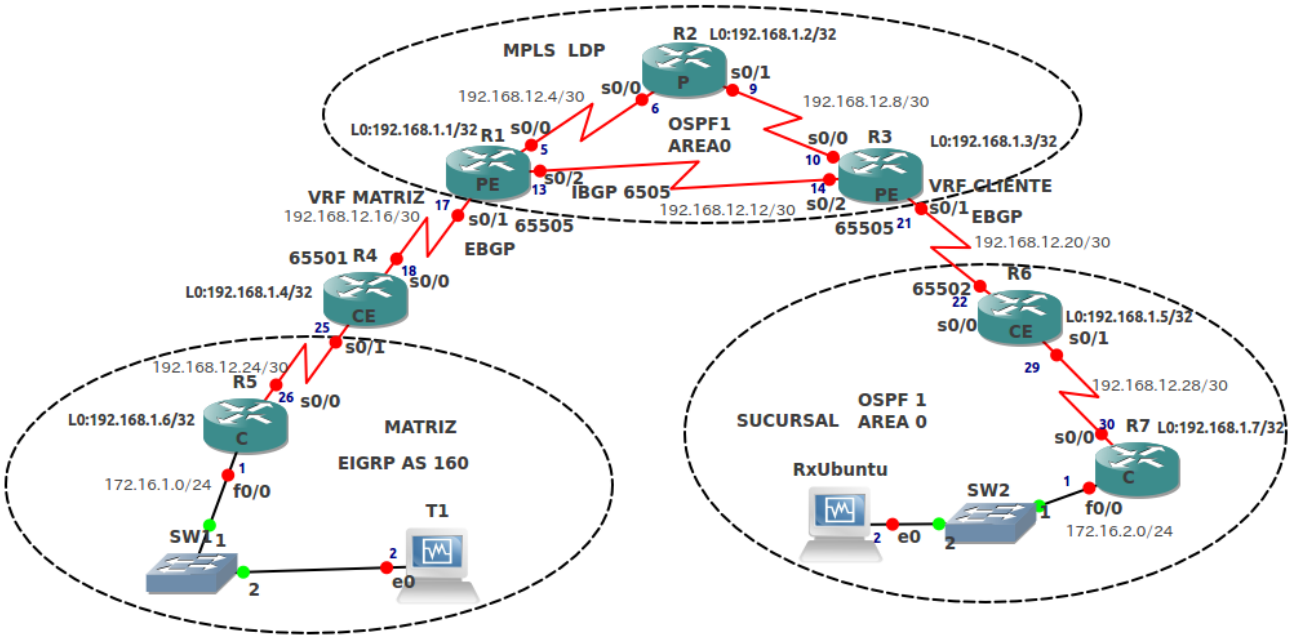


Figura 32: Modelo del diseño de la red en ambiente laboratorio[37]

En la nube matriz se tendrá un router de Gateway que es el CE, es el límite del cliente e igualmente en la nube Sucursal.

Dentro de la matriz se trabajará con el router del cliente C que necesita un protocolo IGP para intercambiar su información que será EIGRP y para el caso de la matriz sucursal será OSPF.

Para la VPN se enlazará entre los PE's y CE's con un protocolo BGP (Border Gateway Protocol), que permite intercambiar información de enrutamiento entre diferentes sistemas autónomos, en la frontera de PE S0/1 donde se crea la virtual routing and forwarding (VRF) que actúa como

[37] Fuente Propia

un router lógico permitiendo definir caminos virtuales para diferentes clientes es así que para la Matriz se crea la VRF MATRIZ y para la sucursal se crea la VRF SUCURSAL.

Para intercambiar información entre la nube matriz y la nube MPLS se necesita aplicar una redistribución donde primero se redistribuye la información entre el protocolo EIGR con BGP y luego BGP con MPLS, repitiéndose el mismo procedimiento para la Sucursal creando así una especie de túnel.

4.5 ASIGNACIÓN DE DIRECCIONAMIENTO Y EQUIPO

A continuación se detalla el direccionamiento de la red:

Equipo	Interfaz	Dirección de red	Protocolo	Default Gateway	Área
P R2	Serial 0/0 Serial 0/1	192.168.12.4/30 192.168.12.8/30	OSPF		0
Loopback0 (R2)	L0	192.168.1.2/32			
PE (R1)	Serial 0/1 Serial 0/0 Serial 0/2	192.168.12.16/30 192.168.12.4/30 192.168.12.12/30	EBGP 65505 OSPF IBGP 6505		0
Loopback0 (R1)	L0	192.168.1.1/32			
PE R3	Serial 0/0 Serial 0/2 Serial 0/1	192.168.12.8/30 192.168.12.12/30 192.168.12.20/30	OSP IBGP 6505 EBGP65505		0
Loopback0 (R3)	L0	192.168.1.3/32			

CE Frontera Matriz R4	Serial 0/0 Serial 0/1 Loopback 0	192.168.12.16/30 192.168.12.24/24 192.168.1.4/32	EBGP (BGP) 65505 EIGRP AS 160		
CE Frontera Sucursal R6	Serial 0/0 Serial 0/1 Loopback 0	192.168.12.20/30 192.168.12.28/30 192.168.1.5/32	EBGP (BGP)65502 OSPF 1		
C Matriz R5	Serial 0/0 Fast 0/0	192.168.12.24/30 172.16.1.0/24	EIGRP AS 160		
PC-T1	Eth0	172.16.1.0/24		172.16.1.1/24	
C Sucursal R7	Serial 0/0 Serial 0/1	192.168.12.20/30 192.168.12.28/30	AS 65502 OSPF 1		
PC-RX	Eth0	172.16.2.0/24		172.16.2.1/24	

Tabla 7: Direccionamiento del modelo del diseño de la red[38]

Como se puede observar en la tabla de direccionamiento se trabaja con direccionamiento privado y subneteada con mascara /30 tanto para el backbone de la MPLS, los router de frontera del cliente CE, los router´s del cliente de la matriz y de la sucursal permitiendo con esto optimizar el espacio de direccionamiento.

Para los host de los router cliente se trabaja con un direccionamiento privada clase B permitiendo optar por un mayor crecimiento de usuarios tanto para la matriz como para la sucursal.

En lo que respecta a los dispositivos que conforman la red se escogió la marca CISCO ya que son dispositivos compatibles, escalables, garantizables, con programación amigable al usuario que son usados para pequeña, medianas y grandes empresas.

[38] Autoria Propia

A continuación se detalla las especificaciones de los dispositivos de la red.

Cisco Catalyst 3745 (Hardware)	
Descripción	**Especificación**
Memoria RAM **Memoria ROM**	128MB Memoria SDRAM 32MB Memoria NVRAM (flash)
Conexión de redes	
Velocidad de transferencia de datos **Versión mínima de Cisco IOS** **Indicadores de estado.** **Tecnologías que soporta** **Características**	225Kbps CISCO IOS 12.4 T Aseguran baja latencia para aplicaciones críticas WAN: Frame Relay, ATM, XDSL Ofrece solución integrada de seguridad, telefonía IP, correo de voz, video, datos, servicios inteligentes como QoS, IP multicast, VPN, Firewall, Prevención de Intrusiones, control de admisiones de llamadas.
Total ranuras de expansión (libres)	Tiene dos puertos 10/100Mbps, dos slots para módulos AIM (Advanced Integration Module).
Interfaces	Tres tarjetas de interfaz WAN y dos HDSM (High Density Service Module).

Tabla 8: Características del Router 3745[39]

Cisco Catalyst 2960 (Hardware)	
Descripción	**Especificación**
Performance	Reenvío de ancho de banda Cisco Catalyst 2960G – 24T : 32Gps 64MB DRAM 32MB Memoria Flash
Conectores y cableado	Puertos 10Base-T: conectores RJ-45, dos pares de categoría 3, 4,5 o par trenzado UTP. Puertos 100 Base –TX conectores RJ-45, dos pares de cable UTP categoría 5. Puertos 1000 Base –T conectores RJ-45, cuatro pares de cable UTP categoría 5. Puertos 1000 Base –T basados en SFP cuatro pares de cable UTP categoría 5.

[39] Autoria Propia

	Puertos 1000 Base –SX, LX/LH, ZX, BX, CWDM basados en SFP conector de fibra LC (fibra multimodo).
MTBF	219,629 hr (MTBF Tiempo medio entre fallos)
Especificaciones de alimentación para Cisco Catalyst 2960	
Potencia max	75W (Consumo máximo)
AC Voltaje de entrada y corriente	100-240V AC (Rango Automático) 1.3 a 0.8 A, 50-60 Hz
Potencia	0.075KVA
Voltaje DC	± 12V 10.5A (Entrada RPS)

Tabla 9: Características del Switch 2960[40]

Como se puede observar para el equipo de backbone se utilizó el router Cisco 3745 con IOS versión mínima 12.4 T, que tiene características VPN MPLS, el mismo que se encarga de recoger todo el tráfico que le llega y lo transfiere a los dispositivos PE (Cisco 3745) donde se concentran todas las rutas y se envían a los diferentes escenarios de los CE como son la matriz y la sucursal.

Como antecedente se debe considerar que el backbone es responsabilidad del proveedor de servicio, los mismos que utilizan dispositivos más robustos como son:

Para el CORE de backbone usan por lo general equipo Cisco 7600 / 7200, para la red MPLS equipo Cisco 3700/ 2900/ 1800, para puntos remotos (cliente) equipo Cisco 1800/ 1700 mínimo con IOS versión 12.4 T, que tienen características VPN MPLS, con puertos LAN 10/100 Mbps y asignación de ancho de banda.

[40] Autoria Propia

4.6 EMULACION DE LA RED

4.6.1 Software usado

El proyecto diseñado se lo emulo con el software especializado GNS3 que es una herrmienta en tiempo real que permite realizar topologías complejas de red para luego ejecutarlas, adicionalmente permite la virtualización de maquinas virtuales como VirtualBox, los mismos que se pueden instalar en sistemas operativos Windows o Linux que para nuestro caso se utilizó Linux (Ubuntu 14.0) que es el sistema operativo con el que trabaja el software D-ITG (Distributed Internet Traffic Generator) de forma estable.

El software D-ITG tiene la ventaja de ser de código abierto que permite inyectar tráfico y realizar mediciones del mismo con diversos protocolos como IPV4 o IPv6 con diferentes tamaño de paquetes, permitiendo calcular el retardo, el jitter, el delay y la pérdida de paquetes que son parámetros para evaluar el QoS.

4.6.2 CONFIGURACIÓN DE EQUIPOS EN LA RED MPLS

1. **Configuración de las interfaces en el backbone**

```
R2# config t
R2 (config) # interface s0/0
R2 (config-if) # ip address 192.168.12.6 255.255.255.252
R2 (config-if) # clock rate 64000
R2 (config-if) # no shutdown
R2# wr
¡Lo mismo que se hizo para R2 se realiza para R1 y R3.
```

Figura 33: Configuración de las interfaces en el Backbone

Como se puede observar en la figura 33 primeramente se realiza la asignación de direccionamiento en las interfaces de todos los dispositivos de la red del backbone en la red MPLS.

2. Configuración del Protocolo OSPF en el backbone MPLS

Configuración en el P (R2) del backbone MPLS:

- Encaminamiento con el Protocolo OSPF proceso 1, área 0

```
R2 (config) # router ospf 1
R2 (config-router) # log-adjacency-changes
R2 (config-router) # network 192.168.1.2 0.0.0.0 area 0
R2 (config-router) # network 192.168.12.4 0.0.0.3 area 0
R2 (config-router) # network 192.168.12.8 0.0.0.3 area 0
! Lo mismo que se hizo para R2 se realiza para R1 y  R3
```

Figura 34: Configuración del protocolo OSPF

Como se puede observar en la figura 34 se realizó el enrutamiento OSPF que es un protocolo de enrutamiento interno (IGP) que anuncian toda la información al arrancar, el protocolo OSPF es un protocolo dinámico.

Una de las características principales de este protocolo es que se envían paquetes link state solo cuando hay falla en algún enlace donde todos los router actualizan su base topológica, hay que considerar que solo se envían las nuevas actualizaciones de rutas y no la tabla completa.

3. Configuracion de BGP

```
R1 (config) # router bgp 65505
```

Figura 35: Configuración del protocolo BGP

Como se puede observar en la figura 35 se da la configuración del protocolo bgp, lo mismo que se hizo para R1 que es el PE se realiza para R3 (PE), tomando como antecedente que antes de configurar la MPLS se establece un full mesh de bgp entre los PE (R1 y R3) del backbone para crear servicios de redes privadas virtuales sobre MPLS (VPN-MPLS), el número del proceso va desde 1 a 65535, tomandose para este proyecto el número 65505 luego se realiza la redistribución de ruta.

4. **Establecimiento de adyacencias entre los pares BGP**

```
R1 (config-router) # bgp log-neighbor-changes
R1(config-router) # neighbor 192.168.1.3 remote-as
R1(config-router) # neighbor 192.168.1.3 update-source Loopback 0
¡La  misma programación que se hizo para R1 (PE) se realiza paraR3 (PE)
```

Figura 36: Configuración para establecimiento de adyacencias

Como se observa en la figura 36 se configura las adyacencias entre los pares BGP, donde se especifica el router vecino y se indica que se actualice el enrutamiento a través de la interfaz de loopback.

5. **Configuración de los protocolos en los clientes**

   Para el área Matriz se configuro el protocolo dinámico EIGRP y para el área SUCURSAL se configuró el protocolo dinámico OSPF.

6. **Redistribución de ruta**

   EIGRP necesita 5 métricas para redistribución de ruta dentro de bgp y luego se redistribuye la ruta de bgp dentro de EIGRP.

   Comando:

   - redistributing protocolo: bandwidth, delay, reliability, load, MTU

   Métricas:

   - redistribute bgp 65501 metric 64 2000 255 1 1500
   - Bandwich (ancho de banda)= 64 (esta en Kilobits)
   - Delay =2000 (milisegundos)
   - Reliability=255 valor más alto confiable
   - Load= 1 Lo menos ocupado el enlace
   - MTU=1500 (unidad máxima de transferencia)

7. Configuración básica de MPLS

Previamente establecidos los protocolos de enrutamiento se configuran las funcionalidades MPLS en los router.

8. Activar IP CEF para trabajar en entornos MPLS

```
R2 (config) # ip cef
Lo mismo que se hizo para R2 (P) se lo realiza a R1 (PE) y R3 (PE).
```

Figura 37: Configuración del ip cef

Como se puede observar en la figura 37 se necesita habilitar ip cef (Cisco express forwarding) en los router del backbone de la MPLS para permitir el modo de procesamiento de paquetes de cisco y funcione la MPLS**.**

9. Activar el protocolo de distribución de etiquetas LDP

```
R2 (config) # interface serial 0/0
R2 (config # mpls ip
R2 (config # mpls label protocol ldp
!Lo mismo se realiza para los routers R1 (PE), R3(PE), R4(CE), R6(CE).
```

Figura 38: Configuración del protocolo LDP

Como se puede observar en la figura 38 se activa el intercambio de distribución etiquetas LDP para que cada interfaz pueda hablar MPLS, esto se lo hace utilizando el comando **mpls label protocol ldp**.

10. Verificación del funcionamiento de MPLS en la red

Para realizar la verificación de MPLS se tiene los siguientes comandos:

sh mpls interfaces.- Al ejecutar este comando en el PE del backbone MPLS se mostrará las interfaces en las que esta funcionando MPLS-LDP.

sh mpls ldp parameters.- Este comando al ser ejecutado muestra los parámetros que esta utilizando el protocolo.

sh mpls forwarding-table.- Este commando muestra la tabla de envío (table de forwarding) del router.

sh mpls ldp neighbor: .- Este commando muestra la vecindad con los demás router.

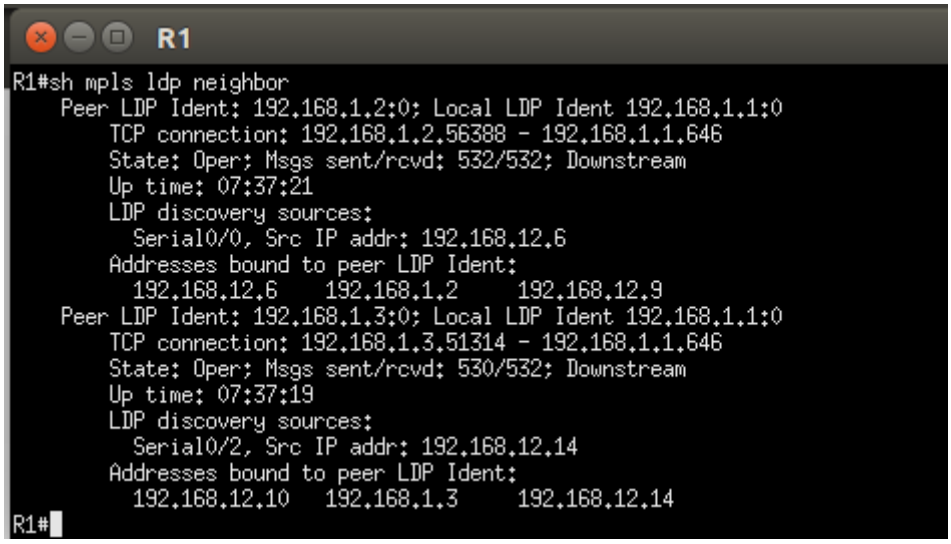


Figura 39: Verificación del funcionamiento de MPLS en la red.

Se puede observar en la figura 39 la verificación del funcionamiento de MPLS al mostrar los routers que mantienen una relación de vecindad.

La configuración completa de la red esta detallada en el Anexo 1.

4.6.3 ELEMENTOS PARA CONFIGURAR LA VPN MPLS

1. **Configurar las vrf en los PE**

```
R1 (config) # address-family ipv4 vrf MATRIZ
R1 (config-router-af) # neighbor 192.168.12.18 remote-as 65501
R1 (config-router-af) # neighbor 192.168.12.18 activate
! Lo mismo que se hizo para R1 se hace para R3 (PE) pero como VRF
```

Figura 40: Configuración de las VRF en los PE

Como se observa en la figura 40 es la configuración de las vrf en los PE dentro de la configuración de bgp donde se crea servicios de redes privadas

virtuales vrf (virtual routing and forwarding) que son para tener un mismo dispositivo físico con diversos clientes con la caracteristica de no se verse entre ellos.

2. **Habilitar la conectividad con los clientes**

```
R1 (config)# ip vrf MATRIZ
R1(config-vrf)#  rd 65505:1
R1(config-vrf)#  route-target import 65505:1
R1(config-vrf)#  route-target export 65505:1
```

Figura 41: Habilitación de conectividad con los clientes

Como se observa en la figura 41 se configuran dos parámetros; el route distinguisher (rd) que es distinguidor de ruta y el router target (rt) que distribuye la ruta hacia los router C (Clientes).

3. **Se redistribuye la ruta dentro de los PE**

```
R1 (config-router)# address-family vpnv4
R1(config-router-af)#  neighbor 192.168.1.3 activate
R1(config-router-af)#  neighbor 192.168.1.3 send-community extended
```

Figura 42: Configuración de redistribución de ruta

Como se observa en la figura 42 se implementa el address family dentro del protocolo BGP para redistribuir la ruta.

4. **Verificación de Conectividad de la red VPN MPLS**

```
miroslava@miroslava-VirtualBox:~$ ping 172.16.2.2
PING 172.16.2.2 (172.16.2.2) 56(84) bytes of data.
64 bytes from 172.16.2.2: icmp_seq=1 ttl=64 time=0.033 ms
miroslava@miroslava-VirtualBox:~$ ping 172.16.1.1
PING 172.16.1.1 (172.16.1.1) 56(84) bytes of data.
64 bytes from 172.16.1.1: icmp_seq=1 ttl=252 time=40.9 ms
```

Figura 43: Verificación de conectividad de la red

Se puede observar en la figura 43 la conectividad entre los host de origen y de destino donde están programadas las VRF MATRIZ y las VRF CLIENTE.

Protocolo BGP en el PE (R1)

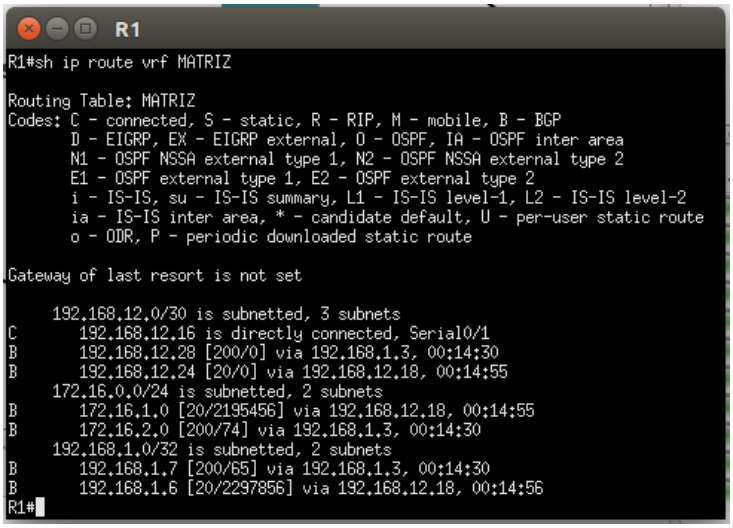


Figura 44: Verificación de las VRF

Como se puede observar en la figura 44 se verifica la tabla de enrutamiento en el (PE) del backbone MPLS que se encuentre activo el protocolo BGP que es el protocolo de frontera que enlaza a la MPLS con el protocolo EIGRP de la MATRIZ.

Protocolo de enlace BGP e EIGRP en el CE (R4) de la Matriz.

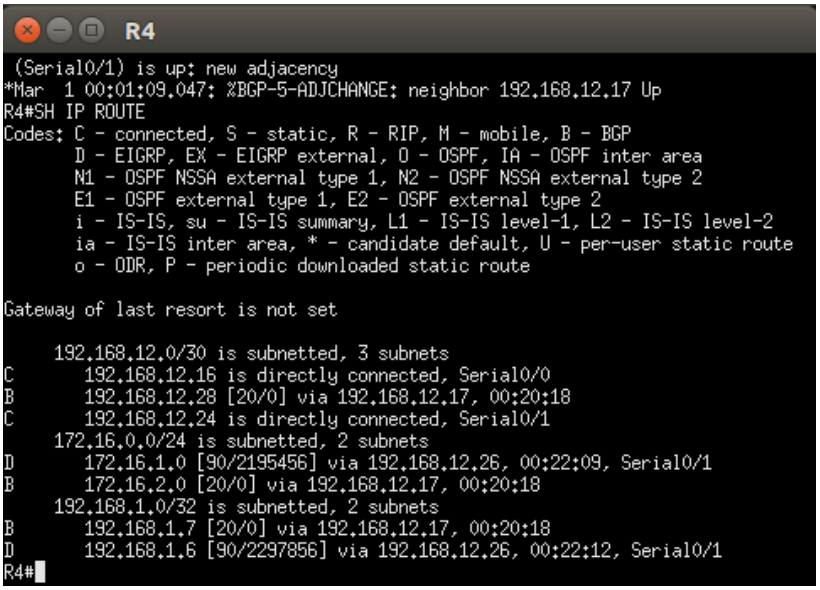


Figura 45: Verificación de los protocolos BGP e EIGRP

Se puede verificar en la figura 45 que en la tabla de enrutamiento del CE (Customer Edge) se trabaja con los dos protocolos el EIGRP (D) que es el protocolo que enruta la matriz y el BGP (B) que es el protocolo que enlaza al backbone MPLS con el protocolo EIGRP.

Verificación de la de las etiquetas

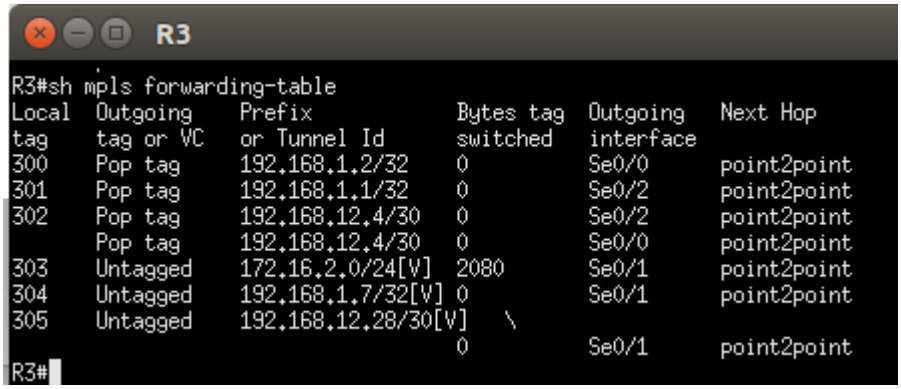


Figura 46: Verificación de etiquetas

Como se observar en la figura 46, el comando **show mpls forwarding-table,** muestra la asignación de etiquetas por cada ruta en este caso esta en el PE del VRF CLIENTE (R3).

Verificación del campo EXP

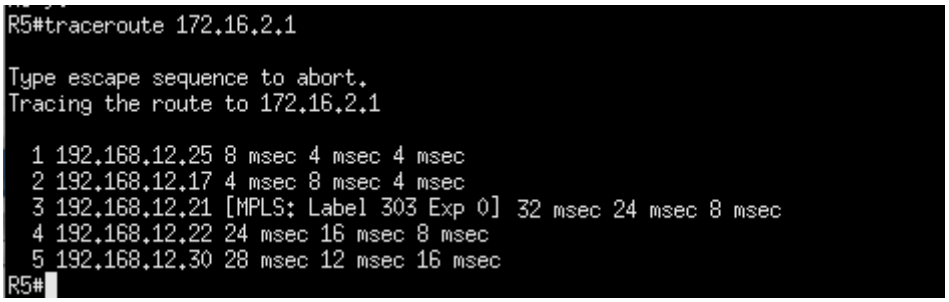


Figura 47: Verificación del campo EXP

Como se puede observar en la figura 47, el comando **traceroute** muestra los saltos para llegar desde una IP origen a una IP destino, en los saltos se aprecia el valor de la etiqueta y el campo EXP que por defecto tiene un valor de 0 que luego se manipulará para QoS mediante DiffServ.

4.7 CALIDAD DE SERVICIO EN LA RED VPN MPLS

Primeramente es necesario entender la importancia de la calidad de servicio que está íntimamente relacionado con la convergencia de redes y el internet del todo donde se conecta el internet a personas, cosas u objetos y se fusiona varios tipos de sensores y procesos con una gran cantidad de tráfico donde para el usuario la calidad de servicio es la percepción de que la aplicación esté funcionando bien o mal por ejemplo si la conversación se entrecorta, mientras que para la parte técnica la calidad de servicio es la posibilidad de maximizar el ancho de banda sin degradar las aplicaciones que están corriendo para lo cual se debe considerar ciertos parámetros para que no degrade una transmisión en tiempo real, como son el control de retardo, un contro de jitter (variación de retardo) y la pérdida de paquetes.

4.7.1 TIPOS DE DATOS

En una red varios tipos de tráfico permite mayor granularidad de la red donde se da prioridad dependiendo de las necesidades de cada empresa, por ejemplo para una empresa puede darle mayor prioridad a la Voz mientras que para otra empresas podrá darle mayor prioridad al envió de correo etc.

Para este proyecto se tendrá los siguientes tipos de tráfico que son Voz, Datos críticos para empresa (Datos transaccionales), Datos de administración (Administración de la Red como IP routing), Datos generales (ping, traceroute entre otros) y Best effort (Scavenger).

4.7.2 ASIGNACIÓN DEL ANCHO DE BANDA

En la red de prueba se considerará un ancho de banda de 64K con las siguientes asignaciones en porcentaje que harán que no se degrade la transmisión:

A continuación se detalla la asignación del ancho de banda para los diferentes tipos de tráfico:

Tipo de tráfico	Asignación de AB
Voz	15%
Datos críticos empresariales	20%
Datos de Administración	10%
Datos Generales	10%
Best effort (Scavenger)	5%

Tabla 10: Consideraciones de la asignación del Ancho de Banda

Como se observa en la tabla 10 se asigna para Voz un 15% del total de ancho de banda para evitar que se degrade la conversación, en lo referente a Datos crítico se asignará un 20% del total del ancho de banda para asegurar el envío correcto de la información, un 10% del total del ancho de banda a Datos de administración para los protocolos de enrutamiento, un 10% para Datos generales como ping que no necesita absorber los recursos de ancho de banda de la red y un 5% del total del ancho de banda para Best Effort donde están los Scavenger (videos, juegos, redes sociales) que es un tipo de tráfico que no le interesa a la empresa más bien la perjudica.

4.8 CALIDAD DE SERVICIO CON MECANISMO DE DIFFSERV

El mecanismo DiffServ consiste en clasificar el tráfico entrante en diferentes niveles y realizar el marcaje.

4.8.1 CLASIFICACIÓN DE LOS PAQUETES

Para obtener el valor QoS Traffic Generator se obvia los dos últimos números del ToS y se sigue la regla siguiente en base a la ponderación dada por ejemplo para el ToS **011** 00000 se tiene:

0	**1**	**1**	0	0	0	0	0
2^5	2^4	2^3	2^2	2^1	2^0		
0	**16**	**8**	**0**	**0**	**0**	**=24**	

Tabla 10: Tabla de ponderación del ToS[41]

Como se observa en la tabla 10 el valor Precedence equivale a los tres primeros bits del ToS por ejemplo si el ToS es **011** 00000 entonces pertenece a la clase3 CS3.

A continuación se da la tabla de valores según la clase de servicio

ToS Bits Precedence	Clase de Servicio	IP Precedence
100 00000	CS4	4
011 00000	CS3	3
010 00000	CS2	2
001 00000	CS1	1

Tabla 11: Tabla de valores según la clase de servicio

La programación se lo realiza en el router del Cliente (C) en R5 como se muestra:

```
class-map match-any CLASE-GENERAL
match  precedence 1
class-map match-any CLASE-VOZ
match  dscp ef
class-map match-any CLASE-DATOS
match  precedence 2
class-map match-any CLASE-ADMIN
match  precedence 3
class-map match-any CLASE-CRITICO
match  precedence 4
```

Figura 48: Programación de las clases

[41] Fuente Propia

Como se puede observar en la figura 48 se realizó la programación de las clases con los valores de Ip precedence para la calidad de servicio con el mecanismo de DiffServ como se describe a continuación mas detalladamente.

4.8.2 MARCAJE CON IP PRECEDEN Y DSCP

Tomaremos en cuenta que al marcar IP Precedence se puede tener 8 diferentes marcaciones y al usar DSCP se obtienen 64 marcaciones siendo más granulado las marcaciones en la red.

Para el proyecto se usará ambas IP Precende y DSCP como se muestra a continuación:

Tipo de tráfico	Marcaje	
Voz	EF	Dscp ef
Datos críticos empresariales	Clase 4	Precedence 4
Datos de Administración	Clase 3	Precedence 3
Datos Generales	Clase 2	Precedence 2
Best effort (Scavenger)	Clase 1	Precedence 1

Tabla 12: Marcaje de tráfico

Como se puede observar en la tabla 12 tiene mayor prioridad el tráfico de Voz que se lo marca DSCP ef (códigos de marcaje) que también lo asigna la RFC 2598/3246 para que el usuario final pueda recibir adecuadamente la transmisión y no se degrade la conversación.

Para datos críticos que tiene una empresa se usará Precendence 4, para datos de administración se usará Precedence 3 donde están los protocolos de enrutamiento, para datos generales se usará Precedence 2 donde están datos como traceroute y ping, para Scavenger (tráfico perjudicial a la red como Videos) llamado Best Effort se usará Precende 1 que es la prioridad más baja en la red.

Se considerará que la marca que coloque el cliente se mantenga en el proveedor para asegurar la calidad de servicio contratado, teniendo ventajas y desventajas por ejemplo como ventaja un ancho de banda contratado no permitirá pérdida de paquetes y no habrá reenvió de paquetes.

Una de las desventajas es el costo para la empresa, pero considerando que la empresa tiene un tiempo de vida entre 5 a 10 años y es una empresa consolidada podrá pagar este servicio, a diferencia de contratar el servicio donde el proveedor impone su marca cuando llega el tráfico del cliente por lo que el servicio que cobra es más barato debido a que no hay aseguramiento de la calidad al cien por ciento porque el proveedor tiene el control del tráfico que ingresa.

Es así que si el proveedor considera que excede el tráfico contratado descartará los paquetes produciéndose mucha latencia o reenvíos de paquetes en la red que a la larga puede terminar en desventaja para la empresa porque tendría que pagar más para que sus paquetes vayan del origen al destino.

Programación:

```
class-map match-any CLASE-GENERAL      ! Creación de la clase GENERAL
 match  precedence 1
class-map match-any CLASE-VOZ          ! Creación de la clase VOZ
 match  dscp ef
class-map match-any CLASE-DATOS        ! Creación de la clase DATOS
 match  precedence 2
class-map match-any CLASE-ADMIN        ! Creación de la clase ADMINISTRACION
 match  precedence 3
class-map match-any CLASE-CRITICO      ! Creación de la clase CRÍTICO
 match  precedence 4
```

Figura 49: Programación de las clases

Como se observa en la figura 49 se da la programación de la creación de clases para Voz, datos , Administración, datos generales y datos críticos.

```
policy-map QOS                  ! Se usa para remarcar el tráfico que sale hacia la red
class CLASE-VOZ
set dscp ef
priority percent 15
class CLASE-CRITICO
set precedence 4
priority percent 20
class CLASE-ADMIN
set precedence 3                ! remarcado a precedence 3
priority percent 10
class CLASE-DATOS
set precedence 2                ! remarcado a precedence 2
priority percent 10
class CLASE-GENERAL
priority percent 5
class class-default             ! El resto de tráfico es remarcado como default,
                                  es la prioridad mas baja y se le da un
                                  tratamiento best effort
```

Figura 50: Programación del remarcado

Como se puede observar en la figura 50 se realizó la programación de la remarcación tomando en cuenta que en Diffserv la marcación del tráfico es lo más cerca posible a la fuente, sin embargo ciertos tipos de tráfico como voz y video tienen que ser remarcados antes de pasar al proveedor de servicios.

Para el envío correcto del tráfico se recomienda que este remarcado se realice en el borde de salida de la CE no dentro del campus MATRIZ, esto se debe a que los servicios que ofrecen los proveedores de servicio evolucionan o se expanden a través del tiempo y una manera fácil de ajustarse a estos cambios es el remarcado solo en el borde del CE.

Comandos de verificación y consulta (Show)

Show class-map

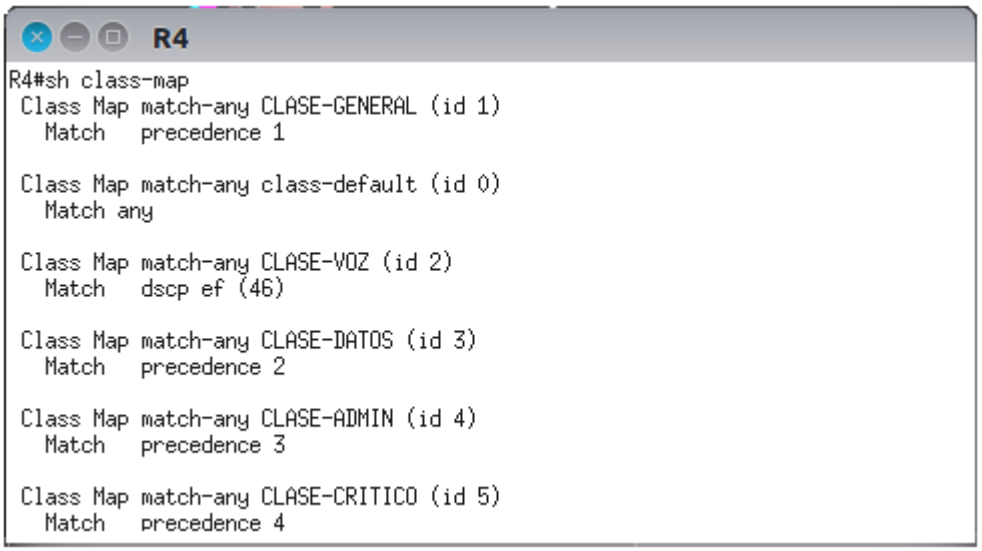


Figura 51: Verificación de la creación de las clases

Como se puede observar en la figura 51 se verifica todas las clases que se han creado en el router de frontera del área Matriz, se puede constatar que la prioridad más alta es la clase crítica y la más baja es la clase por defecto que es class-default.

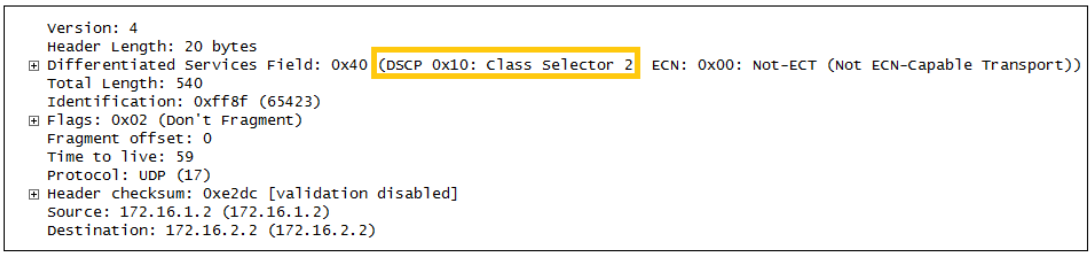


Figura 52: Verificación del class selector

Se puede observar en la figura 52 que al usar la herramienta Wireshark en el CE (R4) el seteo del class selector es 2 cuando se envía el paquete a través del inyector de tráfico con el protocolo UDP.

Aplicación de la política

```
interface Serial0/0
ip address 192.168.12.18 255.255.255.252
clock rate 2000000
service-policy output QOS
```

Figura 53: Programación de la política

Como se puede observar en la figura 53 se programa los policy-map cuando sale el tráfico, esto se lo realiza en la interfaz serial del router CE.

Comandos de verificación y consulta (Show)

Show policy-map

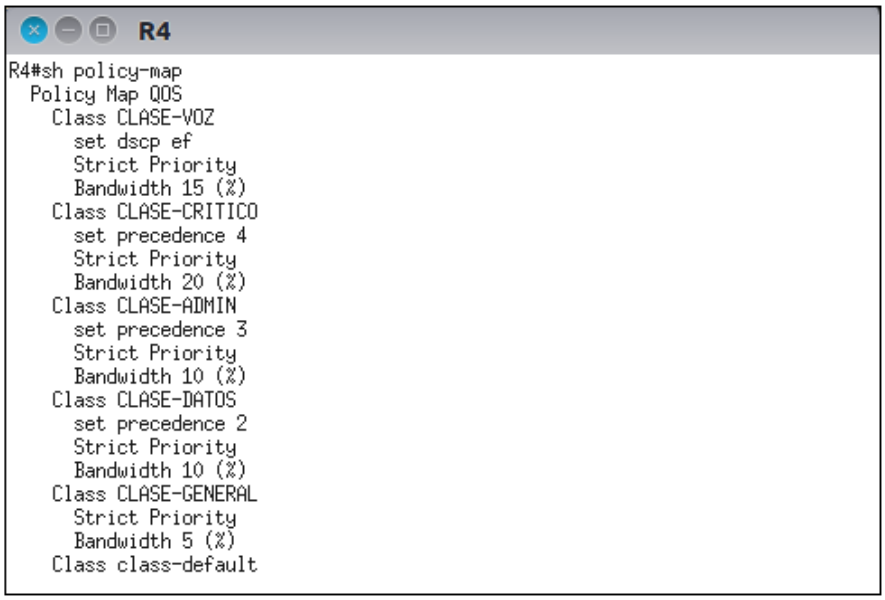


Figura 54: Verificación de las políticas

Se puede observar en la figura 54 todos los policy-maps que se tiene, como se setea la política en cada clase como por ejemplo el ancho de banda mas alto asignado a clase crítica para datos críticos que en este caso es el 20% del ancho de banda total, adicionalmente la prioridad alta que se le da a la misma.

4.8.3 MPLS DIFFSERV

Debido a que las etiquetas MPLS se componen de 3 bits que se utilizan para el marcado QoS, es posible crear un Túnel DiffServ que preserva las marcas en capa 3 a través de la nube del proveedor VPN MPLS, al mismo tiempo hace la realización de remarcado a través de los bits MPLS-EXP para indicar si el tráfico está dentro o fuera del contrato.

Aplicación:

```
policy-map EXP-GROUP
 class class-default
  set qos-group mpls experimental topmost
policy-map MPLS-EXP-A-Q0S-GROUP
 class class-default
  set qos-group mpls experimental topmost
policy-map QOS-GROUP-A-PRECEDENCE
 class class-default
  set precedence qos-group
```

Figura 55: Programación del remarcado

Como se puede observar en la figura 55 en el PE (R3) previamente programadas las marcas, nos aseguramos que la marca del IP precedence del cliente sea copiado al campo experimental del otro extremo de la VPN MPLS para lo cual en el PE (R3) se crea un grupo que para nuestro caso es EXP-GROUP.

Aplicamos la política con el comando policy-map EXP-GROUP, luego se copia las políticas con el comando policy-map MPLS-EXP-A-QOS-GROUP y policy-map QOS-GROUP-A-PRECEDENCE.

Activación en las interfaces PE (R3):

```
interface Serial0/0
service-policy input EXP-GROUP
interface Serial0/1
service-policy output QOS-GROUP-A-PRECEDENCE
interface Serial0/2
service-policy input EXP-GROUP
```

Figura 56: Programación para activación de la interface

Se puede observar en la figura 56 la aplicación de las políticas a las interfaces manteniendo la marca tanto para el tráfico que entra como para el tráfico que sale por la interface.

4.9 INSTRUMENTOS DE MEDICIÓN PARA LA RED

Se utilizaran los siguientes instrumentos de medición para poder evaluar la calidad de servicio:

Wireshark 

: Es una herramienta multiplataforma para el análisis de la red, funciona al igual que lo hace cualquier snniffer como Windump. Esta herramienta muestra los datos en un entorno gráfico más amigable y entendible, con el que podemos capturar paquetes, filtrar información relevante, análisis de paquetes donde se ve anomalías de la red e interpretar errores.

.

D-ITG: Esta herramienta que trabaja bajo el modelo Cliente-Servidor, permite realizar mediciones de desempeño y simulación de tráficos con protocolos diferentes, tiene la ventaja de ser una plataforma de código abierto que permite la generación de tráfico de Datos y cálculos de retardos en un solo sentido (OWD-One Way Delay) e ida y vuelta (RTT-Round Trip Time).

A través del D-ITG se genera tráfico real de Datos, Streamming y VoIP con los códec G.711, G.729 y G.723.1, permitiendo analizar parámetros de calidad de servicio como latencia, jitter y perdida de paquetes que son emitidos como respuesta al terminar el proceso de inyección de tráfico.
Los componentes del D-ITG son como se muestra en la figura:

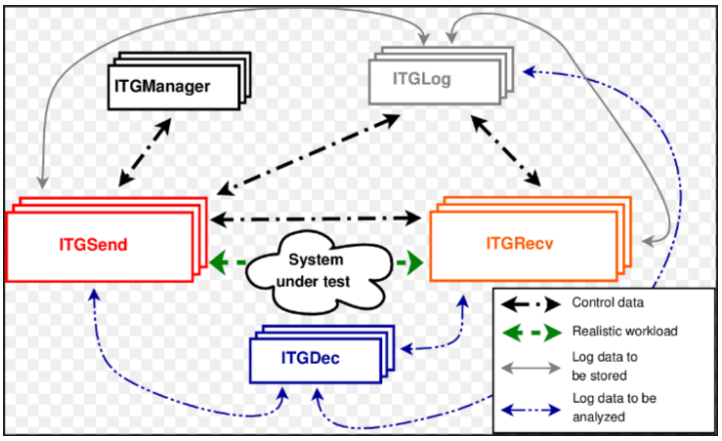


Figura 57: Arquitectura del D-ITG

Como se observa en la figura 57 el componente ITGSend es responsable de generar el tráfico hacia ITGRecv, estos componentes producen el archivo log (ITGLog) donde se detalla la información de los paquetes de cada envío y recepción, el componente ITGRecv actúa como un deamons y puede estar completamente configurado y controlado por ITSend.

ITGDec es el componente encargado de analizar los archivos de registro con el fin de extraer los parámetros de rendimiento relacionados con los flujos de tráfico.

4.10 PROCESO PARA LA EVALUACIÓN DE LA CALIDAD DE SERVICIO.

Primeramente se darán los parámetros adecuados para el tráfico de acuerdo a los estándares internacionales y luego procederemos a indicar el proceso para la inyección del tráfico donde se observara donde se aplica el TOS, dentro del escenario de prueba.

4.10.1 PARÁMETROS DE ACUERDO A LOS ESTÁNDARES

LATENCIA (RETARDO)

La latencia o retardo es la demora o tiempo que se tarda un paquete en transferirse de un origen a un destino, de acuerdo a estándares o recomendaciones de la UIT-T G.1010, Y 1541 y la IEEE 8021.1p que definen los parámetros que evaluan la calidad de servicio, teniendo la siguiente tabla.

Clase de calidad de servicio	Descripción	Umbral de retardo internacional (ms)
0	Tiempo real, alta interacción, sensible al retardo (Voz y Video en tiempo real)	100
1	Tiempo real, interactivo, sensible al retardo (Voz y Video en tiempo real de menor calidad)	150
2	Datos de alta prioridad (transaccionales altamente interactivos)	200
3	Datos de mediana prioridad (Datos transaccionales interactivos)	225
4	Datos de baja prioridad (transacciones cortas, datos en grandes cantidades, flujo continuo de video streamming)	250
5	Datos de mejor esfuerzo	300

Tabla 13: Valoraciones de Retardo[42]

De lo considerado el retardo máximo que sufre en flujo continuo de video streaming es de 250ms porque cuando comienza a conversar el usuario A al no escuchar al usuario B comienzan hablar simultáneamente.

En base a los valores anteriores se obtiene la siguiente tabla:

Tráfico	Excelente	Muy Bueno	No Adecuado
VoIP	<100ms	>100ms y <150ms	>150ms
Datos	< 250ms	>250ms y <300ms	>300ms
Streaming	<=100 ms	>100ms y <=250ms	> 250ms

Tabla 14: Valoraciones cualitativa de Latencia (Retardo) [43]

[42] Tomado de (Buñay Guisñay, 2013), Estándares de la UIT-T, G.1010, Y 1541 y la IEEE 802.1p

[43] Tomado de (Buñay Guisñay, 2013), Estándares de la UIT-T, G.1010, Y 1541 y la IEEE 802.1p

Como se puede observar la transmisión es adecuada para valores menores a 100ms de acuerdo a los estándares de UIT-T G.1010, Y 1541 y la IEEE 8021.1p.

JITTER

Debido al retardo que se produce en los flujos de datos se genera un problema llamado jitter que aparece por congestión en la red, especialmente por una incorrecta sincronización de bits entre los elementos de red.

La tabla de los umbrales máximos de Jitter según las recomendaciones UIT-T, G.1010, Y.1541 y la IEEE 802.1p (Buñay Guisñay, 2013) es:

Clase de calidad de servicio	Descripción	Umbral de Jitter internacional (ms)
0	Tiempo real, alta interacción, sensible al retardo (Voz y Video en tiempo real)	45
1	Tiempo real, interactivo, sensible al retardo (Voz y Video en tiempo real de menor calidad)	50
2	Datos de alta prioridad (transaccionales altamente interactivos)	55
3	Datos de mediana prioridad (Datos transaccionales interactivos)	N/A
4	Datos de baja prioridad (transacciones cortas, datos en grandes cantidades, flujo continuo de video streamming)	N/A
5	Datos de mejor esfuerzo	N/A

Tabla 15: Valoraciones de Jitter[44]

[44] Tomado de (Buñay Guisñay, 2013), Estándares de la UIT-T, G.1010, Y 1541 y la IEEE 802.1p

En base a los valores anteriores se obtiene la siguiente tabla:

Tráfico	Excelente	Muy Bueno	No Adecuado
VoIP	<40ms	>40ms y <50ms	>50ms
Datos	< 55ms	>55ms y <70ms	>70ms
Streaming	<=35 ms	>35ms y <=65ms	> 65ms

Tabla 16: Valoraciones cualitativa de Jitter[45]

Como se puede observar en la tabla 16 la transmisión es adecuada para valores menores a 35ms de acuerdo a los estándares de UIT-T G.1010, Y 1541 y la IEEE 8021.1p.

PÉRDIDA DE PAQUETES

Para las comunicaciones en tiempo real con servicios como Streaming que se basan en el protocolo UDP que es un protocolo que no está orientado a conexión, muchas veces se produce pérdida de paquetes que no se reenvían, porque hay un descarte de paquetes que no llegan a tiempo al receptor, para los datos de muestra no hubo pérdida de paquetes.

Tomando las referencias de las recomendaciones UIT-T G.1010, Y. 1541 y la IEEE 802.1p se establecen los umbrales máximos de pérdida de paquetes.

[45] Tomado de (Buñay Guisñay, 2013), Estándares de la UIT-T, G.1010, Y 1541 y la IEEE 802.1p

Clase de calidad de servicio	Descripción	Umbral de Jitter internacional (ms)
0	Tiempo real, alta interacción, sensible al retardo (Voz y Video en tiempo real	1%
1	Tiempo real, interactivo, sensible al retardo (Voz y Video en tiempo real de menor calidad)	3%
2	Datos de alta prioridad (transaccionales altamente interactivos)	3%
3	Datos de mediana prioridad (Datos transaccionales interactivos)	5%
4	Datos de baja prioridad (transacciones cortas, datos en grandes cantidades, flujo continuo de video streamming)	5%
5	Datos de mejor esfuerzo	5%

Tabla 17: Valoraciones cualitativa de Pérdida de paquetes[46]

En base a los valores anteriores se obtiene la siguiente tabla:

Tráfico	Excelente	Muy Bueno	No Adecuado
VoIP	<1%	>1% y <3%	>3%
Datos	< 3%	>3% y <5%	>5%
Streaming	<=2%	>2% y <=5%ms	> 5%

Tabla 18: Valoraciones cualitativa de Pérdida de paquetes[47]

[46] Tomado de (Buñay Guisñay, 2013), Estándares de la UIT-T, G.1010, Y 1541 y la IEEE 802.1p

[47] Tomado de (Buñay Guisñay, 2013), Estándares de la UIT-T, G.1010, Y 1541 y la IEEE 802.1p

Como se puede observar la transmisión es adecuada para valores menores a 1% de acuerdo a los estándares de UIT-T G.1010, Y 1541 y la IEEE 8021.1p.

4.10.2 CONFIGURACIÓN DEL D-ITG PARA LA INYECCIÓN DE TRÁFICO.

Se necesita configurar al emisor y al receptor como se muestra a continuación.

Configuración del Emisor

En la configuración del Emisor se debe configurar las pestañas Define flow y Setting.

Define Flow:

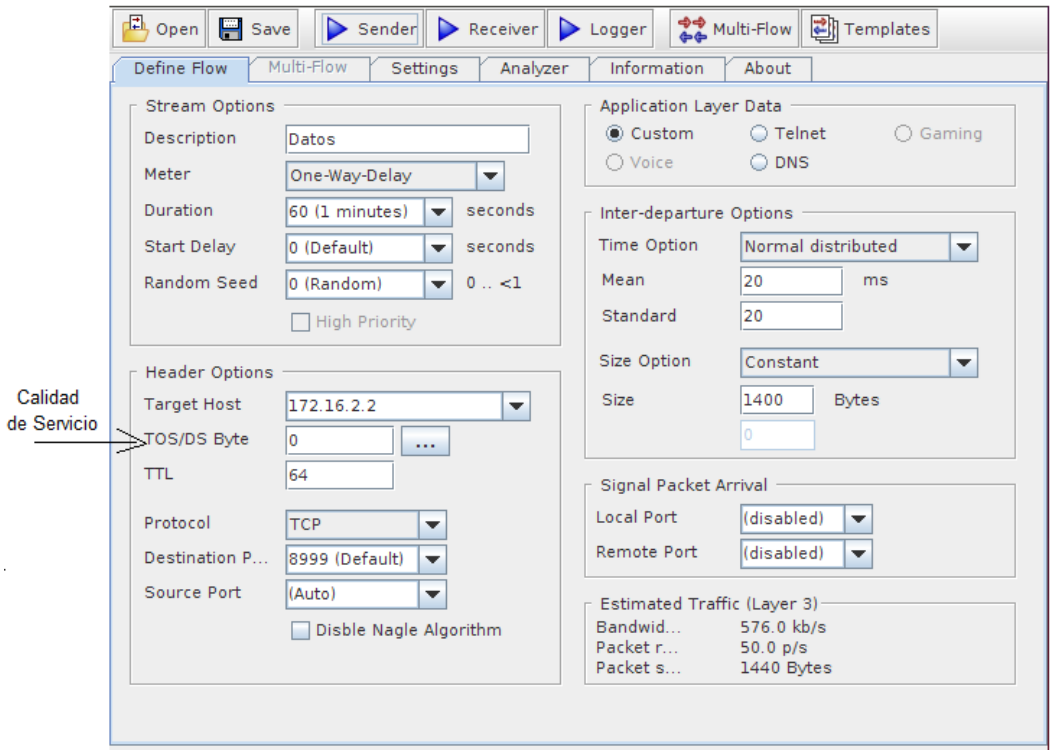


Figura 58: Configuración del Emisor – Define Flow

Se observa en la figura 58 los diferentes campos del emisor donde los más importantes son el *Meter* que es el tipo de transmisión, el tiempo de transmisión (duration), el tipo de dato (application layer data), el tamaño del

paquete y el TOS (Tipo de servicio) que sirve para analizar los parámetros de calidad de servicio, en estimación de tráfico se puede observar con este software que da el ancho de banda requerido y el número de paquetes por segundo.

Setting

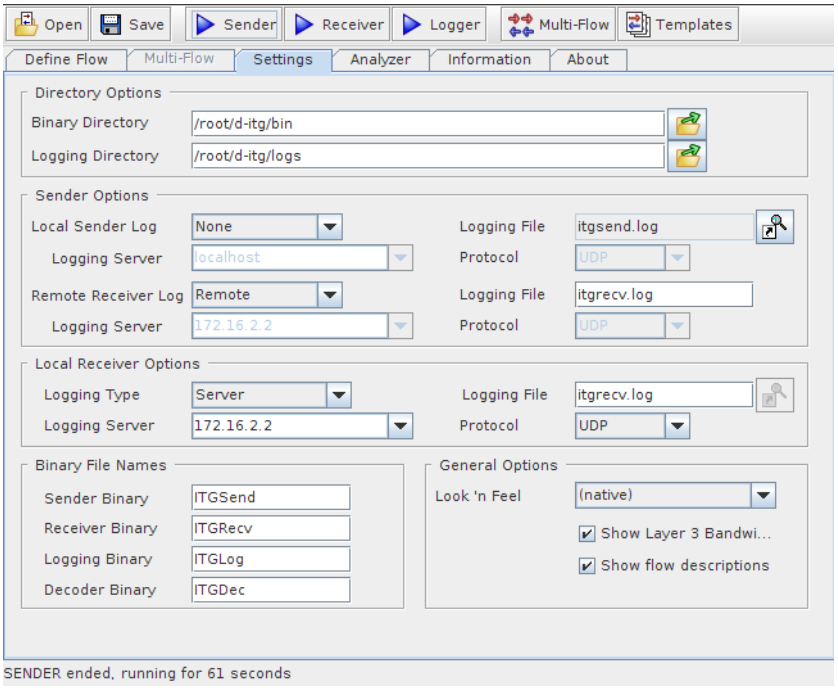


Figura 59: Configuración del Emisor - Setting

En la figura 59 se observa la configuración del setting donde lo importante es colocar la ip del receptor y el nombre del archivo ***.log*** donde se recepta la información para el análisis de tráfico

Verificación del envió:

```
SENDER_STARTING: bin/ITGSend -x itgrecv.log -a 172.16.2.2 -T TCP -t 60000 -U 1000 2000 -n 1400 0
SENDER_MESSAGE: ITGSend version 2.8.1 (r1023)
SENDER_MESSAGE: Compile-time options: bursty multiport
SENDER_MESSAGE: Started sending packets of flow ID: 1
SENDER_MESSAGE: Finished sending packets of flow ID: 1
```

Figura 60: Verificación del envío

Se puede observar en la figura 60 el flujo de envío del tráfico del emisor con los parámetros previamente seteados.

Configuración del Receptor

```
sudo –
cd d-itg
/d-itg/bin# ./ITGRecv
```

Figura 61: Configuración del receptor

Se puede observar en la figura 61 la configuración para activar el inyector de tráfico en modo receptor.

Verificación de la activación

```
root@miroslava-VirtualBox:~/d-itg# cd bin
root@miroslava-VirtualBox:~/d-itg/bin# ./ITGRecv
ITGRecv version 2.8.1 (r1023)
Compile-time options: bursty multiport
Press Ctrl-C to terminate
Listening on TCP port : 8999
Finish on TCP port : 8999
```

Figura 62: Verificación del Receptor

Se observa en la figura 62 que el puerto 8999 está escuchando en espera de los paquetes del transmisor.

Generación del archivo log

```
root@miroslava-VirtualBox:~/d-itg/bin# mv itgrecv.log Prueba-datos.log
root@miroslava-VirtualBox:~/d-itg/bin# ls
ITGDec  ITGLog  ITGManager  ITGRecv  ITGSend  libITG.so  Prueba-datos.log
root@miroslava-VirtualBox:~/d-itg/bin# ITGDec Prueba-datos.log
root@miroslava-VirtualBox:~/d-itg/bin# ./ITGDec Prueba-datos.log
```

Figura 62: Generación del archivo .log

Como se puede observar en la figura 62 se generó el archivo Prueba-datos.log donde se encuentran en forma transparente los parámetros de jitter, delay, bit rate y packet loss.

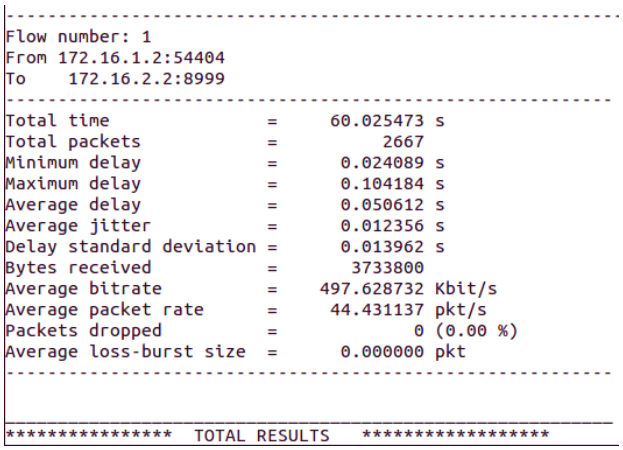


Figura 63: Visualización del archivo prueba-datos.log

Se puede observar en la figura 63 que al enviar el flujo de datos del Transmisor al Receptor los parámetros detallados del bit rate, jitter, delay y packet loss para el análisis del tráfico.

Generación de los parámetros para analizar el tráfico.

La generación de los archivos .dat se lo realiza a través del siguiente formato:

- Para bit rate –b
- Para delay –d
- Para jitter –j
- Para packetloss –p.

El comando para ejecutar estos parámetros es:

/.ITGDec [log_name] –b 500 -d 500 -p 500 –j 500

Ejemplo:

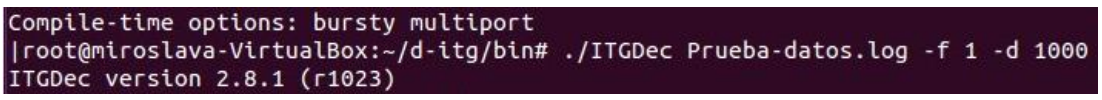


Figura 64: Generación del parámetro delay.dat

Se puede observar en la figura 64 el formato bajo Linux para generar el archivo delay.dat para un flujo de datos cada 1000 ms.

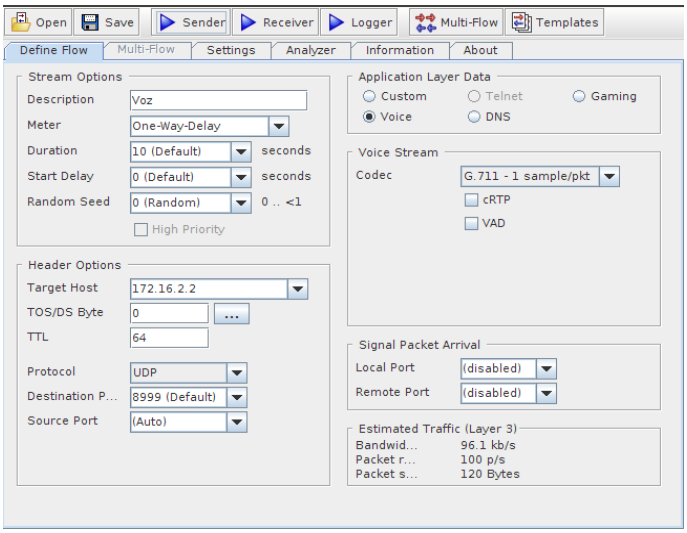
En el **Anexo 2** se encuentran en forma detallada todos los elementos del D-ITG.

4.11 OBTENCION DE DATOS SIN MECANISMO QoS

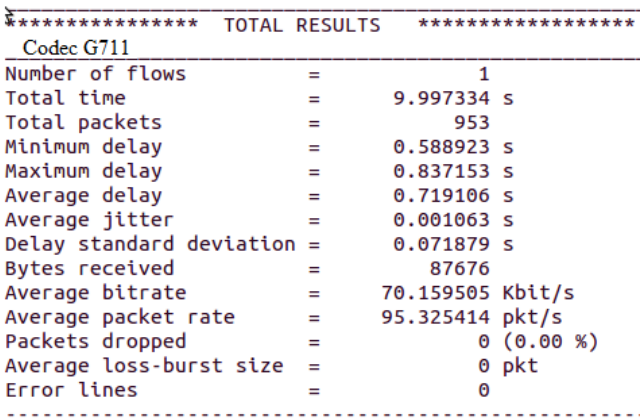
En el escenario de prueba se procede a trabajar tres tipos de tráfico que son VoIP, Streaming y Datos, primeramente se activa en las máquinas virtuales el generador de tráfico D-ITG y luego se inyecta tráfico como se muestra a continuación.

4.11.1 VOZ

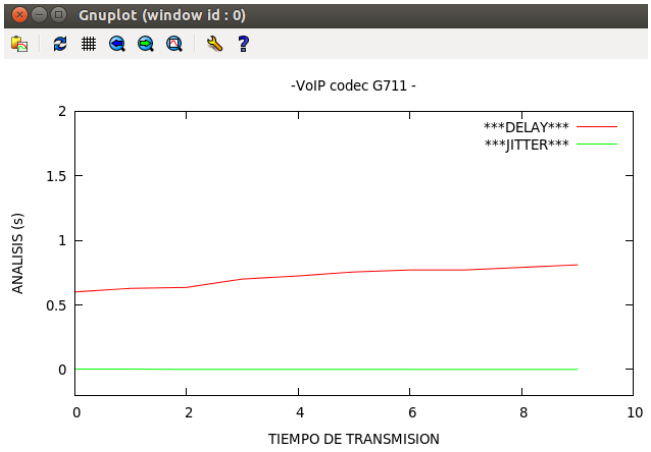
CODEC G711



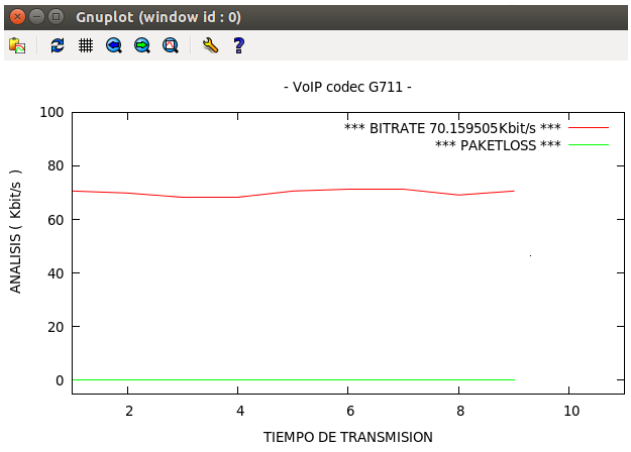
a)



b)



c)



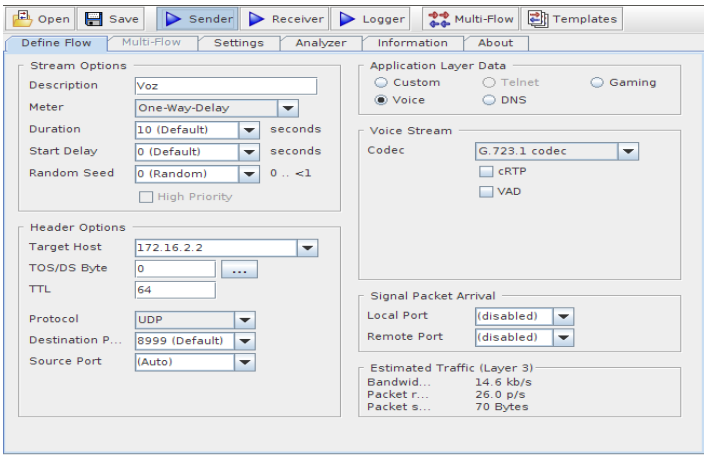
d)

Figura 65: VoIP Codec G711 a) Inyector de tráfico TX b) Resultados en el receptor c) gráficas de delay y jitter d) gráfica de bit rate y packetloss

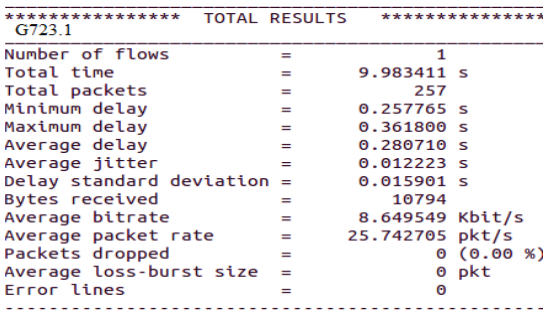
Se puede observar en la figura 65 las características del tráfico de Voz bajo el códec G711, el retardo (delay) obtenido es 719 ms que de acuerdo a las recomendaciones de la UIT-T G.1010, Y 1541 y la IEEE 8021.1p es alto lo que implicaría que cuando el usuario del transmisor esta hablando el usuario receptor no se entera y la transmisión es lenta.

En lo que se refiere al jitter de acuerdo a las recomendaciones están en los valores aceptados que deben ser menores a 100ms para este caso al receptor llega en 10ms, adicionalmente no existen packet perdidos en la simulación de tráfico de voz porque no se envío grandes volumenes de tráfico en el transmisor.

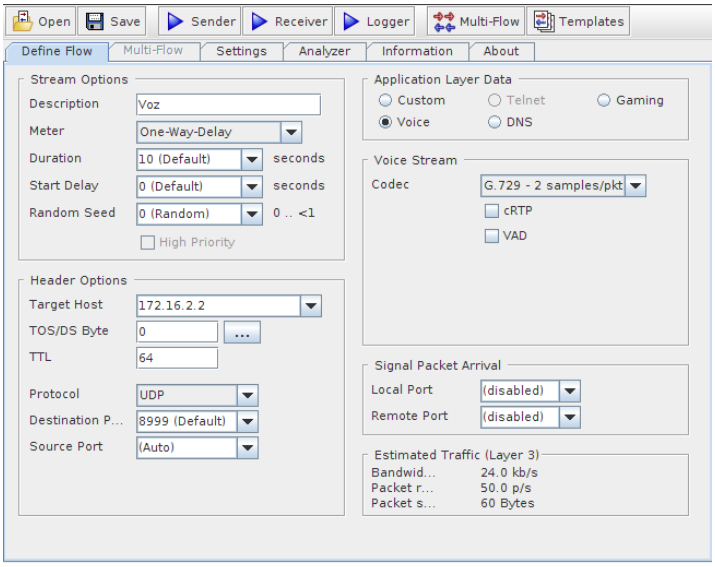
VOZ CODEC G723.1 G729-2



a)



b)



c)

```
**********  TOTAL RESULTS   **********
G729-2
----------------------------------------------------
Number of flows          =            1
Total time               =     9.985926 s
Total packets            =          490
Minimum delay            =     0.263724 s
Maximum delay            =     0.357237 s
Average delay            =     0.292589 s
Average jitter           =     0.008587 s
Delay standard deviation =     0.015576 s
Bytes received           =        15680
Average bitrate          =    12.561679 Kbit/s
Average packet rate      =    49.069060 pkt/s
Packets dropped          =            0 (0.00 %)
Average loss-burst size  =            0 pkt
Error lines              =            0
----------------------------------------------------
```

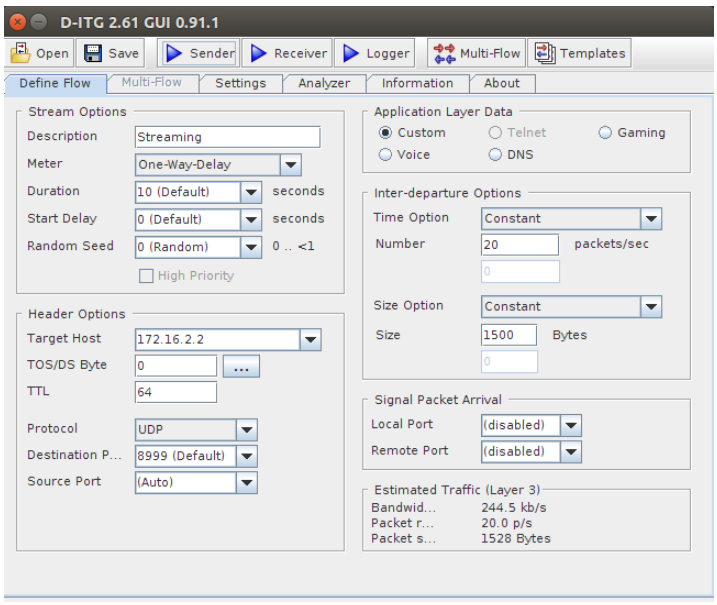
d)

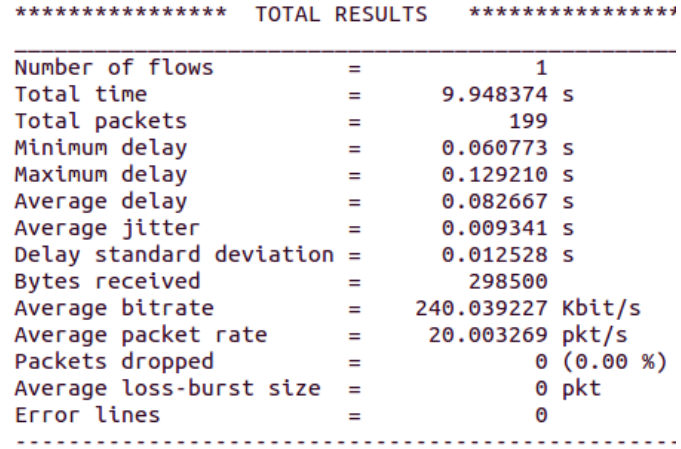
Figura 66: VoIP a) Inyector de tráfico TX códec G723.1 b) Resultados en el receptor c) Inyector de tráfico TX códec G729.2 d) Resultados en el receptor

Se puede observar en la figura 66 la inyección de tráfico de los códec G723.1 y G729.2, comparando con la figura 65 que de los tres códec en la transmisión de tráfico de voz sin mecanismo de calidad de servicio el que tiene menor delay es el codec G723-2 con un delay promedio de 280ms que es alto para los estandáres adecuados de acuerdo a las recomendaciones de la UIT-T G.1010, Y 1541 y la IEEE 8021.1p de transmisión que debe ser menor de 100ms lo que va producir retardo en la recepción

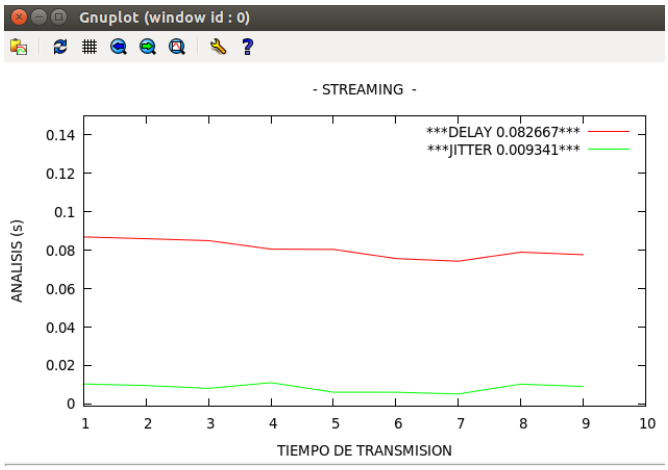
En el caso del jitter están en los rangos aceptables que deben ser menores a 40ms, de lo analizado el mejor códec para este parámetro es el G729-2 y para el parámetro de bit rate el codec mas adecuado es el G711 con un velocidad de 70.159Kbits/s.

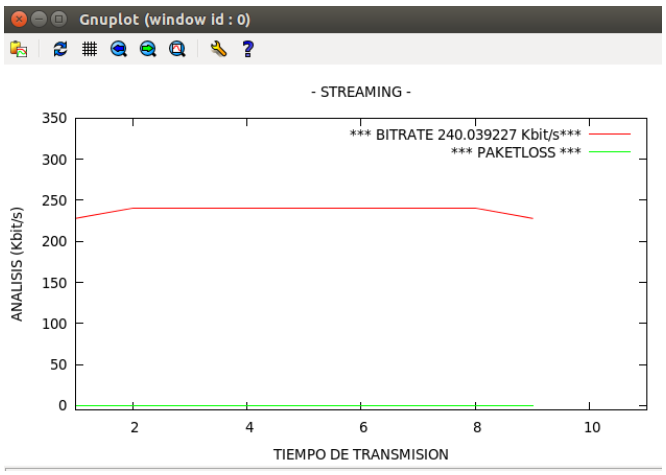
4.11.2 STREAMING





a) b)



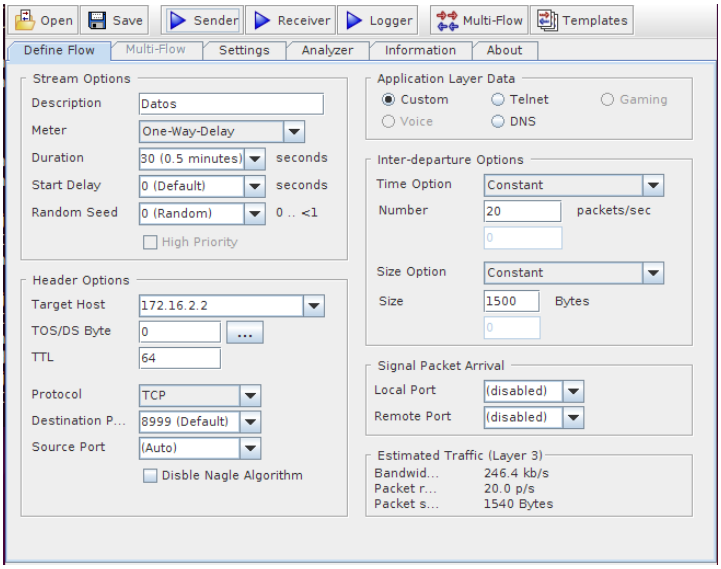


c) d)

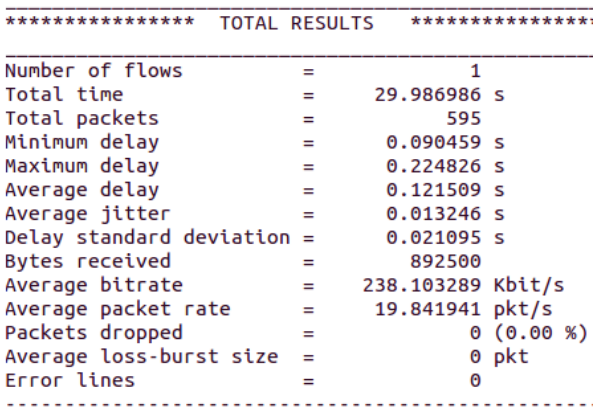
Figura 67: Streaming a) Inyector de tráfico TX b) Resultados en el receptor c) gráficas de delay y jitter d) gráfica de bitrate y packetloss

Como se puede observar en la figura 67 para tráfico de streaming se trabajará con 20 paquetes y cada paquete con un tamaño de 1500bytes usando protocolo UDP requiriendo un ancho de banda de 244.5 Kbits y proporcionando un retardo promedio de 82 ms que de acuerdo a las recomendaciones de la UIT-T G.1010, Y 1541 y la IEEE 8021.1p estaría en los rangos aceptables de delay, jitter y bitrate.

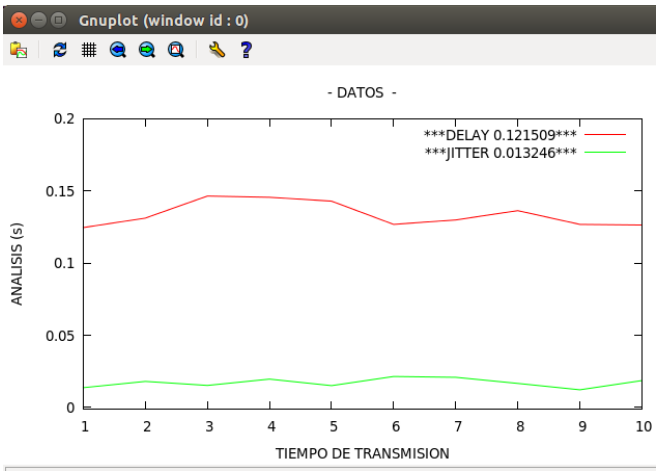
4.11.3 DATOS



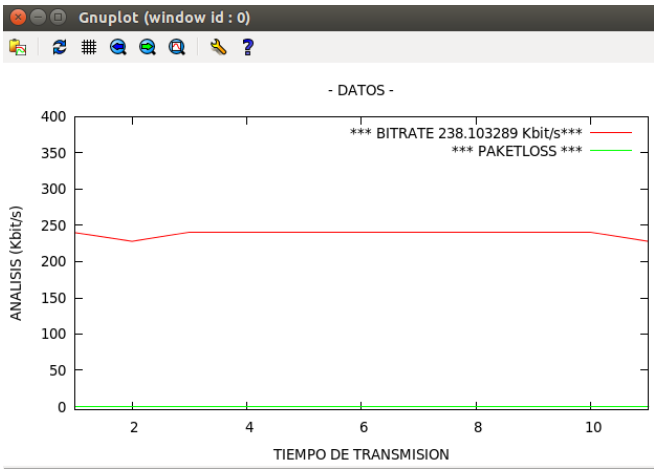
a)



b)



c)



d)

Figura 68: Datos a) Inyector de tráfico TX b) Resultados en el receptor c) gráficas de delay y jitter d) gráfica de bitrate y packetloss

Como se puede observar en la figura 68 para el tráfico de datos se trabajará con 20 paquetes y cada paquete con un tamaño de 1500bytes con protocolo TCP requiriendo un ancho de banda de 246,4 Kbits proporcionando un retardo promedio de 121 ms que sobrepasa los rangos aceptables de acuerdo a las recomendaciones de la UIT-T G.1010, Y 1541 y la IEEE 8021.1p que indican que para una buena recepción debe ser menor a 100ms, mientras que para jitter estaría en los rangos aceptables.

4.12 OBTENCION DE DATOS APLICANDO DIFFSERV.

Para mejorar la transmisión se utilizará el mecanismo de DiffServ donde se realizará la diferenciación y priorización del tráfico, manejandose la siguiente tabla:

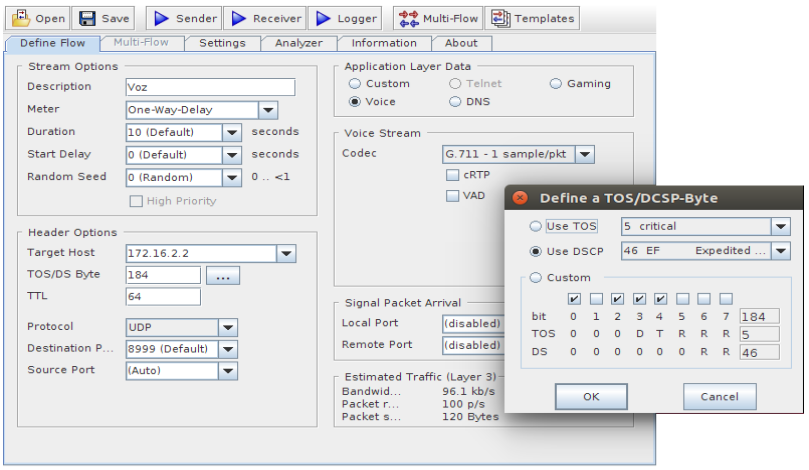
Tipo de Tráfico	ToS Bits Precedence	Traffic Generator QoS (PHB)	Valores QoS (DSCP) Traffic Generator	DiffServ IP precedence	AB
Voz	**101 11000**	Dscp ef	ef		15%
D. críticos Streaming	**100 00000**	CS4	32	4	20%
D. de Admin Datos	**011 00000**	CS3	24	3	10%
D. Gen.	**010 00000**	CS2	16	2	10%
Best effort Scavenger	**001 00000**	CS1	8	1	5%

Tabla 19: Valoraciones para la calidad de Sevicio con los tipos de tráfico

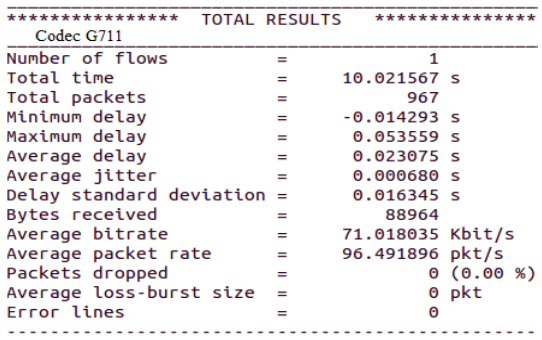
Como se puede observar en la tabla 19 estos valores se colocaron en el software D-ITG para manejar calidad de servicio con el mecanismo DiffServ tanto con Dscp como con IP precende. El PHB (Per Hop Behavoir) es el que denota una combinación de comportamientos de reenvíos, clasificación, planificación y descarte en cada salto de paquetes pertenecientes a un mismo ancho de banda (AB) en la red, adicionalmente proporciona una cantidad dada de los recursos de la red garantizando calidad de servicio en los diferentes tipos de tráfico.

4.12.1 VOZ - CODEC G711

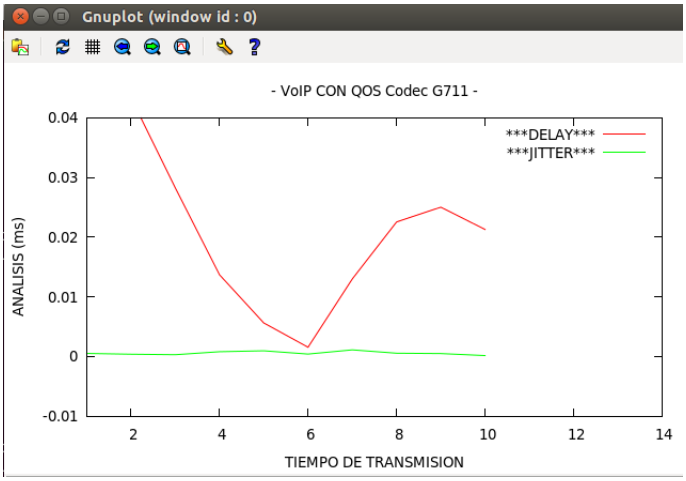
Como se dijo anteriormente para Voz se maneja diferentes Codec a continuación se muestra la gráfica para el códec G711 aplicando el mecanismo DiffServ.



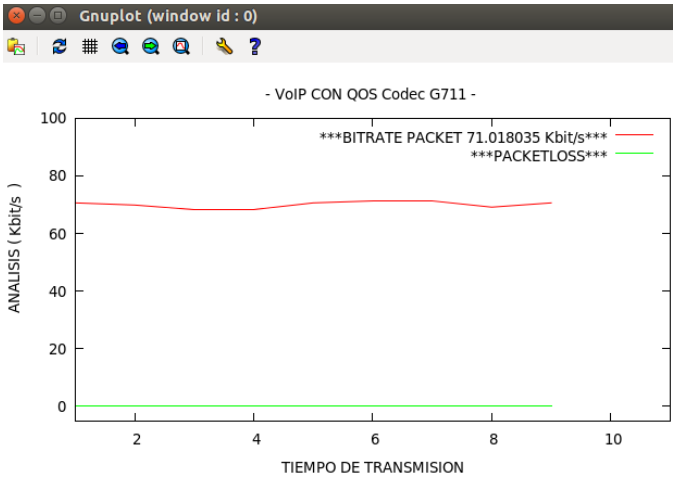
a)



b)



c)



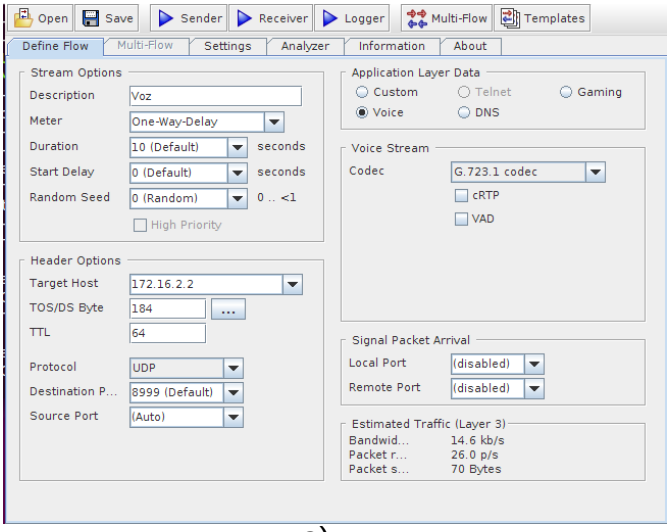
d)

Figura 69: VoIP Codec G711 a) Inyector de tráfico TX b) Resultados en el receptor c) gráficas de delay y jitter d) gráfica de bitrate y packetloss

Se puede observar en la figura 69, que aplicando el mecanismo de DiffServ en los router y en el inyector D-ITG con el DSCP en EF para VoIP con el códec G711, el delay que se tiene esta en un promedio de 20ms que

es una transmisión permitida para que el receptor reciba una transmisión adecuada, igualmente para los parámetros de jitter y bitrate son muy adecuados de acuerdos a los valores permitidos que deben ser menores a 40ms para el caso del jitter de acuerdo a las recomendaciones de la UIT-T G.1010, Y 1541 y la IEEE 8021.1p.

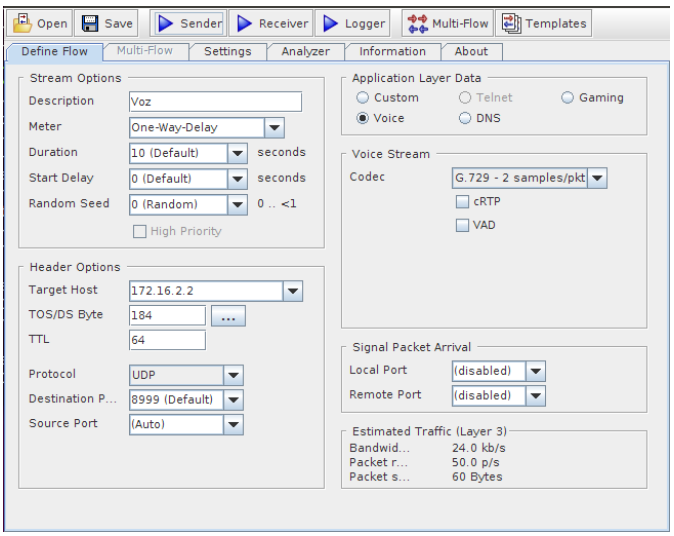
VOZ CODEC G723.1 G729-2



a)

```
**********  TOTAL RESULTS  **********
 Codec G.723.1
------------------------------------------------------
Number of flows          =            1
Total time               =     9.993484 s
Total packets            =          257
Minimum delay            =    -0.005136 s
Maximum delay            =     0.061601 s
Average delay            =     0.008509 s
Average jitter           =     0.008523 s
Delay standard deviation =     0.009194 s
Bytes received           =        10794
Average bitrate          =     8.640830 Kbit/s
Average packet rate      =    25.716757 pkt/s
Packets dropped          =            0 (0.00 %)
Average loss-burst size  =            0 pkt
Error lines              =            0
------------------------------------------------------
```

b)



c)

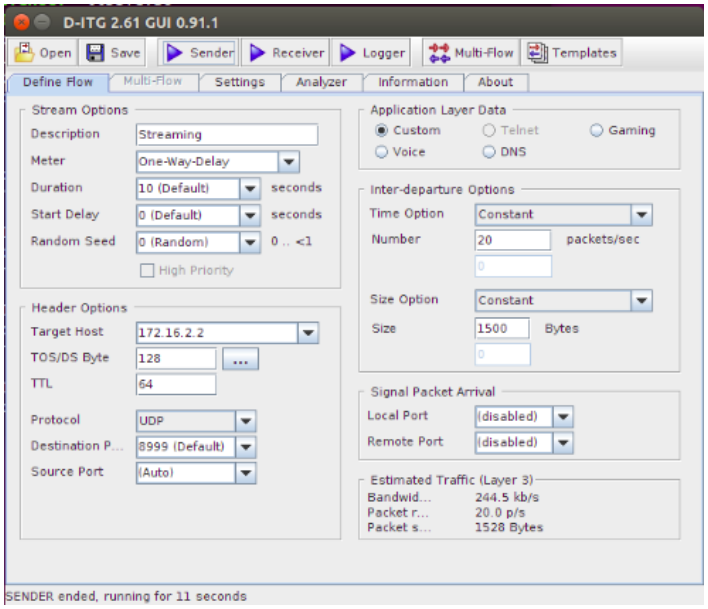
```
**********  TOTAL RESULTS  **********
 G.729-2
------------------------------------------------------
Number of flows          =            1
Total time               =     9.986965 s
Total packets            =          489
Minimum delay            =    -0.007589 s
Maximum delay            =     0.053521 s
Average delay            =     0.010302 s
Average jitter           =     0.006706 s
Delay standard deviation =     0.011280 s
Bytes received           =        15648
Average bitrate          =    12.534739 Kbit/s
Average packet rate      =    48.963824 pkt/s
Packets dropped          =            0 (0.00 %)
Average loss-burst size  =            0 pkt
Error lines              =            0
------------------------------------------------------
```

d)

Figura 70: a) Inyector de tráfico TX códec G723.1 b) Resultados en el receptor c) Inyector de tráfico TX códec G729-2 d) Resultados en el receptor

Se observa en la figura 70 y comparando con la figura 69 que aplicando el mecanismo de Diffserv para los tres códec en delay da mejor respuesta el códec G723-1 al tener 8 ms que es menor a 100ms de acuerdo a las recomendaciones de la UIT-T G.1010, Y 1541 y la IEEE 8021.1p y en jitter el códec G729-2 es el que da mejor respuesta con 6ms que es un rango aceptable en la transmisión que debe ser menor a 40ms.

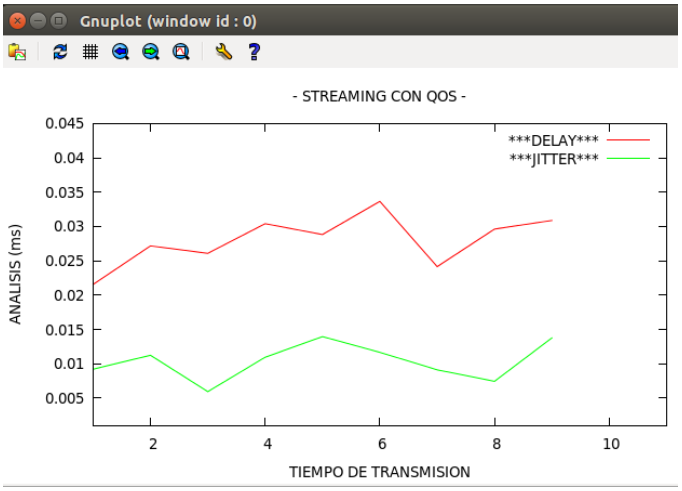
4.12.2 STREAMING



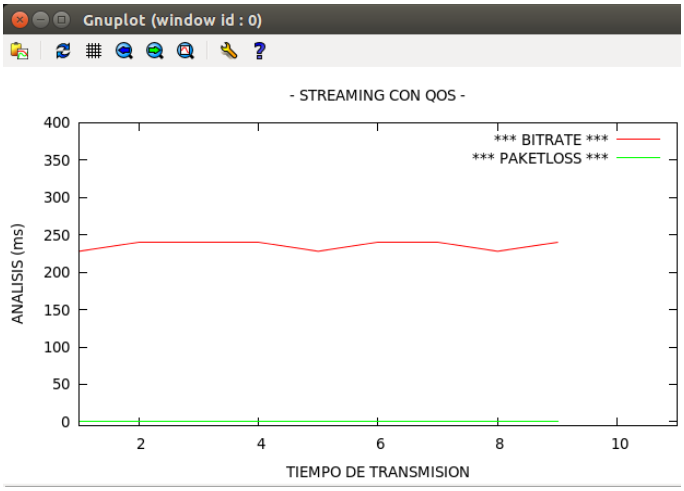
a)

```
************  TOTAL RESULTS  ************
Number of flows          =          1
Total time               =   9.935801 s
Total packets            =        198
Minimum delay            =   0.008346 s
Maximum delay            =   0.072002 s
Average delay            =   0.027420 s
Average jitter           =   0.010085 s
Delay standard deviation =   0.011593 s
Bytes received           =     297000
Average bitrate          = 239.135224 Kbit/s
Average packet rate      =  19.927935 pkt/s
Packets dropped          =          0 (0.00 %)
Average loss-burst size  =          0 pkt
Error lines              =          0
```

b)



c)

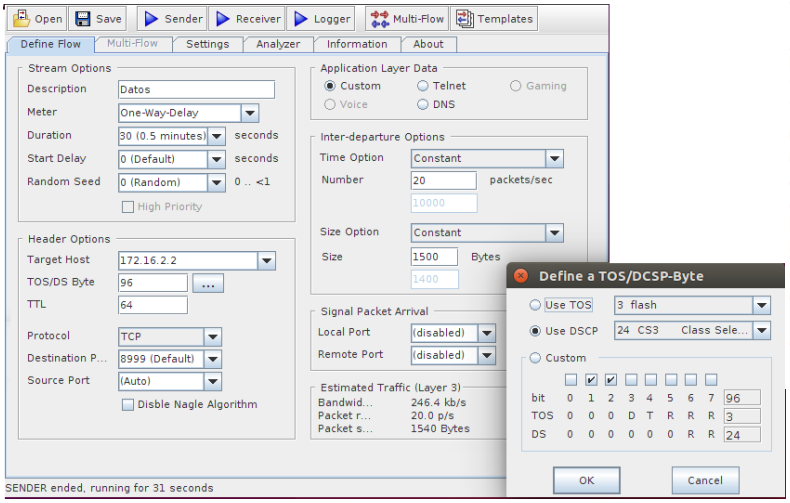


d)

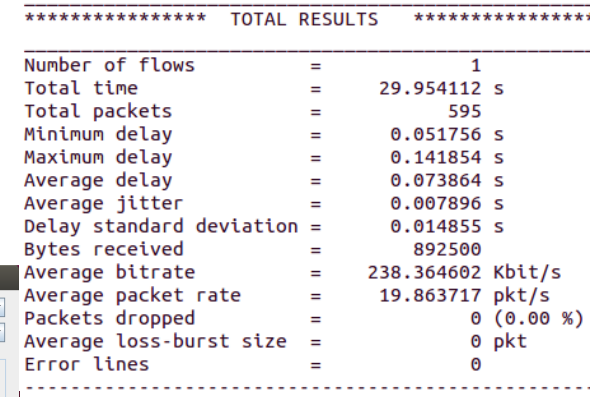
Figura 71: Streaming a) Inyector de tráfico b) Resultados en el receptor c) gráficas de delay y jitter d) gráfica de bitrate y packetloss

Como se puede observar en la figura 71 para el tráfico de Streaming los valores que manda el inyector de tráfico va marcado con CS3 de una manera constante de envío de 20 paquetes/s con un tamaño de 1500 bytes dando un estimativo de ancho de banda de 244.5Kbits por segundo.

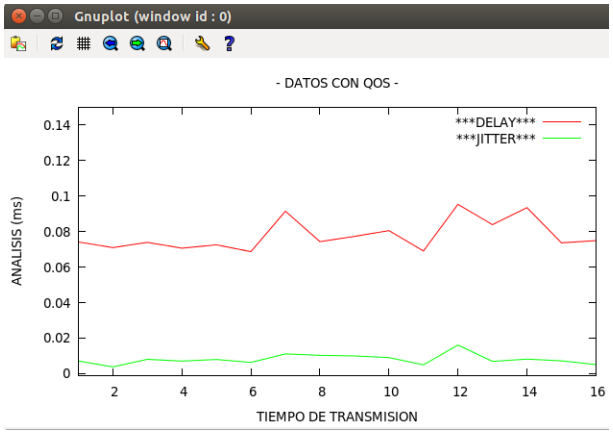
4.12.3 DATOS



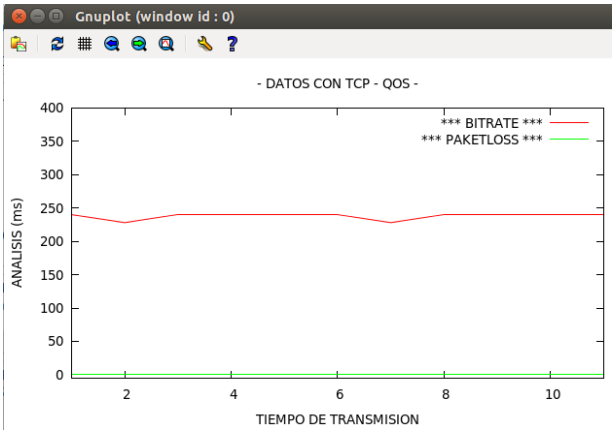
a)



b)



c)



d)

Figura 72: Datos a) Inyector de tráfico b) Resultados en el receptor c) gráficas de delay y jitter d) gráfica de bitrate y packetloss

Como se puede observar en la figura 72 para el tráfico de datos los valores que mandó el inyector de tráfico va marcado con CS3, se realizó de una manera constante el envío de 20 paquetes/s con un tamaño de 1500 bytes dando un estimativo de ancho de banda de 246,4Kbits por segundo usando el gnuplot dan las gráficas de los paramétros de calidad de servicio que se analiza en el siguiente ítem.

4.13 ANÁLISIS DE LOS PARÁMETROS EN EL ESCENARIO DE PRUEBAS

En el escenario de prueba se procede a trabajar tres tipos de tráfico que son VoIP, Streaming y Datos, primeramente se activa en las máquinas virtuales el generador de tráfico D-ITG como se describió anteriormente, luego se coloca los parámetros de acuerdo al tipo de tráfico a generar.

A continuación se analizará los parámetros de calidad de servicio de retardo (delay), jitter y packet loss, donde primeramente para cada parámetro se colocara la tabla de las recomendaciones de la UIT-T G.1010, Y 1541 y la IEEE 8021.1p para hacer una comparación con los mismos y ver el comportamiento del tráfico al aplicar el mecanismo de DiffServ.

4.13.1 RETARDO

Para el tráfico de Voz y Streaming se consideró el protocolo UDP y para el tráfico de datos se consideró el protocolo TCP para que los datos lleguen completos, hay que tomar en cuenta que se hará el análisis de la red sin configurar QoS y luego configurando QoS con el mecanismo DiffServ.

De acuerdo a las recomendaciones de la UIT-T G.1010, Y 1541 y la IEEE 8021.1p se obtiene la siguiente tabla:

Tráfico	Excelente	Muy Bueno	No Adecuado
VoIP	<100ms	>100ms y <150ms	>150ms
Datos	< 250ms	>250ms y <300ms	>300ms
Streaming	<=100 ms	>100ms y <=250ms	> 250ms

Tabla 20: Valoraciones cualitativa de Latencia (Retardo) [48]

[48] Tomado de (Buñay Guisñay, 2013), Estándares de la UIT-T, G.1010, Y 1541 y la IEEE 802.1p

Como se observa en la tabla 20 el retardo máximo para VoIP es de 150ms para que no se solape la conversacion, para Datos el retardo máximo es 300ms para una adecuada transmisión y para Streaming un tope de 250ms.

Tráfico	G.711	G.723.1	G.729	Datos	Streaming
VPN MPLS (ms)	719.00	280.00	292.58	121.50	82.66
VPN MPLS y DiffServ (ms)	23.00	8.50	10.00	73.86	27.42

Tabla 21: Datos tomados del escenario de prueba

Se puede observar en la tabla 21 que comparando con los valores cualitativos de la latencia de la Tabla 20 que los valores obtenidos para la latencia en el escenario de prueba son demasiados altos sin aplicar el mecanismo de calidad de servicio y en retardo baja considerablemente cuando se aplica calidad de servicio.

Tráfico	G.711	G.723.1	G.729	Datos	Streaming
VPN MPLS	No adecuado	No adecuado	Muy Bueno	Muy Bueno	Muy Bueno
VPN MPLS y DiffServ	Muy Bueno	Excelente	Excelente	Excelente	Excelente

Tabla 22: Latencia o Retardo de la red[49]

Observando la tabla 22 podemos concluir que la transmisión mejora considerablemente al estar activo la calidad de servicio con el mecanismo DiffServ, lo que podemos apreciar también en las gráficas que se lo realizaron con la herramienta GNUPLOT en Linux en las máquinas virtuales.

[49] Fuente Propia

4.13.2 GRÁFICA DEL RETARDO

Figura 73: Valoraciones cualitativa de Latatencia (Retardo)

Se puede observar en la figura 73 que la red VPN MPLS mejora notablemente el retardo por la conmutación de etiquetas en vez de direcciones, permitiendo que la conmutación sea rápida entre los router, adicionalmente con el mecanismo de DiffServ con el trato diferenciado de los paquetes da alta prioridad a paquetes de VoIP y menor prioridad a paquetes de dato, se observa que los tiempos bajan considerablemente dando garantía a la calidad de servicio.

4.13.3 JITTER

Debido al retardo que se produce en los flujos de datos se genera un problema llamado jitter que aparece por congestión en la red, especialmente por una incorrecta sincronización de bits entre los elementos de red. La tabla de los umbrales máximos de Jitter según las recomendaciones UIT-T, G.1010, Y.1541 y la IEEE 802.1p son: (Buñay Guisñay, 2013)

Tráfico	Excelente	Muy Bueno	No Adecuado
VoIP	<40ms	>40ms y <50ms	>50ms
Datos	< 55ms	>55ms y <70ms	>70ms
Streaming	<=35 ms	>35ms y <=65ms	> 65ms

Tabla 23: Valoraciones cualitativa de Jitter[50]

[50] Tomado de (Buñay Guisñay, 2013), Estándares de la UIT-T, G.1010, Y 1541 y la IEEE 802.1p

Como se puede observar en tabla 23 el jitter máximo para VoIP es 50ms, para Datos el jitter máximo es 70ms y para Streaming un tope de 65ms para que no haya una variación de flujo de datos entre el transmisor y el receptor. A continuación se dan los datos tomados en el escenario de prueba.

Tráfico	G.711	G.723.1	G.729	Datos	Streaming
VPN MPLS (ms)	1	12.22	8.52	13.24	9.3
VPN MPLS y DiffServ (ms)	0.68	8.52	6.70	7.8	10

Tabla 24: Datos tomados del escenario de prueba

Como se puede observar en la tabla 24 la red a nivel de jitter maneja parámetros adecuados que son aceptables de acuerdo a la Tabla 23 que son los estándares internacionales y mejora mucho más aplicando el mecanismo de DiffServ.

Tráfico	G.711	G.723.1	G.729	Datos	Streaming
VPN MPLS	Muy Bueno	Muy Bueno	Muy Bueno	Muy Bueno	Muy Bueno
VPN MPLS y DiffServ	Excelente	Excelente	Excelente	Excelente	Excelente

Tabla 25: Jitter[51]

Se puede observar en la tabla 25 de manera cualitativa, que los tiempos bajan considerablemente dando garantía a la calidad de servicio con el mecanismo de DiffServ mejora el problema del jitter.

[51] Fuente propia

GRÁFICA DEL JITTER

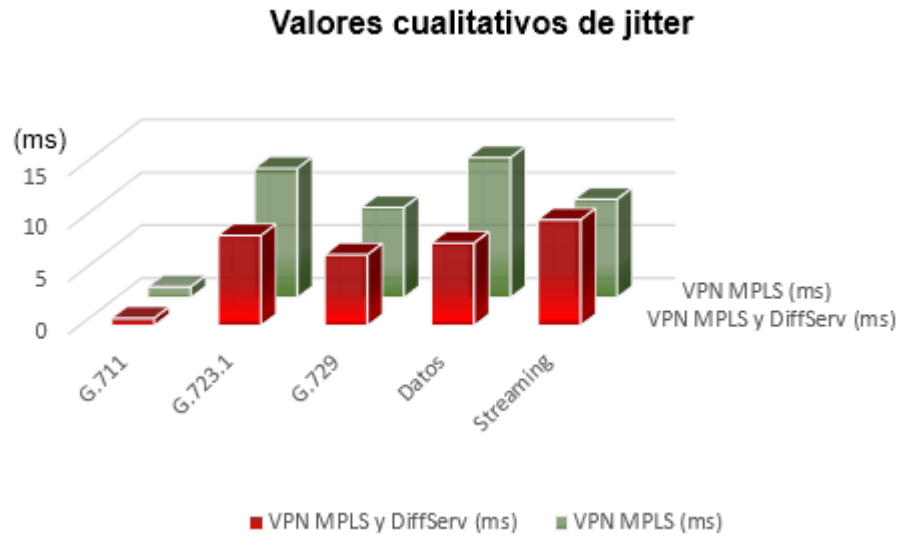


Figura 74: Valoraciones cualitativa de Jitter

En la figura 74 se puede observar que en redes VPN MPLS que el jitter baja por la conmutación de etiquetas (label switching) que permite enrutar a más velocidad disminuyendo el retardo y el jitter.

Al aplicar el mecanismo de DiffServ es más notoria la reducción porque aparte de tener más velocidad se tiene mayor prioridad para los paquetes de VoIP, al crear políticas tanto de entrada como de salida en las interfaces de los routers se garantiza delay, jitter y pérdida de paquetes.

4.13.4 PÉRDIDA DE PAQUETES

Para las comunicaciones en tiempo real con servicios como Streaming y Voz que se basan en el protocolo UDP que es un protocolo que no está orientado a conexión, muchas veces se produce pérdida de paquetes que no se reenvían porque hay un descarte de paquetes que no llegan a tiempo al receptor.

Tomando las referencias de las recomendaciones UIT-T G.1010, Y. 1541 y la IEEE 802.1p se establecen los umbrales máximos de pérdida de paquetes.

Tráfico	Excelente	Muy Bueno	No Adecuado
VoIP	<1%	>1% y <3%	>3%
Datos	< 3%	>3% y <5%	>5%
Streaming	<=2%	>2% y <=5%ms	> 5%

Tabla 26: Valoraciones cualitativa de Pérdida de paquetes[52]

Como se observa en la tabla 26 el porcentaje máximo en pérdida de paquetes es 3% para VoIP, para Datos lo máximo es el 5% y para Streaming un tope de 5ms.

Tráfico	G.711	G.723.1	G.729	Datos	Streaming
VPN MPLS (ms)	0.00	0.00	0.00	0.00	0.00
VPN MPLS y DiffServ (ms)	0.00	0.00	0.00	0.00	0.00

Tabla 27: Datos tomados del escenario de prueba

Tráfico	G.711	G.723.1	G.729	Datos	Streaming
VPN MPLS	No hay Pérdidas	No hay Pérdidas	No hay Pérdidas	No hay Pérdidas	No hay Pérdidas
VPN MPLS y DiffServ	No hay Pérdidas	No hay Pérdidas	No hay Pérdidas	No hay Pérdidas	No hay Pérdidas

Tabla 28: Pérdida de paquetes[53]

[52] Tomado de (Buñay Guisñay, 2013), Estándares de la UIT-T, G.1010, Y 1541 y la IEEE 802.1p

[53] Fuente propia

Como se puede observar en la tabla 27 y tabla 28 en redes VPN MPLS y DiffServ se observa que no hubo pérdida de paquetes para los datos de prueba porque se tiene etiquetado de paquetes en base a criterios de prioridad y adicionalmente en ambos caso de la muestra que son la VPN MPLS y LA VPN MPLS con DiffServ no se saturo el canal con el tráfico generado.

4.14 SEGURIDAD DE LA INFORMACION

Como se menciono anteriormente las redes MPLS VPN no cumplen con confidencialidad, no repudio y datos criptográficos pudiendo ser interceptados los datos durante la transmisión sin conocimiento del transmisor y del receptor, dando como solución la implementación de IPSec VPN que es la única manera de implementar las VPNs seguras.

Las soluciones IPSec VPN están dadas en dos categorías:

- Site to Site IPSec VPN: Que se tiene las siguientes subdivisiones :
    - Full Mesh
    - Hub and Spoke
    - DMVPN
    - Static VTI
    - GETVPN
- Acceso Remoto IPSec VPN: Con las siguientes subdivisiones
    - Easy VPN
    - Dynamic VTI

4.14.1 PASOS PARA IMPLEMENTAR IPSec

Una implementación de IPSec es como un Security Gateway (SG), que da protección al tráfico IP y se basa en los requerimientos que se establece en una Base de Datos de Políticas de Seguridad (SPD), mantenidas por un usuario o administrador del sistema o por una aplicación.

Para proporcionar seguridad de tráfico se usa la cabecera de Autenticación (AH) y la Carga de Seguridad Encapsulada (ESP). A continuación se detalla cada uno de los mismos:

- Cabecer de Autenticación (AH): Que proporciona integridad sin conexión, adicionalmente autenticación del origen de datos y servicio de protección antireplay.

- Carga de Seguridad Encapsulada (ESP): Que proporciona confidencialidad (encriptación), integridad sin conexión, confidencialidad limitada de flujo de tráfico, servicio de protección antireplay y autenticación del origen de datos.

Tanto AH y ESP son instrumentos de control de acceso que se basan en claves criptográficas y manejo de flujo de tráfico.

A continuación se detallan los pasos para la implementación del mismo:

Paso 1	**Preparando la configuración IPSec**	• **Determine IKE (Internet Key Exchange) y política IPSec.** • **Verificar que se establezca la conectividad con el router miembro.**
Paso 2	Configuración de parámetros IKE (Internet Key Exchange)	a) Garantizar que el modo de configuración este habilitado. b) Habilitar IKE/ISAKMP en el router. c) Crear la política IKE para que se pueda utilizar las claves compartidas. • Establecer la prioridad de la política e ingresar al modo config –ISAKMP. • Establecer la autenticación de utilizar claves previamente compartidas. • Establecer cifrado IKE. • Establecer un grupo Diffie Hellman. • Establecer el algoritmo hash. • Establecer la asociación con el servidor IKE. • Salir del modo de configuración **config-isakmp** • Configurar la clave pre compartida y dirección peer (miembro). • Salir del modo de configuración. • Examinar el conjunto de políticas de cifrado.
		a) Verificar que el modo de configuración está habilitada. b) Verificar que las opciones de cifrado IPSec estén disponibles. c) Verificar que el conjunto de opciones de transformación estén disponibles.

Paso 3	Configurar parámetros IPSec	d) Definir un conjunto de transformación e) Configurar el modo túnel. f) Salir del modo de configuración. g) Verificar la configuración. h) Configurar la encriptación de las listas de acceso. i) Verificar si el modo de configuración esta habilitado. j) Configurar ACLs k) Configurar crypto maps l) Configurar el nombre, número y tipo de intercambio de claves del mapa a ser usado, m) Especificar el conjunto de transformaciones definidas anteriormente. n) Asignar los peers VPN utilizando el nombre del host o la dirección IP de los peer, o) Salir del modo de configuración cryto map. p) Aplicar crypto map a la interfaz q) Acceder al modo de configuración de la interfaz. r) Asignar el crypto maps a la interfaz,
Paso 4	Verificar y probar la configuración IPSec	a) Verificar las políticas IKE de configuración. b) Verificar la configuración del conjunto de transformación. c) Verificar la configuración de crypto maps. d) Verificar el estado actual IPSec.
Paso 5	Afinamiento de cripto ACL	a) Ajustar las configuraciones de cripto ACL que se utiliza para determinar el tráfico interesante.

Tabla 29: Pasos para configurar IPSec en la VPNMPLS

Como se puede observar en la tabla 29 se listan los pasos para configurar IPSec en la red VPN MPLS. La implementación del IPSec no forma parte del temario de esta tesis.

CAPITULO 5

5 CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES Y RECOMENDACIONES

5.1.1 CONCLUSIONES

- La implementación de la tecnología VPN MPLS en el backbone de una red permite seguridad, confidencialidad, integridad de datos y un escalamiento creciente de la red por su fácil adaptación a cualquier tecnología de red.

- Las redes VPN MPLS con el mecanismo DiffServ ofrece garantías de calidad de servicio para los diferentes tipos de tráfico como son VoIP, Streaming y Datos.

- El mecanismo DiffServ permite dividir el tráfico en clases, controlando la cantidad de tráfico que cada cliente envía a la red y priorizándolo el envío a través de políticas de clasificación mejorando la eficiencia de una red significativamente.

- La herramienta D-ITG permite generar e inyectar tráfico a nivel de red, transporte y aplicación con gran exactitud, calcula el ancho de banda mínimo que necesita el enlace y permite evaluar los indicadores de calidad de servicio como son bit-rate, jitter, delay, packets dropped para los diferentes tipos de tráfico.

- Al analizar los datos obtenidos con el software D-ITG se observa que en el indicador de retardo sin el mecanismo de DiffServ y con el mecanismo DiffServ se obtuvo un promedio respectivamente de 430.52ms y 13.83 ms para el tráfico de VoIP, 82.67 ms y 27.42 ms para el tráfico de Streaming, 121.50ms y 73.86ms para el tráfico de Datos, como se puede

observar sin aplicar el mecanismo de DiffServ no son valores adecuados para la VPN MPLS, mientras que aplicando el mecanismo de DiffServ los valores trabajan en el rango recomendado por los estándares de la UIT-T G.1010, Y 1541 y la IEEE 8021.1p para proporcionar calidad de servicio.

- Al analizar el Indicador de Jitter para las redes VPN MPLS sin el mecanismo de DiffServ y aplicando el mecanismo de DiffServ se obtiene respectivamente 7.24 ms y 5.3 ms para VoIP, 9.3ms y 10ms para Streaming, 13.24 ms y 7.8 ms para Datos, se observa que los valores disminuyen con el mecanismo de DiffServ porque se maneja prioridades y políticas a más de tener mayor velocidad con la tecnología MPLS.

- Al analizar el Indicador de paquetes perdidos para las redes VPN sin el mecanismo de DiffServ y aplicando el mecanismo de DiffServ se observa que no hay pérdidas de paquetes porque se tiene etiquetado de paquetes en base a criterios de prioridad y calidad de servicio.

5.1.2 RECOMENDACIONES

- Se recomienda usar la tecnología MPLS porque permite una conmutación de etiquetas más rápida y eficiente a diferencia de las técnicas de encaminamiento IP tradicionales que lo hacen por direccionamiento del destino que son más lentas.

- Se recomienda disponer de máquinas con capacidad de procesamiento y memorias suficientes para usar las herramientas GNS3 y D-ITG (mínimo 4GB de memoria RAM y 4GHz de velocidad de la PC) que permiten simular plataformas robustas como Cisco y analizar el tráfico de una red respectivamente, las mismas que están licenciadas como herramientas gratuitas.

- Se recomienda antes de usar la herramienta D-ITG para inyectar algún tipo de tráfico configurar adecuadamente el protocolo de la capa de transporte TCP o UDP, su aplicación si es Telnet, DNS, Voice y el tiempo de inyección de tráfico del emisor y del receptor, porque de estas configuraciones difieren los resultados.

- Se recomienda a los administradores de red hacer un análisis de las necesidades del usuario para aplicar políticas de entrada y salida en las interfaces.

6 BIBLIOGRAFÍA

González Morales, A. (Mayo de 2006). Redes Privadas Virtuales. Pachuca, México. Obtenido de http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Redes%20privadas%20virtuales.pdf

Alvarez Gonzaga, B. (s.f.). Configuración de una Red Privada Virtual VPN utilizando Windows Server 2008. Obtenido de http://braulioedunet.webcindario.com/configurar-vpn.pdf

Alvarez, R. B. (2007). Contribución en el Análisis y Simulación de una red MPLS con la internet de servicios diferenciados Diffserv. Lima, Perú. Obtenido de http://cybertesis.unmsm.edu.pe/bitstream/cybertesis/2337/1/Bustamante_ar.pdf

Buñay Guisñay, P. A. (2013). Aplicación de la Arquitectura DIFFSERV sobre redes MPLS para la provisión de Qos punto a punto en la transmsión de tráfico en tiempo real. Riobamba, Ecuador. Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/4034/1/20T00464.pdf

Catarina. (s.f.). MPLS VPN. Obtenido de http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/capitulo3.pdf

Cevallos Romero, E. (Abril de 2015). Evaluación de Parámetros de QoS en redes Wimax que soportan Voz y Video. Quito, Pichincha, Ecuador.

Chiqui Guachiullca, M. (Febrero de 2015). Estudio de Factibilidad de IP TV en la red IP / MPLS de Etapa EP utilizando VPN MPLS. Cuenca, Ecuador. Obtenido de http://dspace.ups.edu.ec/handle/123456789/7758

Cosios Castillo, E. R. (Junio de 2004). Estudio y Diseño de Redes Virtuales Privadas (VPN) basadas en tecnologías MPLS. Quito, Pichincha, Ecuador. Obtenido de bibdigital.epn.edu.ec/bitstream/15000/4382/1/CD-3980.pdf

Doménico Luna, J. I. (s.f.). Medición y análisis de tráfico en redes MPLS. Perú. Obtenido de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/212/LUNA_JAVIER_MEDICION_ANALISIS_TRAFICO_REDES_MPLS.pdf?sequence=2

España, C. (2008). *El arte de la tecnología y la comunicación.* Obtenido de http://blogsdelagente.com/planetadigital/2008/09/29/migracion-mpls-por-que-cuando-com/

ESPE. (2015). *Plan Estrategico de la ESPE.* Obtenido de http://www.espe.edu.ec/portal/files/Plan_Estrategico_Institucional_ESPE_2014-2017.pdf

Fernández Muñoz, S. D. (Febrero de 2007). Diseño de un canal Privado de comunicaciones entre dos puntos utilizando la infraestructura de Internet y Análisis del Canal VPN de la Universidad Politécnica Salesiana. Cuenca, Azuay, Ecuador. Obtenido de http://www.dspace.ups.edu.ec/bitstream/123456789/754/12/Tesis.pdf

Fernández, M. Á. (01 de Mayo de 2002). Network World. Obtenido de http://www.networkworld.es/archive/mpls-ventajas-para-las-empresas

Gómez , J. R., & Peña Moliner, C. (2005). MPLS y su Aplicación en Redes Privadas Virtuales (L2VPN y L3VPN). Obtenido de http://www.laccei.org/LACCEI2005-artagena/Papers/IT083_MolinerPena.pdf

Guy, T. C. (1 de Marzo de 2006). Arquitectura de calidad de servicio (QoS) basada en directivas de Windows Server "Longhorn" y Windows Vista. Obtenido de https://www.microsoft.com/spain/technet/recursos/articulos/cg0306.mspx

Hernández, K. R. (Noviembre de 2008). Estudio de las ventajas e implementación de servicios IP VPN, sobre una infraestructura MPLS en la región centroamericana. Guatemala. Obtenido de http://biblioteca.usac.edu.gt/tesis/08/08_0221_EO.pdf

Hidalgo Llumiquinga, C., & Laguapillo Muñoz, D. (Noviembre de 2011). Diseño e Implementación de una Laboratorio que permita emular y probar servicios IP y MPLS de la red de Backbone CISCO de la corporación Nacional de Telecomunicaciones CNT. Quito, Pichincha, Ecuador. Obtenido de file:///C:/Users/INTEL/Downloads/CD-3980%20(2).pdf

Humans, N. (2013). *net. Humans.* Obtenido de https://www.nethumans.com/solutions/itSecurity/VPN.aspx

Lab-MPLS. (s.f.). *Lab 7. Multiprotocol Label Switching.* Obtenido de http://people.ccaba.upc.edu/careglio/wp-content/uploads/2013/12/Lab7-MPLS.pdf

Menéndez Avila, R. (Agosto de 2012). Estudio del desempeño e implementación de una solución MPLS-VPN sobre múliples sistemas aútonomos. Lima, Perú. Obtenido de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/1500/MENENDEZ_AVILA_RICARDO_SOLUCION_MPLS_VPN.pdf?sequence=1

Moraga, S. A. (2004). *Estudio y configuración de calidad de servicio para protocolos IPv4 e IPv6 en una red de fibra óptica WDM.* Obtenido de www.scielo.cl/pdf/rfacing/v13n3/art15.pdf

Morales Santiago, Gilberto Nuñez Trejo, Jonathan Patiño Toribio, Pedro Porras Flores, Benjamin Alejandro, Presbitero Pacheco. (Mayo de 2007). Diseño de la configuración de una red MPLS para proporcionar servicios de VPN para Basher Network. Mexico, Mexico. Obtenido de http://tesis.ipn.mx/jspui/bitstream/123456789/5387/1/ice11.pdf

Onestopclick. (2015). *Onestopclick Researching Networking Solutions*. Obtenido de http://networking.onestopclick.com/article/61/327/mpls-ip-vpn-explained.html

Orozco Lara, F. R. (3 de Septiembre de 2014). Diseño de una Red Privada con tecnología MPLS para la carrera de Ingeniería de Networking de la Universidad de Guayaquil. Guayaquil, Guayas, Ecuador. Obtenido de http://repositorio.ucsg.edu.ec/bitstream/123456789/2198/1/T-UCSG-POS-MTEL-23.pdf

Paspuel Fraga, D. (Julio de 2014). Optimización del ancho de banda de acceso a internet y control de tráfico de la Universidad Técnica del Norte aplicando calidad de servicio

(QoS). Ibarra, Ecuador. Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/3770/1/04%20RED%20036%20TESIS.PDF

Pincay Espinoza, E. (2015). Análisis comparativo de la calidad de servicio entre redes actuales y redes de próxima generación. Riobamba, Chimborazo, Ecuador. Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/3776/1/18T00581.pdf

Pupiales, S. K. (2010). Diseño de una red de Backbone con tecnología MPLS para el soporte de servicio triple play en la empresa ECUANET-MEGADATOS S.A. Ibarra, Imbabura, Ecuador. Obtenido de repositorio.utn.edu.ec/.../04%20RED%20001%20BACKBONE%20MPL...

Quevedo Bravo, D. P., & Vaca Nuñez, C. L. (Diciembre de 2011). Diseño e Implementación de calidad de Servicio (QoS) en la red de transporte de datos del municipio del Distrito Metropolitano de Quito (MDMQ). Quito, Pichincha, Ecuador. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/4409/1/CD-4028.pdf

Reyes, T. G. (Junio de 2007). Análisis de los modelos de servicios diferenciales y servicios integrales para brindar QoS en Internet. Mexico, Huajuapan de Leon. Obtenido de http://mixteco.utm.mx/~resdi/historial/Tesis/Tesis-Thelma.pdf

Rodríguez, D. (Noviembre de 2008). Transmisión de Voz, Video y Datos en Redes Privadas Virtuales VPN MPLS. Buenos Aires, Argentina. Obtenido de http://www.ub.edu.ar/investigaciones/tesinas/259_rodriguez.pdf

Trujillo Machado, E. R. (Marzo de 2006). Diseño e Implementación de una VPN en una empresa comercializadora utilizando IPSEC. Quito, Pichincha, Ecuador. Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/214/1/CD-0210.pdf

7 ANEXOS

7.1 ANEXO 1 CONFIGURACIONES

CONFIGURACIÓN DE EQUIPOS DE LA RED VPN MPLS

Configuración de la interface PE (R1)

R1# config t

R1 (config) # interface s0/1

R1 (config-if) # ip address 192.168.12.16 255.255.255.252

R1 (config-if) # clock rate 64000

R1 (config-if) # no shutdown

R21 (config-if) #exit

R1 (config) # interface s0/2

R1 (config-if) # ip address 192.168.12.12 255.255.255.252

R1 (config-if) # clock rate 64000

R1 (config-if) # no shutdown

R1 (config-if) # exit

R1 (config) # interface loopback 0

R1 (config-if) #ip address 192.168.1.1 255.255.255.255

R1 (config-if) # end

R1# wr

Configuración de la interface PE (R3)

R3# config t

R3 (config) # interface s0/0

R3 (config-if) # ip address 192.168.12.10 255.255.255.252

R3 (config-if) # clock rate 64000

R3 (config-if) # no shutdown

R3 (config-if) #exit

R3 (config) # interface s0/1

```
R3 (config-if) # ip address 192.168.12.20 255.255.255.252
R3 (config-if) # clock rate 64000
R3 (config-if) # no shutdown
R3 (config-if) #exit

R3 (config) # interface s0/2
R3 (config-if) # ip address 192.168.12.14 255.255.255.252
R3 (config-if) # clock rate 64000
R3 (config-if) # no shutdown
R3 (config-if) # exit
R3 (config) # interface loopback 0
R3 (config-if) #ip address 192.168.1.3 255.255.255.255
R3 (config-if) # end
R3#  wr
```

Configuración del Protocolo OSPF en PE (R1)

Configuración de los equipos con:

- Encaminamiento con el Protocolo OSPF proceso 1, área 0

```
R1 (config) # router ospf 1
R1 (config-router) # log-adjacency-changes
R1 (config-router) # network 192.168.1.1 0.0.0.0 area 0
R1 (config-router) # network 192.168.12.4 0.0.0.3 area 0
R1 (config-router) # network 192.168.12.12 0.0.0.3 area 0
```

Para habilitar MPLS en los routers se debe indicar las interfaces que participaran con el comando **mpls ip.**

Activar CEF para trabajar en entornos MPLS

```
R1 (config) # ip cef
R1 (config-if) # mpls label protocol ldp
R1 (config-if) # mpls ip
```

R3 (config) # ip cef

R3 (config-if) # mpls label protocol ldp

R3 (config-if) # mpls ip

Activar el protocolo de distribución de etiquetas LDP

R5 (config) # interface serial 0/1

R5 (config) # mpls ip

R5 (config) # mpls label protocol ldp

R7 (config) # interface serial 0/2

R7 (config) # mpls ip

R7 (config) # mpls label protocol ldp

R5 (config) # interface serial 0/0

R5 (config) # mpls ip

R5 (config) # mpls label protocol ldp

R5 (config) # interface f0/0

R5 (config) # mpls ip

R5 (config) # mpls label protocol ldp

R7 (config) # interface serial 0/0

R7 (config) # mpls ip

R7 (config) # mpls label protocol ldp

R7 (config) # interface f0/0

R7 (config) # mpls ip

R7 (config) # mpls label protocol ldp

R5 (config) # interface serial 0/0

R5 (config # mpls ip

R5 (config) # mpls label protocol ldp

R5 (config) # interface f0/0

R5 (config) # mpls ip

R5 (config) # mpls label protocol ldp

Configuración de la red MPLS en R3 (PE)

Implementación de la red VPN MPLS

R3 (config) # interface serial 0/1

R3 (config-if) # ip vrf forwarding CLIENTE

R3 (config) # ip address 192.168.12.21 255.255.255.252

R3 (config) # clock rate 2000000

R3 (config) # router bgp 65505

R3 (config) # bgp-log-neeighbor-changes

R3 (config) # neighbor 192.168.1.3 remote-as 65505

R3 (config) # neighbor 192.168.1.3 update-source Loopback 0

R3 (config) # no auto-summary

R3 (config) # address-family vpnv4

R3 (config)# neighbor 192.168.1.3 activate

R3 (config)# neighbor 192.168.1.3 send-community extended

R3 (config)# exit-address-family

R3 (config) # address-family ipv4 vrf CLIENTE

R3 (config) # neighbor 192.168.12.21 remote-as 65505

R3 (config) # neighbor 192.168.12.21 activate

R3 (config) # no synchronization

R3 (config) # exit-address-family

Configuración de los dispositivos de la red

PC2 (RX-Ubuntu):

IP Address: 172.16.2.2 /24

Default Gateway; 172.16.2.1 /24

PC3 (PC-Fisica):

IP Address: 172.16.3.2 /24

Default Gateway; 172.16.3.1 /24

CONFIGURACIÓN DE LA CALIDAD DE SERVICIO

Configuración en PE (R3)

```
policy-map EXP-GROUP
 class class-default
  set qos-group mpls experimental topmost
policy-map MPLS-EXP-A-Q0S-GROUP
 class class-default
  set qos-group mpls experimental topmost
policy-map QOS-GROUP-A-PRECEDENCE
 class class-default
  set precedence qos-group

interface Serial0/0
 ip address 192.168.12.10 255.255.255.252
 mpls ip
 clock rate 2000000
 service-policy input EXP-GROUP

interface Serial0/1
 ip vrf forwarding CLIENTE
 ip address 192.168.12.21 255.255.255.252
 clock rate 2000000
 service-policy output QOS-GROUP-A-PRECEDENCE
```

```
interface Serial0/2
 ip address 192.168.12.14 255.255.255.252
 mpls ip
 clock rate 2000000
 service-policy input EXP-GROUP
```

Configuración de el CE (R4) MATRIZ

```
class-map match-any CLASE-GENERAL
 match  precedence 1
class-map match-any CLASE-VOZ
 match  dscp ef
class-map match-any CLASE-DATOS
 match  precedence 2
class-map match-any CLASE-ADMIN
 match  precedence 3
class-map match-any CLASE-CRITICO
 match  precedence 4

policy-map QOS
 class CLASE-VOZ
  set dscp ef
  priority percent 15
 class CLASE-CRITICO
  set precedence 4
  priority percent 20
 class CLASE-ADMIN
  set precedence 3
  priority percent 10
 class CLASE-DATOS
  set precedence 2
```

```
 priority percent 10
class CLASE-GENERAL
 priority percent 5
class class-default

interface Serial0/0
 ip address 192.168.12.18 255.255.255.252
 clock rate 2000000
 service-policy output QOS
```

Configuración de el C (R5) MATRIZ

```
class-map match-any PING
class-map match-any CLASE-GENERAL
 match  precedence 1
class-map match-any CLASE-VOZ
 match  dscp ef
class-map match-any CLASE-DATOS
 match  precedence 2
class-map match-any CLASE-ADMIN
 match  precedence 3
class-map match-any CLASE-CRITICO
 match  precedence 4

policy-map QOS
class CLASE-VOZ
set dscp ef
priority percent 15
class CLASE-CRITICO
set precedence 4
priority percent 20
class CLASE-ADMIN
set precedence 3
```

```
priority percent 10
class CLASE-DATOS
set precedence 2
priority percent 10
class CLASE-GENERAL
priority percent 5
class class-default

interface Serial0/0
 ip address 192.168.12.26 255.255.255.252
 clock rate 2000000
 service-policy output QOS
```

Configuración de el CE (R6) SUCURSAL

```
class-map match-any CLASE-GENERAL
 match  precedence 1
class-map match-any CLASE-VOZ
 match  dscp ef
class-map match-any CLASE-DATOS
 match  precedence 2
class-map match-any CLASE-ADMIN
 match  precedence 3
class-map match-any CLASE-CRITICO
 match  precedence 4


policy-map QOS
 class CLASE-VOZ
  set dscp ef
  priority percent 15
 class CLASE-CRITICO
  set precedence 4
  priority percent 20
 class CLASE-ADMIN
  set precedence 3
  priority percent 10
 class CLASE-DATOS
  set precedence 2
  priority percent 10
 class CLASE-GENERAL
  set precedence 1
```

```
 priority percent 5
class class-default

interface Serial0/1
 ip address 192.168.12.29 255.255.255.252
 clock rate 2000000
 service-policy output QOS
```

Configuración de el C (R7) SUCURSAL

```
class-map match-any CLASE-GENERAL
 match  precedence 1
class-map match-any CLASE-VOZ
 match  dscp ef
class-map match-any CLASE-DATOS
 match  precedence 2
class-map match-any CLASE-ADMIN
 match  precedence 3
class-map match-any CLASE-CRITICO
 match  precedence 4

policy-map QOS
 class CLASE-VOZ
  priority percent 15
 class CLASE-CRITICO
  priority percent 20
 class CLASE-ADMIN
  priority percent 10
 class CLASE-DATOS
  priority percent 10
 class CLASE-GENERAL
  priority percent 5
  set precedence 1
 class class-default
```

```
interface FastEthernet0/0
 ip address 172.16.2.1 255.255.255.0
 duplex auto
 speed auto
 service-policy output QOS
```

7.2 ANEXO 2 SOFTWARE UTILIZADOS

GNS3

GNS3 es un simulador gráfico de redes que permite diseñar topologías complejas de red y luego ejecutarlas, adicionalmente permite la virtualizacion de sistemas operativos (Windows o Linux) con herramientas de VMWare o VirtualBox. GNS3 está estrechamente vinculada con: Dynamips, un emulador de IOS que permite los usuarios ejecutar binarios imágenes IOS de Cisco Systems (Pupiales, 2010).

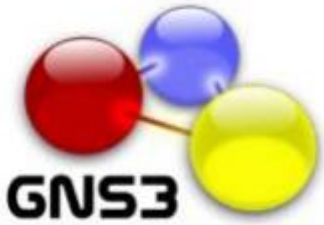


Figura 75: Simbolo del programa

Para completar las simulaciones, GNS3 se vincula con:

- Dynamips: Un emulador de router Cisco para las plataformas 1700, 2600, 3600, 3700, 7200 que permite a los usuarios ejecutar imágenes IOS de Cisco System.
- Dynagen: Es un front-end basado en texto para Dynamips elaborado por Greg Anuzelli que permite interactuar con Dynamips, utiliza el formato .INI de configuración e integra consola para administración de Dynagen, permitiendo a los usuarios listar dispositivos, suspender y recargar instancias, determinar los valores de Idle-PC, realizar capturas, etc (Pupiales, 2010).
- Qemu: Es un emulador de PIX.GNS3, para salvar las configuraciones, es una herramienta complementaria a los verdaderos laboratorios para los administradores de redes.

REQUERIMIENTOS DEL SOFTWARE:

- La PC debe tener como mínimo 4GB de memoria RAM.
- La velocidad de la PC como mínimo de 4GHz.

INSTALACIÓN DE GNS3

GNS3 se ejecuta en Windows, Linux y Mac OS X y requiere las siguientes dependencias: Qemu, Putty, Wincap y Wireshark que se lo consigue instalando el software GNS3 all-in-one que integra las mismas.

Los usuarios de Linux deben descargar Dynamips y extraerlo en una ubicación específica, luego se instala las dependencias y finalmente se ejecuta GNS3. Los usuarios Debian/Ubuntu pueden instalar el paquete Python-qt4 o instalar el paquete GNS3.deb y seguir paso a paso en la pagina: https://community.gns3.com/welcome.

IMÁGENES IOS

En Windows, la imagen se debe ubicar preferentemente en C:/Program Files \ Dynamips \ images o en la ubicación deseada. En sistemas Linux/Unix se debe ubicar de preferencia en /opt/images.
Las imágenes Cisco IOS están comprimidas y funcionan bien con Dynamips, aunque el proceso de arranque es significativamente mas lento debido a la descompresión (idéntico a los routers reales), es recomendable descomprimir las mismas de antemano para que el simulador no realice esta tarea, en sistemas Linux/Inx/Cygwin puede utilizar el utilitario unzip.

Unzip –p c3725-adventerprisek9-mz.124-15.T14.bin > c3725-adventerprisek9-mz.124-15.T14.image.

ADMINISTRACIÓN DE RECURSOS

Los Dynamips hacen uso intensivo de la memoria RAM y de la CPU para poder realizar la emulación y utilizan por defecto 64 MB en RAM en sistemas UNIX y 16 MB en Windows, los Dynamips también hacen

uso intensivo de la CPU porque está emulando la CPU de un router instrucción por instrucción, el sistema no tiene manera de saber cuando el router virtual está en estado ocioso (Idle) por lo que ejecuta todas las instrucciones que constituyen las rutinas de idle del IOS. Cuando se haya ejecutado el proceso del Idle-Pc para una determinada imágen de IOS, la utilización de la CPU decrecerá drásticamente.

CONFIGURANDO LAS PREFERENCIAS DE DYNAMIPS

Para realizar Dynamips en GNS3, se tiene que configurar el camino para alcanzarlo y el puerto base, estos valores serán utilizados por el Hypervisor Manager y para cargar los archivos .net, se debe buscar en Preferencias del menu Editar.

D-ITG

Es una herramienta utilizada para inyectar tráfico y realizar mediciones de tráfico en una red con diversos protocolos, una de las ventajas que tiene este software es que es una plataforma de código abierto que puede producir tráfico IPV4 o IPv6 con diferente tamaño de paquetes, es capaz de calcular el retardo, el jitter, delay y pérdida de paquetes, soporta los siguientes sistemas operativos:

- Linux (Ubuntu, Debian, Fedora, CentosOS, OpenWRT)
- Windows (XP, Vista, 7)
- OSX (Leopard)
- FreeBSD

D-ITG maneja el modelo cliente-servidor con cuatro componentes ejecutables que son ITGSend, ITGRecv, ITGLog, ITGDec.

- **ITGSen**d: Es el emisor de la inyección de tráfico, se puede generar un flujo o múltiples flujos dirigidos a un receptor o a varios receptores, según los parámetros que se configuro.
- **ITGRecv:** Es el receptor, que puede recibir un flujo o múltiples flujos del emisor.

- **ITGLog:** Es el que administra y contrala la generación de ficheros .log tanto del emisor como del receptor,
- **ITGDec:** Es aquel que permite dividir el fichero .log en cuatro archivos .dat que son el delay.dat, bitrate.dat, jitter.dat y packetlost.dat, los mismos que son usados para el análisis del QoS.

A continuación se dará los pasos para su instalación.

INSTALACIÓN:

- Descargar la versión 2.8.1-r1023 desde el sitio: http://traffic.comics.unina.it/software/ITG/
- Copiar y descomprimir el paquete dentro de un directorio /root
- Abrir un terminal de comandos e instalar los paquetes g++, octave.
- Ubicar dentro del directorio /root/D-ITG-2.8.1-rc1/src y colocar cp/root/D-ITG-2.8.1-rc1/scr

Configuración de Directorios:

- Crear dentro del D-ITG-2.8.1-rc1 la carpeta llamada logs mkdir/root/D-ITG-2.8.1-rc1/logs
- Copiar los archivos ITG* y lib* de /root/D-ITG-2.8.1-rc1/src al directorio usr/local/bin
- Luego cp /root/D-ITG-2.8.1-rc1/bin/ITG*/usr/local/bin
  cp /root/D-ITG-2.8.1-rc1/bin/ITG*/usr/local/bin
- Se da permisos de ejecución para ITGPlot con cd /root/D-ITG-2.8.1-rc1/src/ITGPlot
  Chmod + x ITGplot

Configuración de ITGSend

Todos los componentes ejecutables ITGSend, ITGRecv, ITGDec e ITGLog pueden ser llamados desde el directorio /root/D-ITG-2.8.1-rc1/bin/

La sintaxis de ITGSend para tráfico unidireccional es:

./ITGSend <nombre del archivo> -l <fichero-emisor.log> -x <fichero-receptor.log>

Ejemplo:

./ITGSend P1_n_20_8_0-1 –l ITGSend_P1_n_20_8_0-2.log –x ITGRecv_ P1_n_20_8_0-2.log

P1_n_20_8_0-1	Nombre del fichero de configuración
-l	Permite generar el fichero .log del emisor
-x	Genera el fichero .log del receptor
ITGRecv_P1_n_20_8_0-1.log	Nombre del fichero .log que almacena los Resultados del receptor.

La sintaxis para inyectar un solo flujo con ITGSend es la siguiente:

./ITGSend –a <dirección IP del receptor> [-m <dirección de flujo>] [-rp <puerto de destino>] [-i <interfaz de salida>] [-b <valor DS>] [-d <retardo de generación>] [-t <duración del flujo>] [-T <protocolo>] [-f <tiempo de vida del paquete>] [-C <cantidad de paquetes generados por segundo>] [-c <bytes de carga útil de cada paquete>]

Siendo:

-a <dirección del equipo receptor>: Especifica la dirección IP del Host destino.

-m <Dirección de Flujo>: Para realizar la medición en un solo sentido emisor a recptor se us owdm, requiriendo sincronización externa, otro comando es rttm que es una medición de ida y vuelta y no requiere sincronización externa pero incluye retardos, por defecto se tiene owdm.

-rp <puerto destino>: especifica el puerto que recibe la inyección de tráfico, el puerto por defecto es 8999.

-i <interface de salida>: Especifica la interfaz de salida (eth0) por la que inyecta tráfico opción soportada solo en la plataforma Linux.

-b <valor DS>: Permite marcar el campo DS del encabezado IP, permitiendo dar calidad de servicio, diferenciando el tipo de tráfico.

Para desplegar la interfaz gráfica se ejecuta la siguiente instrucción: /root/D-ITG# java -jar ITGGUI.jar.

Configuración del Emisor

En la configuración del Emisor se debe configurar las pestañas Define flow y Setting.

Define flow

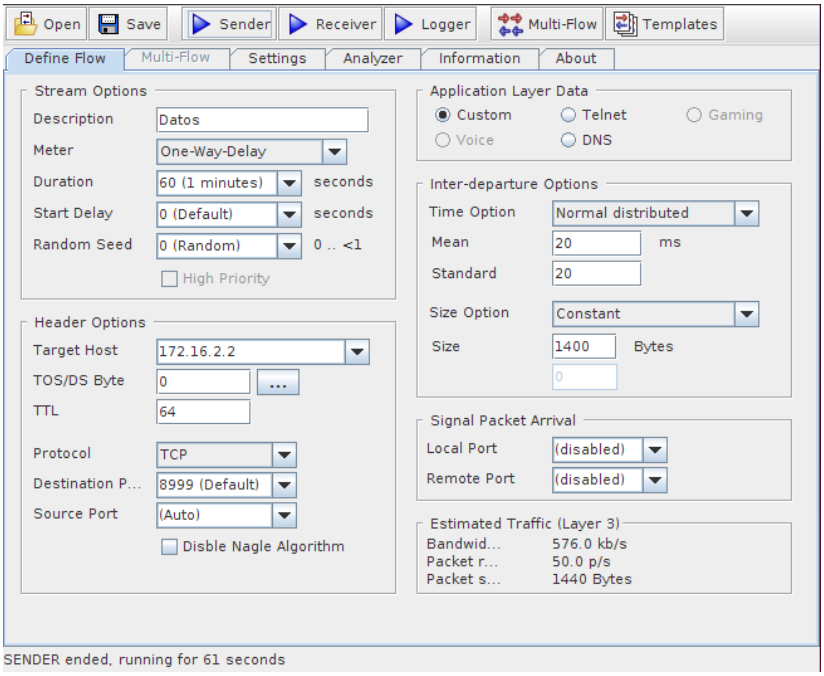


Figura 76: Define Flow

Se observa en la figura 76 los diferentes campos del emisor describiéndose los más importantes:

- *Descripción*: Nombre que se le da al archivo.
- *Meter:* Generación de tráfico en un solo sentido (OWD-One Way Delay) o de ida y vuelta (RTT-Round Trip Time).
- *Duration:* Tiempo que dura la transmisión en segundos.
- Target Host: Dirección destino ip del receptor.
- *TOS (Type of Service) / DS Byte:* Son los bits del campo del tipo de servicio

- *Protocolo:* El tipo de protocolo que se usará para la transmisión.
- *Destination Port:* Es el puerto destino que por defecto es el 8999.
- *Source Port:* Es el puerto origen que se le deja en automático.
- *Application Layer Data:* Se selecciona el tipo de tráfico a enviar teniendo custom (personalizado), Voz, telnet y DNS.
- *Time option:* Forma de envió del tráfico existiendo varios como uniformemente distribuido, normalmente distribuido.
- Mean: intervalos de envío.
- *Size option:* opción del tamaño del paquete si es constante o variante en el tiempo
- *Size:* Es el tamaño del paquete.

Verificación del emisor

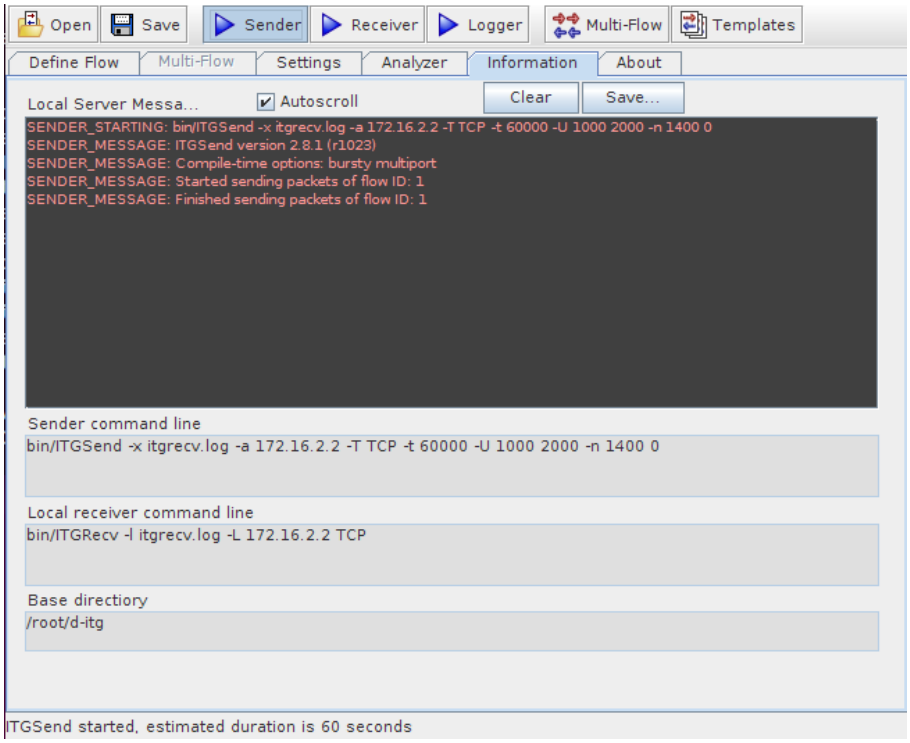


Figura 77: Verificación del emisor

Configuración del Receptor

- Configuración

  - sudo –
  - cd d-itg
  - /d-itg/bin# ./ITGRecv

```
root@miroslava-VirtualBox:~/d-itg# cd bin
root@miroslava-VirtualBox:~/d-itg/bin# ./ITGRecv
ITGRecv version 2.8.1 (r1023)
Compile-time options: bursty multiport
Press Ctrl-C to terminate
Listening on TCP port : 8999
Finish on TCP port : 8999
```

Figura 78: Verificación del puerto en escucha

Verificación de activación del receptor

```
root@miroslava-VirtualBox:~/d-itg# cd bin
root@miroslava-VirtualBox:~/d-itg/bin# ./ITGRecv
ITGRecv version 2.8.1 (r1023)
Compile-time options: bursty multiport
Press Ctrl-C to terminate
```

Figura 79: Verificación de la activación del receptor