UNIVERSIDAD TÉCNICA PARTICULAR DE LOJA

La Universidad Católica de Loja

ESCUELA DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE SISTEMAS INFORMÁTICOS Y COMPUTACIÓN

MODALIDAD PRESENCIAL

Simulación de algoritmos de enrutamiento dinámico sobre la red WAN MPLS de la UTPL

Trabajo de fin de carrera previa a la obtención del título de Ingeniería en Sistemas Informáticos y Computación.

AUTOR:

Piedra Illescas Gonzalo Patricio

DIRECTOR:

Ing. Córdova Erréis Carlos Gabriel

CODIRECTOR:

Ing. Jaramillo Campoverde Byron Gustavo

LOJA - ECUADOR

2012

Ing. Carlos Gabriel Córdova Erréis

DIRECTOR DE TESIS

C E R T I F I C A:

Que el Sr. Gonzalo Patricio Piedra Illescas, autor de la tesis "***Simulación de algoritmos de enrutamiento dinámico sobre la red WAN MPLS de la UTPL***", ha cumplido con los requisitos estipulados en el Reglamento General de la Universidad Técnica Particular de Loja, la misma que ha sido coordinada y revisada durante todo el proceso de desarrollo, desde su inicio hasta la culminación, por lo cual autorizo su presentación.

Loja, Febrero del 2012

_____

Ing. Carlos Gabriel Córdova Erréis

DIRECTOR DE TESIS

Ing. Byron Gustavo Jaramillo Campoverde

CODIRECTOR DE TESIS

C E R T I F I C A:

Que el Sr. Gonzalo Patricio Piedra Illescas, autor de la tesis "***Simulación de algoritmos de enrutamiento dinámico sobre la red WAN MPLS de la UTPL***", ha cumplido con los requisitos estipulados en el Reglamento General de la Universidad Técnica Particular de Loja, la misma que ha sido coordinada y revisada durante todo el proceso de desarrollo, desde su inicio hasta la culminación, por lo cual autorizo su presentación.

Loja, Febrero del 2012

_____

Ing. Byron Gustavo Jaramillo Campoverde

CODIRECTOR DE TESIS

CESIÓN DE DERECHO

Yo, **Gonzalo Patricio Piedra Illescas**, declaro ser autor del presente trabajo y eximo expresamente a la Universidad Técnica Particular de Loja y a sus representantes legales de posibles reclamos o acciones legales.

Adicionalmente declaro conocer y aceptar la disposición del Art. 67 del Estatuto Orgánico de la Universidad Técnica Particular de Loja que su parte pertinente textualmente dice. “forman parte del parte del patrimonio de la Universidad la propiedad intelectual de investigaciones, trabajos científicos o técnicos y tesis de grado que se realicen a través, o con el apoyo financiero, académico o institucional (operativo) de la Universidad”.

F.....

Gonzalo Patricio Piedra Illescas

AUTORIA:

En el presente Proyecto de tesis, todas las opiniones, criterios, conclusiones y recomendaciones vertidas en el presente informe de investigación son de absoluta responsabilidad del autor.

DEDICATORIA:

Este trabajo de investigación lo dedico en primer lugar a mi creador, quien siempre estuvo a mi lado dándome fuerza y valor para cumplir con mis metas, a mi hijo quien me motivo a seguir adelante y no desmayar, a mi esposa por ese apoyo incondicional y a mis padres por el sacrificio que hicieron toda su vida por darme un mejor futuro y bienestar.

AGRADECIMIENTO:

Mi agradecimiento a todas las personas que hicieron posible mi superación en mi formación profesional, a mi Director y Codirector de Tesis por su colaboración, apoyo y comprensión durante la realización del Proyecto de Tesis, y a todas aquellas personas que de una u otra manera me apoyaron durante este Proyecto que es una prueba más en mi vida profesional.

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

En este proyecto de tesis, se parte de la revisión de los algoritmos de enrutamiento y enrutados que están en la red WAN MPLS de la UTPL, con el objetivo de conocer el estado actual de la red, para luego analizar de acuerdo a las características y necesidades cual es el mejor algoritmo de enrutamiento dinámico que se puede aplicar en la red tanto con IPv4 e IPv6. Una vez escogido el algoritmo dinámico que mejor se adapte a la red, se propone que algoritmo se utilizará, una tabla de direccionamiento y un esquema de red basado en la red actual. Con todos estos datos se realiza el laboratorio de prácticas simulado con GNS3, para realizar pruebas, analizar las ventajas, desventajas y como puede afectar el algoritmo dinámico en la red WAN MPLS de la UTPL, finalmente se deja como resultado una propuesta y documentación del proceso de implementación, los cuales serán valorados por los administradores de la red WAN de la UTPL.

JUSTIFICACIÓN

En la actualidad la red WAN de la UTPL tiene implementado la tecnología MPLS en siete centros asociados, los cuales están configurados con dispositivos Routers y Switch conectados a través de un proveedor de servicio de internet, el cual comunica a los diferentes centros asociados. Dentro de los dispositivos que se encuentran en los diferentes centros asociados se tiene configurados tres servicios importantes como son video conferencia, datos y VoIP. Actualmente las configuraciones de enrutamiento son estáticas, lo cual provoca un gran inconveniente al momento de agregar nuevos dispositivos, comprometiendo la reconfiguración de la red. Para esto se realizará investigaciones acerca de los algoritmos de enrutamiento dinámico y enrutados para mejorar el rendimiento administrativo de la red y la escalabilidad la cual se puede mejorar aplicando algoritmos dinámicos. Antes de realizar una implementación es necesario crear un laboratorio de prácticas para la simulación de la red WAN MPLS de la UTPL, esto con el fin de identificar cuál es el mejor algoritmo de enrutamiento dinámico y enrutado que se adapte a las necesidades de la red, y poder identificar posibles problemas que se pueden dar en una futura implementación. Además la simulación nos sirve para probar, verificar y realizar pruebas con lo que ya está implementado actualmente, comparando y apreciando los posibles problemas que se pueden suscitar al momento de implementar un nuevo algoritmo de enrutamiento y enrutado. La simulación de este algoritmo nos sirve para identificar, escoger y aplicar un algoritmo que pueda aprovechar la tecnología MPLS.

OBJETIVOS

- Analizar los diferentes algoritmos de enrutamiento dinámico y seleccionar el que se ajuste a los requerimientos de la UTPL.
- Realizar la simulación de la red WAN de la UTPL en GNS3.
- Probar en el entorno simulado el algoritmo de enrutamiento dinámico seleccionado para la red WAN de la UTPL.
- Presentar la propuesta de implementación de algoritmos de enrutamiento dinámicos para la red WAN de la UTPL.

ALCANCE

La simulación de los algoritmos de enrutamiento dinámico sobre la red WAN MPLS de la UTPL, se debe realizar en base a los dispositivos que se tiene actualmente en la red WAN de la UTPL, los cuales son dispositivos CISCO. Se deberá utilizar una herramienta que simule la red de acuerdo a los algoritmos de enrutamiento dinámico que se utilizará y que soporte la simulación de los dispositivos a configurar en la red.

1 CAPÍTULO

ANÁLISIS DEL ESTADO ACTUAL DE LA RED WAN

1. INTRODUCCIÓN

En la ciudad de Loja y específicamente en la UTPL se tiene implementado redes WAN con la tecnología MPLS, en algunos centros regionales de la UTPL se ha implementado con éxito esta tecnología. La cual cuenta con varios servicios como, internet, video conferencia, voz sobre IP y transferencia de datos. En la actualidad su direccionamiento es estático lo cual representa un problema para aprovechar enormemente esta tecnología. La implementación de protocolos dinámicos en los enlaces privados de la UTPL sería una solución a este problema. Es necesario realizar una simulación del protocolo de enrutamiento que mejor se adapte a esta tecnología y a los requerimientos de la red WAN de la UTPL. Es por esta razón que se requiere un análisis del estado actual de las redes WAN MPLS[1] para aplicar un algoritmo de enrutamiento que mejore las prestaciones de esta tecnología. Para esto se requiere realizar una investigación acerca de los protocolos de enrutamiento y enrutados que se puede aplicar de mejor manera en esta tecnología para aprovechar los beneficios que presta. En la actualidad se están terminando las direcciones ipv4, lo cual sugiere que se debe implementar otro protocolo enrutado para emplear un protocolo que sea adecuado para el crecimiento de la red WAN de la UTPL y que nos de mejores beneficios que el protocolo actual.

1.1 Red WAN UTPL

La UTPL, en la actualidad está trabajando con dos proveedores de internet, como son, Global Crossing [2], el cual es una red global integrada de IP en el mundo que brinda soluciones de telecomunicaciones, y Telconet [3], que nos ofrecen tecnología MPLS L2/L3 para los enlaces urbanos e inter urbanos para lo cual garantiza la QoS[2] y modernidad de la red.

Estos proveedores también tienen soporte para última milla [1], de fibra óptica, hardware en el Core Cisco, tecnologías aplicadas y capacidades de red a nivel urbano, interurbano y ciudades.

En la Figura 1, se puede ver la distribución de la red WAN de la UTPL. Aquí se encuentra tres niveles, el Internet, que es el que distribuye a las máquinas el servicio de internet, la red WAN MPLS, donde se encuentran los centros asociados que actualmente tiene esta tecnología implementada, y túnel-IP que es por donde se transmiten diferentes servicios con diferentes direcciones por un solo enlace a través del protocolo enrutado IPv4. Más adelante se realiza una descripción de cada uno para entender a profundidad como está conformada la red WAN MPLS.

[1] Multiprotocol Label Switching
[2] Calidad de servicio

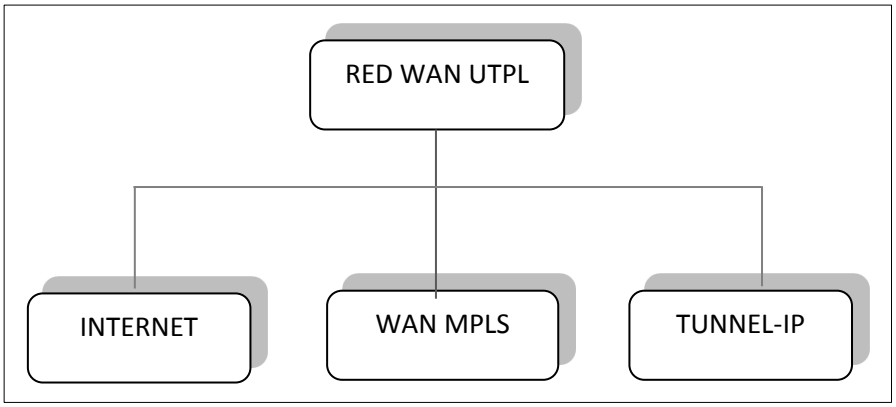


Figura 1. Esquema de la red WAN

1.1.1 Internet

El enlace con los centros asociados se los realiza mediante la red WAM-MPLS, a través de TUNNEL-IP, en la provincia de Loja.

El ancho de banda que la UTPL brinda a través de sus proveedores, es el que se muestra en la siguiente tabla, en la cual se evidencia la distribución de las conexiones de internet.

Tabla 1. Ancho de banda que ofrecen los proveedores para UTPL en Loja.

INTERNET			
UBICACIÓN	**DESCRIPCIÓN**	**BANDWIDTH**	**PROVEEDOR**
Loja	Internet	10 Mb	Global Crossing
Loja	Internet	50.1Mb	Telconet

Estos proveedores Global Crossing y Telconet utilizan protocolos de enrutamiento BGP[3] en sus Routers externos para proveernos del servicio de internet.

1.1.2 WAN MPLS

Actualmente la UTPL cuenta con siete centros asociados que tienen implementada la tecnología WAN MPLS, los cuales distribuyen su ancho de banda en tres canales, Datos, video y VoIP.

Todos los valores de Bandwidth (ancho de banda) de los diferentes centros asociados que cuentan con la tecnología WAN MPLS los podemos ver en el ANEXO 1. Cada centro asociado cuenta con VLANs diferentes que se direccionan por un túnel IP para el segmentado técnico de servicios de Datos, VoIP e internet. Las direcciones de red son distribuidas para los diferentes canales de cada centro asociado.

[3] Border Gateway Protocol

Tabla 2. VLANS de cada centro regional

CENTRO REGIONAL	DESCRIPCIÓN	DIRECCIÓN DE RED	VLANS	ANCHO DE BANDA
QUITO	Datos	172.16.40.0/24	40	384 kbps
	VoIP	172.16.46.0/24	46	1500 kbps
	Video	200.0.30.1/28	30	512 kbps
GUAYAQUIL	Datos	172.16.42.0/24	42	256 kbps
	VoIP	172.16.48.0/24	48	128 kbps
	Video	200.0.30.17/29	30	640 kbps
CUENCA	Datos	172.16.44.0/24	44	256 kbpa
	VoIP	172.16.47.0/24	47	128 kbps
	Video	200.0.30.25/29	30	640 kbpd
MANTA	Datos	172.16.77.0/24	77	256 kbps
	VoIP	172.16.78.0/24	78	128 kbps
	Video	200.0.30.81/29	30	640 kbps
SANTO DOMINGO	Datos	172.16.67.0/24	67	256 kbps
	VoIP	172.16.68.0/24	68	128 kbps
	Video	200.0.30.73/29	30	320 kbps
VILLA FLORA	Datos	172.16.249.0/24	249	256 kbps
	VoIP	172.16.58.0/24	58	128 kbps
	Video	200.0.30.65/29	30	320 kbps
SAN RAFAEL	Datos	172.16.250.0/24	250	256 kbps
	VoIP	172.16.87.0/24	87	128 kbps
	Video	200.0.30.89/29	30	320 kbps

1.1.3 Tunel IP

El túnel que se ha realizado en la red WAN MPLS es el canal de datos con una capacidad mínima de 128 kb y máxima de 512kb como se puede apreciar en la Tabla 3. En la actualidad existen tres formas de realizar el tunelado IP, como son IPIP[4], SIT[5] y GRE[6]. [4]

Tabla 3.Túnel IP en la Ciudad y Provincia de Loja

TUNNEL IP			
UBICACIÓN	DESCRIPCIÓN	BANDWIDTH	PROVEEDOR
HOSPITAL MILITAR	Datos	128Kb/128Kb	Telconet
C. SAN AGUSTÍN	Datos	128Kb/128Kb	Telconet
IESS	Datos	128Kb/128Kb	Telconet
POLICLÍNICO	Datos	128Kb/128Kb	Telconet
CARIAMANGA	Datos	256Kb/256Kb	Telconet
VIEJA MOLIENDA	Datos	512Kb/512Kb	Telconet

[4] IP sobre IP
[5] Site to site
[6] Generic Routing Protocol

1.1.4 Esquema de red WAN MPLS

Esta tecnología está implementada en siete ciudades, en las cuales se ha realizado pruebas de calidad de servicio en cada centro asociado, con el fin de concluir si el proveedor está cumpliendo con los requisitos solicitados por el departamento de telecomunicaciones, en dichas pruebas se comprobó que la calidad de servicio que prestan los servidores están en los rangos de ancho de banda que corresponden. Se ha realizado pruebas de los tres canales en cada centro asociado, comprobando la consistencia en sus resultados (ANEXO 2).

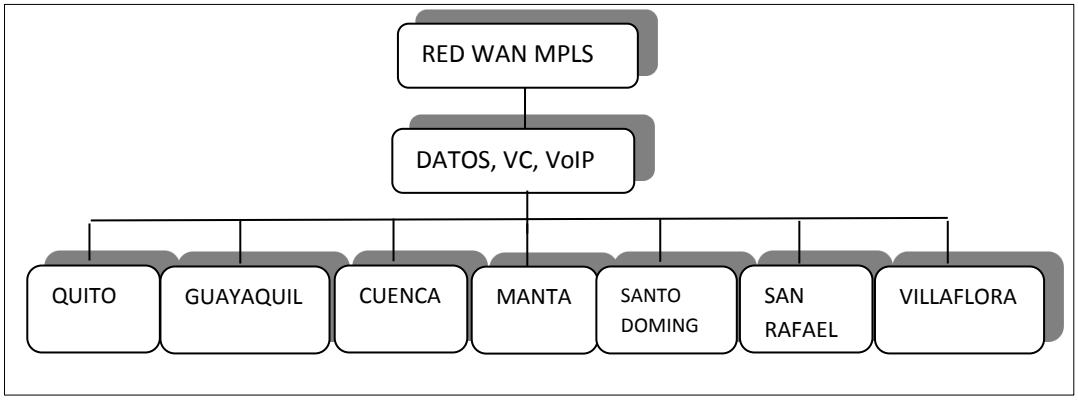


Figura 2. Esquema de red WAN MPLS

1.1.5 Descripción física de los centros regionales

Centro regional Quito – Guayaquil - Cuenca

En el centro regional Quito se dividió el ancho de banda en dos partes. 1Mbps para lo que es internet, y 3,3 Mbps para los canales de Video (1.5Mbps), Datos (512kbps) y VoIP[7] (384kbps). Como se observa en la Figura 3, se está utilizando un método de encapsulamiento nativo de cisco llamado Dot1q, [5] para permitir el encapsulamiento de VLANs diferentes, en este caso las que se utiliza en los tres canales. En el canal de internet se utiliza un Switch de capa 3, para configuración de protocolos de enrutamiento RIP, y finalmente se brinda el servicio de internet. También se tiene configurado un enlace para aulas virtuales. Cada canal cuenta con su propia VLAN para transmitir los datos.

Los centros regionales son similares en su estructura, su configuración es estática con un protocolo enrutado Ipv4, en la actualidad no se está utilizando ningún protocolo de enrutamiento dinámico, solo direcciones estáticas para realizar la transmisión de datos entre dispositivos, pero los IOS de los dispositivos están actualizados para soportar cambios modernos en la red como pueden ser la implementación de protocolos de enrutamiento dinámico.

[7] Voz sobre IP

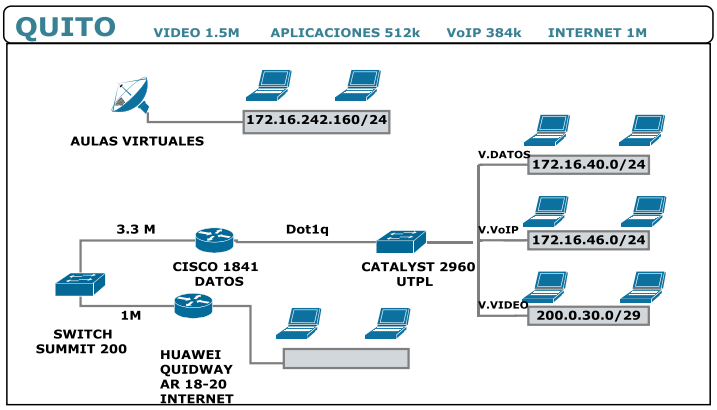


Figura 3. Centro regional QUITO

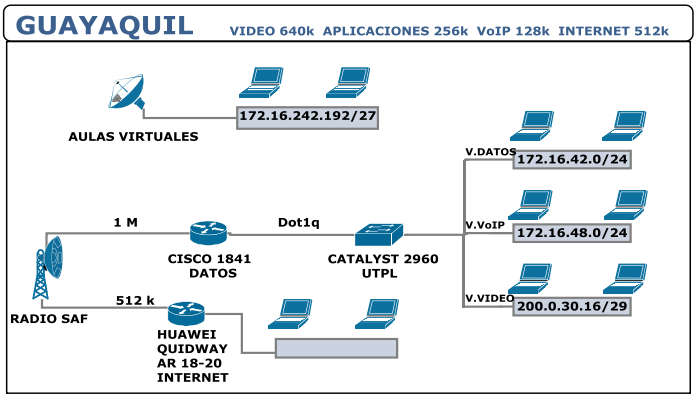


Figura 4. Centro regional GUAYAQUIL

La topología de red de centro asociado de Guayaquil es muy similar a la de Quito, con la única diferencia en los anchos de banda, como se puede apreciar en la Figura 4. En el centro regional de Cuenca existe la misma diferencia, solo la topología de red es similar y los anchos de banda son diferentes.

Centro regional Loja

Por medio de fibra Óptica [7], se transmiten 10 Mbps para el servicio de internet, que se distribuye a través de la dirección de red 172.16.1.0/24 y 3,5 Mbps para los canales de: Datos (1.5Mbps), VoIP (768kbps) y Video (1.2Mbps). Se tiene implementado una antena RADIO SAF 1E1 [8], [9] para enviar la señal (1Mbps) por microondas para el servicio de aulas virtuales. Éste es un transceptor que se lo utiliza para enviar y recibir la señal entre dos equipos.

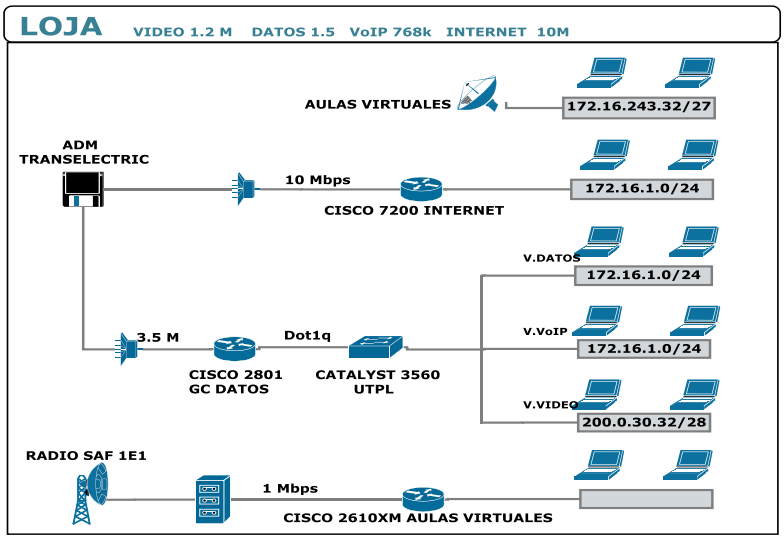


Figura 5. Centro regional LOJA

Centro regional Manta – Villaflora – Santo Domingo

Estos tres centros regionales tienen una estructura física y configuración de los dispositivos similar, con la diferencia de su direccionamiento de red.

Tabla 4. Direccionamiento de red

CENTRO REGIONAL	SERVICIO	DIRECCIÓN DE RED
MANTA	Datos	172.16.67.0/24
	Video	172.16.73.0/29
	VoIP	172.16.68.0/24
VILLAFLORA	Datos	172.16.249.0/24
	Video	172.16.64.0/29
	VoIP	172.16.58.0/24
SANTO DOMINGO	Datos	172.16.77.0/24
	Video	172.16.80.0/29
	VoIP	172.16.78.0/24

El dispositivo principal por donde la señal se transmite es el Conversor de Fibra Ethernet, que transforma la señal de fibra óptica a fibra Ethernet para poder distribuirla. Luego se utiliza un Router y un Switch para enviar por un solo canal físico la información de las tres VLANs. Cada VLAN tiene un canal lógico por donde se transmite la información, y esta información puede viajar entre el Router y el Switch por medio del encapsulamiento nativo Dot1q. De esta forma se utiliza los canales de Datos, VoIP y Video. Este centro también tiene el servicio de aulas virtuales para la interacción maestro-alumno.

Todos los canales varían en su ancho de banda debido a que en algunos lugares se los utiliza con más frecuencia, tal es el caso de las grandes ciudades, y en otros lugares casi no se los utiliza debido a la falta de tecnología o simplemente porque no hay una gran necesidad de utilizar un servicio, pero si otros. Es por esto que cuando se realiza

una conexión con un servicio, existen centros asociados que no tiene una buena transmisión de servicios, debido a la variación del ancho de banda. Cuando se realiza las pruebas esto se puede notar por el retardo de la señal, pixelación o en un caso extremo la desconexión del servicio. Esto ha sucedido en pruebas reales y lo que se hace es variar los anchos de banda para mejorar la señal y conocer cuál es el ancho de banda más apropiado.

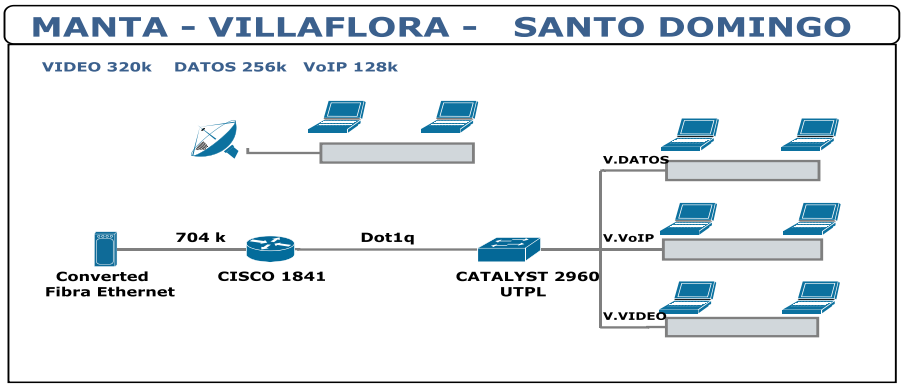


Figura 6. Centro regional MANTA – VILLAFLORA – SANTO DOMINGO

Centro regional San Rafael

A diferencia de los otros centros, se utiliza dos antenas de radio SAF [6] para enviar la señal vía microonda, el ancho de banda de estas antenas es de 320kbps y 384kbps como se muestra en la Figura 7. Dentro del canal físico tenemos tres canales lógicos, Datos (256kbps), VoIP (128kbps) y Video (320kbps). Se aplica encapsulamiento entre el Router y los Switch para poder transferir ancho de banda por diferentes VLANs.

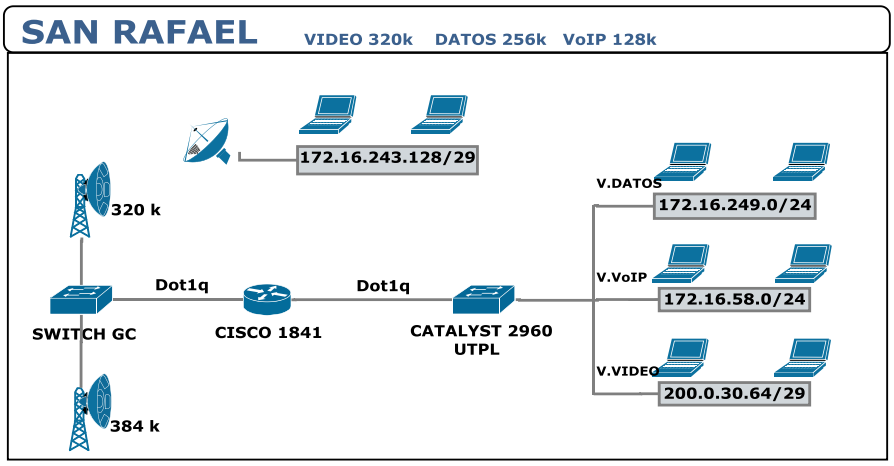


Figura 7. Centro regional SAN RAFAEL

1.1.6 Revisión de la configuración de los dispositivos de la red WAN MPLS de la UTPL

En cada Router existen dos interfaces, la FastEthernet 0/0 y la FastEthernet 0/1 las cuales tienen sub-interfaces por las cuales se conectan los servicios de Datos, VoIP, videoconferencia, y administrador. La configuración de QoS[8] es igual en todos los dispositivos routers. Las tablas de enrutamiento nos indican por donde se va la información y hacia donde esta re-direccionada.
En cada centro asociado se tiene un canal físico que es por donde se transmite los diferentes servicios que van de forma encapsulada por canales lógicos para poder transmitir con diferentes direcciones y en diferentes VLANs.

Configuración de los Routers de los Centros Asociados

En el ANEXO 3, se puede visualizar el archivo de configuración del router de Quito, el cual cuenta con dos interfaces, una para el enlace WAN y otra para los servicios que presta, los cuales están distribuidas de acuerdo a su uso, como son: video conferencia, datos, voz IP y administración del dispositivo. Se aplica calidad de servicio, la cual está configurada con precedencia 3, 4, 5 en orden de importancia de menor a mayor, siendo así el servicio más importante, el de Aplicaciones, seguido de video conferencia y voz sobre IP. La tabla de enrutamiento que se puede observar en el ANEXO 4, nos indica que algunas direcciones no pasan por capa 2, a las cuales se les antepone la letra (C) indicando que están conectadas directamente, mientras otras direcciones pasan por capa 3 y se les antepone la letra (S) indicando que están configuradas con direcciones estáticas.
En el resto de los centros asociados la configuración de los routers es similar, lo que cambia es el direccionamiento y las tablas de enrutamiento debido a que las direcciones de red utilizadas son diferentes. En cuanto a la topología que se utiliza, en todos los centros asociados es similar. Toda esta información se puede apreciar en los archivos de configuración de los Routers que están desde el ANEXO 3 hasta el ANEXO 16. El resumen de cómo está conectado y que interfaces de los dispositivos se utiliza esta resumido en una tabla en el ANEXO 17.

1.2 Discusión

Las configuraciones de los centros asociados tienen en común una topología que hay que tomar en cuenta al momento de realizar la simulación de la red, además su configuración es similar lo que nos simplificaría un poco el trabajo.

Se debe tomar en cuenta que cada centro asociado presta tres servicios diferentes y que cada uno tiene su propio ancho de banda.

Si trabajamos con un algoritmo de enrutamiento dinámico, se debe tomar en cuenta que la configuración cambiará mucho y que algunos datos como configuraciones estáticas

[8] Calidad De Servicio

no se podrá apreciar en la nueva configuración, pero si se tomará como información necesaria para conocer cómo debe estar direccionada la red.

Es muy importante la parte de los IOS actualizados de los dispositivos, los cuales soportan algoritmos de enrutamiento en el caso de implementarlos.

Existen algunas configuraciones a tomar en cuenta como son el encapsulamiento para prestar los servicios y la calidad de servicio aplicado a los tres servicios que presta la red WAN de la UTPL.

En resumen lo que nosotros tenemos claro hasta ahora es como está estructurada la red, la configuración de sus diferentes dispositivos y como se enlazan entre ellos, que tipo de servicios prestan, cuál es su ancho de banda. Esto nos da una perspectiva de cómo está la red WAN de la UTPL, nos da una idea global, que nos permite conocer el estado actual.

2

CAPÍTULO

ANÁLISIS DE LOS PROTOCOLOS ENRUTADOS Y DE ENRUTAMIENTO EN LA RED WAN MPLS

2. INTRODUCCIÓN

En la actualidad en la UTPL no se tiene implementado un protocolo de enrutamiento en la red WAN, ya que todo su direccionamiento es estático y lo que se utiliza es un protocolo enrutado IPv4 el cual está agotando sus direcciones a nivel mundial, en este capítulo se realiza una investigación acerca de los protocolos enrutados y de enrutamiento que se pueden usar en la tecnología MPLS, los tipos y características, con el fin de entender su funcionamiento y aplicabilidad en la red WAN de la UTPL para luego ser simulado en un laboratorio para entender cuales pueden ser sus beneficios.

2.1 Protocolos MPLS de enrutamiento

Los protocolos de enrutamiento sirven para intercambiar las tablas de enrutamiento y compartir la información. Nos permiten enrutar los protocolos enrutados como pueden ser protocolos IP, IPX[9], Apple Talk.

Los protocolos de enrutamiento se clasifican en IGP[10] y EGP[11]. Los protocolos IGP se clasifican a su vez en protocolos de Vector Distancia y protocolos de Estado de Enlace. Los protocolos de Vector Distancia, son los que determinan la dirección y la distancia hacia cualquier enlace en la internetwork, se clasifican en RIP, IGRP y EIGRP. Los protocolos de estado de enlace fueron diseñados para superar las limitaciones de los protocolos Vector Distancia, se clasifican en: OSPF e IS-IS. Por otra parte el EGP se clasifica en BGP[12].

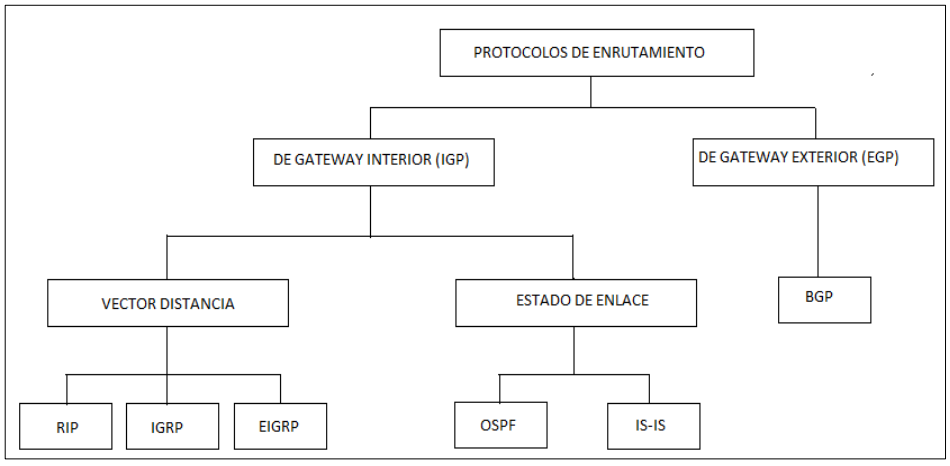


Figura 8. Clasificación de Protocolos de Enrutamiento.

2.1.1 Gateway interior

IGP: Este protocolo sirve para maximizar la capacidad de la red y disminuir los costos. Lo que hace principalmente es rutear los datos para que se dirijan a un tunelado. De

[9] Internet Packet Exchange
[10] Interior Gateway Protocol
[11] Exterior Gateway Protocol
[12] Border Gateway Protocol

esta manera evita el congestionamiento, latencia, perdida de paquetes y mejora el desempeño. Este protocolo se divide en dos:

Vector distancia

RIP[13]: Es un protocolo de encaminamiento interno que no está conectado al backbone de internet. Tiene la capacidad de inter-operar con cualquier equipo de encaminamiento. Utiliza UDP para enviar sus mensajes a través del puerto 520. Calcula el camino más corto hacia la red destino utilizando el algoritmo vector distancia. Entre las características más destacadas tenemos:

- Tienen un máximo de 15 saltos
- No utiliza subneteo
- Tiempo de actualización cada 30 seg.
- Tiempo de desactivación cada 180 seg.
- Tiempo de borrado en 300 seg.
- Distancia administrativa o de confiabilidad es de 120 en RIPv2[14]

IGRP[15]: Es un protocolo desarrollado y patentado por CISCO. Se utiliza en redes grandes, complejas y con diferentes topologías, converge más rápido que el protocolo RIP y no tiene límite de salto. Utiliza una métrica compuesta que se basa en el ancho de banda, el retardo, la confiabilidad y la carga de enlace. Cada router publica destinos con una distancia correspondiente, el router que recibe la información, ajusta la distancia y envía la información a sus routers vecinos. Entre sus principales características tenemos:

- Tiempo de actualización cada 90 seg.
- Utiliza factores distintos para determinar la métrica
- Representa la Velocidad del enlace entre los rangos de 12000Mbps y 10 Gbps.
- No tiene límites de saltos.
- Versatilidad para manejar automáticamente topologías indefinidas y complejas.
- Escalabilidad.
- Las métricas son los anchos de banda y el retardo.

EIGRP[16]: Es una versión avanzada del protocolo IGRP el cual combina las ventajas de los protocolos de estado de enlace y de vector distancia. Utiliza una métrica compuesta igual que la de IGRP, cuyas variables incluyen, ancho de banda, retardo, carga y confiabilidad. A diferencia de RIP e IGRP, este protocolo no tiene actualizaciones periódicas, sino que envía las actualizaciones cada que se produce un cambio. Cuenta con paquetes *Hello* para establecer relación con los vecinos y detectar la perdida de estos. Cuando un router receptor recibe un paquete *Hello* del router emisor, el router

[13] Routing Information Protocol
[14] Routing Information Protocol
[15] Interior Gateway Routing Protocol
[16] Enhanced Interior Gateway Routing Protocol.

receptor le envía la tabla de enrutamiento y el bit de inicialización al router emisor. [33]

Estado de Enlace

OSPF[17]: Es un protocolo de enrutamiento dinámico complejo, sofisticado, libre y soportado por la mayoría de los dispositivos destinados a realizar conexiones a la red. Cuando dice de enrutamiento dinámico se refiere a que evita las modificaciones manuales y asegura que la conexión con otros nodos sea inmediata. La estructura de este protocolo muestra que su conexión es jerárquica, que para realizar conexiones utiliza áreas separadas, las cuales se conectan a un backbone, o sea a las conexiones principales de la red que son conexiones de gran velocidad, utiliza varios dispositivos ruteadores que se los nombra de acuerdo a su uso jerárquico como puede ser un *router interno*, el mismo que tiene conectadas todas las redes de su área a un router principal. Dentro de una estructura que se basa en su jerarquía se puede encontrar varios Routers internos que controlan un área que tiene una jerarquía. Otro dispositivo es el *router de área de borde*, su función principal es conectar las áreas a un backbone o área cero para compartir la información y gestionar las redes. Por cada router interno existe un router de área de borde. El dispositivo que tiene mayor jerarquía se llama *router de backbone*[18], aquí tienen que interconectarse todas las áreas. Existen otros dispositivos que pertenecen a un área pero que su conexión a internet no la realizan mediante el área cero, a estos dispositivos se los conoce con el nombre de sistemas autónomos de router de frontera o *Autonomous System Boundary Routers. [23][25]*. Para que cada router sepa que vecino tiene utilizan el protocolo Hello y luego utilizan el protocolo de flooding donde envían una dirección del estado del anuncio (Link State Advertisements LSA) para que todos converjan a la misma base de datos que tiene cada router. Esta base de datos contiene el costo y los datos de las tablas de enrutamiento de los Routers. [24]. Las versiones actuales OSPFv2, OSPFv3 de este protocolo también soportan IPv6 y son usados para enrutamiento MPLS. Estos protocolos se basan en el costo y no en el número de saltos.

IS-IS[19]**:** Maneja una especie de mapa el cual se va creando a medida que la red converge. Utiliza el estado de enlace para encontrar el camino más corto mediante el algoritmo SPF (Shortest Past First). Emplea encapsulamiento para los paquetes. Es muy parecido a OSPF pero lo diferencias las ventajas que tiene como compatibilidad IPv6 que le permite conectar redes con encaminamientos distintos.

2.1.2 Gateway exterior

BGP: Border Gateway Protocol. Este protocolo principalmente lo que realiza es un intercambio de información de las tablas de rutas de los Routers externos de cada

[17] Open Shortest Path First.
[18] principales conexiones troncales de Internet (columna vertebral).
[19] Intermediate System to Intermediate System.

sistema autónomo. Un ejemplo claro de esto son los proveedores de servicio de internet, los cuales cuentan con varios sistemas autónomos que se comunican entre sí mediante Routers externos, ellos necesitan un protocolo para enviar la información entre los Routers, aquí entra el protocolo BGP. No utiliza el protocolo de información de rutas RIP, porque no necesita conectar redes internas. Actualmente existe nuevas versiones de este protocolo como son BGP v4 y Multi Protocolo-BGP. [26] BGP v4, anuncia los prefijos de la red de los sistemas autónomos dependiendo de la política de encaminamiento. Es decir si un sistema autónomo se anuncia en la red y otra red de sistema autónomo recibe ese anuncio, entonces la información fluye, pero esto se da gracias a las políticas de encaminamiento de exportación e importación que tiene cada sistema autónomo. Se basa en políticas para realizar la conexión. Para el paso de mensajes de un sistema autónomo a otro por medio de este protocolo debe existir un protocolo de transporte llamado TCP. Una característica muy importante de este protocolo es que no usa métricas como Bandwidth, saltos, entre otros. [27]

2.2 Protocolos Enrutados

Los protocolos enrutados son un conjunto de protocolos que ofrecen información para que un router lo envíe al dispositivo correspondiente hasta llegar a su destino. Estos protocolos asignan a cada dispositivo un número de red y de host y en algunos casos solo en número de red. Estos protocolos definen el formato y uso de los campos dentro de un paquete.

Los protocolos de enrutamiento más conocidos son: Protocolos IP, IPX, DEC net, Apple Talk, Banyan VINES y XNS[20]. De estos los que pueden ejecutar en MPLS son IP, IPX y Apple Talk. [28][29][30].

IP: Forma parte de la familia de protocolos TCP/IP, y permite el transporte de paquetes de datos sin calidad de servicio. Los tres campos que se utilizan para identificar el destinatario del mensaje son: La dirección IP, dirección de equipo y la máscara de subred.

El protocolo IPX está descartado para utilizarlo debido a que sus sistemas operativos de red pertenecen a la red Novell NetWare[31], motivo por el cual no va ser tratado ya que nuestra red no es Novell.

El otro protocolo APPLE TALK también lo hemos descartado para el uso de nuestra red, porque está actualmente en desuso y se utiliza en ordenadores Mac [32], y lo que se necesita es un protocolo actual.

El protocolo que está apto para su aplicación es el protocolo IP que actualmente se está utilizando en la red WAN de la UTPL en su versión cuatro.

[20] Xerox Network Systems

Este protocolo IP es el más adecuado debido a que actualmente ya se está utilizando en la red WAN de la UTPL y es compatible con dispositivos Cisco.

El resumen de los protocolos enrutados y de enrutamiento se puede ver en el ANEXO 18, ANEXO 19 y ANEXO 42.

2.3 Discusión

- Se puede evidenciar que existen algunos protocolos de enrutamiento como el OSPF y EIGRP que de acuerdo a sus características (ver ANEXO 18) pueden servir para implementarlos en la red WAN de la UTPL.
- De los protocolos enrutados se puede decir que el protocolo IP es el más opcionado para trabajar ya que se lo utiliza actualmente en la red WAN de la UTPL y tiene una versión actualizada IPv6 que se puede llegar a implementar.
- Se ha identificado dos protocolos de enrutamiento que pueden ser los apropiados para la red WAN como es el protocolo OSPF y EIGRP. Uno universal y el otro propietario de Cisco respectivamente.

CAPÍTULO 3

PROPUESTA Y CARACTERÍSTICAS DE NUEVOS PROTOCOLOS ENRUTADOS Y DE ENRUTAMIENTO

3. INTRODUCCIÓN

La UTPL en la actualidad no está aprovechando algunos de los beneficios de una red WAN MPLS como es la implementación de algoritmos de enrutamiento dinámico, por esta razón se realizará una propuesta de simulación de algoritmo de enrutamiento para ver los posibles resultados que se puede obtener , y se aprovechara las características del mismo para cubrir los requerimientos de la red WAN de la UTPL. Para esto se escogerá un algoritmo de enrutamiento que cubra los requerimientos y se establecerá que características lo definen apropiado para esta red.

3.1 Requerimientos de la red WAN de la UTPL

Entre los principales requerimientos que la UTPL requiere para su red WAN MPLS tenemos:

- De acuerdo a la gran magnitud de la red, que los algoritmos de enrutamiento deben soportar redes grandes (más de 15 saltos) ya que los centros asociados que hemos tomado en cuenta están distribuidos en diferentes partes del País.
- Otro requerimiento es que el algoritmo de enrutamiento debe soportar la escalabilidad porque se puede dar el caso que la UTPL integre otro centro asociado a la red entonces la topología de red cambiaria un poco y el protocolo de enrutamiento debe adaptarse a este tipo de cambios.
- Se tendrá que mejorar el enrutamiento de los servicios de datos, VoIP y video en las dos versiones del protocolo enrutado, porque la UTPL tiene asignado rangos de direcciones tanto para IPv4 como para IPv6 y es necesario aprovechar estos rangos de direcciones asignados por LACNIC.
- Por parte del cliente, en este caso la UTPL, requiere un protocolo de enrutamiento que soporte los equipos cisco que actualmente se está utilizando, con el fin de sacar provecho.
- Permitir la calidad de servicio entre los servicios que presta, sobre todo la confiabilidad en la conexión y la seguridad de los datos.

3.2 Criterios de selección del protocolo de enrutamiento

Para escoger el algoritmo de enrutamiento adecuado para la red WAN de la UTPL analizaremos los siguientes criterios:

- **Topología de Red**.
  La UTPL realiza cambios en la red por su crecimiento y escalabilidad, debido a esto es necesario un algoritmo de enrutamiento que se adapte a los cambios que se pueden realizar en la red WAN de la UTPL. El mejor algoritmo de enrutamiento que se puede adaptar a esos cambios es EIGRP. OSPF queda descartado para este criterio porque requiere un modelo jerárquico lo que puede hacer que rediseñemos nuestra red, esto quiere decir que no acepta cualquier topología de red.

- **Resumen de Ruta y Dirección**.
  Los protocolos que mejor se adaptan al direccionamiento y resumen de rutas son el algoritmo de enrutamiento EIGRP y OSPF, ya que estos utilizan VLSM para manejar mascaras de subred variables que hacen que no se desperdicie direcciones de red u host en una red.

- **Velocidad de Convergencia**.
  De los protocolos de enrutamiento que se vio en el capítulo 2, los que más rápido convergen son el OSPF y EIGRP, porque realizan una búsqueda de ruta alternativa en el caso de que la ruta asignada no se encuentre habilitada y al hacerlo convergen más rápido que otros protocolos de enrutamiento conocidos. Esto se debe a que no consume mucha memoria ni recursos del CPU en el caso de EIGRP y sobre todo se realiza una combinación de las métricas para encontrar la ruta más rápida. De estos dos algoritmos de enrutamiento el que más nos conviene es el algoritmo de enrutamiento EIGRP porque consume menos recursos y utiliza criterios adicionales como ancho de banda, retardo, carga y confiabilidad en las métricas.

- **Selección de Ruta**.
  Para seleccionar la ruta, el algoritmo EIGRP es el más adecuado ya que realiza una combinación de métricas para seleccionar la ruta a la cual necesita llegar. OSPF utiliza la métrica de ancho de banda, pero lo mejor es utilizar combinaciones de métricas para establecer mejor una ruta.

- **Capacidad de ampliación**.
  En este criterio lo que se analiza es el consumo de ciclos de CPU y anchos de banda. EIGRP (protocolo vector distancia) consume menos ciclos de CPU y menos ancho de banda, en cambio, OSPF (estado de enlace) utiliza más ciclos de CPU pero menos ancho de banda. Para escoger el protocolo adecuado tenemos que darnos cuenta que EIGRP es un algoritmo de enrutamiento DUAL porque pertenece a los dos tipos de protocolos de enrutamiento, entonces dependería de nosotros con cual utilizarlo, en cambio OSPF pertenece a un solo tipo de protocolo de enrutamiento y no se puede escoger. Por la facilidad de escoger con que trabajar es mejor el algoritmo de enrutamiento EIGRP.

- **Sencillez de simulación**.
  Los algoritmos de enrutamiento de vector distancia como RIP, IGRP, y EIGRP no requieren demasiado esfuerzo en la planificación ni en la topología para ejecutarse de forma eficaz, en cambio, los algoritmos de enrutamiento de distancia administrativa requieren escoger una sola topología de red, así mismo se debe tener mucho cuidado con el modelo de direccionamiento. Por estos motivos escogemos EIGRP en este criterio.

- **Seguridad**.
  Los dos protocolos más opcionados OSPF y EIGRP utilizan poderosos métodos de autenticación como es MD5, por lo que en este criterio se puede escoger cualquiera de los dos protocolos.

- **Compatibilidad**.
  En este criterio debemos tomar en cuenta lo que tiene el cliente(UTPL), con lo que contamos actualmente, la UTPL tiene actualmente equipos Cisco en la red WAN, y es conveniente sacarles el mayor provecho para que rindan de mejor manera, por lo que se puede decir que el Protocolo de enrutamiento EIGRP es el más opcionado. En caso de que la UTPL contara con equipos diferentes a los de Cisco, entonces estaríamos hablando de escojer el algoritmo de enrutamiento OSPF, ya que este algoritmo es universal.

A continuación presentamos una tabla resumen de los criterios de selección para el algoritmo de enrutamiento dinámico en la cual se puede evidenciar cual es el algoritmo de enrutamiento que se va a simular.

Tabla 5. Resumen de criterios de selección del algoritmo de enrutamiento

CRITERIOS	**PROTOCOLOES DE ENRUTAMIENTO**	
	OSPF	**EIGRP**
TOPOLOGÍA DE RED		✓
RESUMEN DE RUTAS Y DIRECCIÓN	✓	✓
VELOCIDAD DE CONVERGENCIA	✓	✓
SELECCIÓN DE RUTAS	✓	✓
CAPACIDAD DE AMPLIACIÓN		✓
SENCILLEZ DE SIMULACIÓN		✓
SEGURIDAD	✓	✓
COMPATIBILIDAD	✓	✓

Como se puede observar en la tabla anterior el algoritmo que proponemos para el proyecto es el algoritmo de enrutamiento EIGRP por los criterios antes mencionados. En el capítulo 2 se realizó un estudio de los algoritmos de enrutamiento según sus características, en el ANEXO 20 se puede observar que las características que cumple el protocolo de enrutamiento EIGRP también lo hacen apto para la simulación.

3.3 Análisis de las Características de los Protocolos Enrutados

En el capítulo 2 vimos que el algoritmo más opcionado es el algoritmo de enrutamiento IP el cual tiene dos versiones IPv4 e IPv6.

Entre sus principales características tenemos:

- Protocolo no orientado a conexión, esto quiere decir que se moverá de forma libre y puede ser enrutado por cualquier ruta, pero no garantiza la recepción del paquete. [5]

- Fragmentación de paquetes, se da en caso de que el ruteador no transporte datagramas tan grandes, entonces se realiza una fragmentación del mismo.
- Otra de las características que tienes es que si un paquete no es recibido permanece por un tiempo finito, y luego se destruye.
- Su direccionamiento puede ser mediante direcciones lógicas de 32bits dependiendo de con que versión del protocolo estemos trabajando.

Actualmente las máquinas vienen configuradas para manejar estos dos versiones de protocolos IPv4 e IPv6 en sistemas operativos Windows.

3.4 Comparación de Protocolos Enrutados IP

De acuerdo a las características de ambos protocolos que hemos analizado, nos podemos dar cuenta que tienen bastantes diferencias [38]. Para poder apreciar de mejor manera estas diferencias ver el ANEXO 19. En caso de que se requiera un mejor rendimiento, seguridad, más espacio de direccionamiento y autoconfiguración se tendrá que aplicar IPv6. Pero se cree conveniente aplicar los dos algoritmos enrutados porque se encuentran en transición actualmente.

3.5 Propuesta de algoritmos enrutados y de enrutamiento

De acuerdo al estudio realizado en los capítulos 2 y 3 de este proyecto, proponemos el uso del algoritmo de enrutamiento EIGRP por su compatibilidad con los requerimientos de la UTPL y por sus características. De igual forma el algoritmo enrutado propuesto es el algoritmo enrutado IP, porque está en pleno uso en la UTPL y porque es un protocolo que tiene una versión más reciente que cumplirá especificaciones futuras como puede ser la Movilidad IP, de esta forma queda asentado el uso de estos dos protocolos para las pruebas, simulación e implementación de la red WAN de la UTPL con el propósito de mejora y aprovechar la tecnología MPLS que tiene la UTPL en la actualidad.

3.6 Discusión

- Podemos acotar que el protocolo de enrutamiento más óptimo para la aplicabilidad de enrutamiento dinámico que hemos escogido para proponer es el protocolo de enrutamiento EIGRP, por sus características y compatibilidad con los factores que tenemos en la UTPL como son los de carácter físico como los dispositivos y de carácter lógico como es el protocolo EIGRP, de acuerdo a la fiabilidad y dificultad de aplicarlo.
- El protocolo enrutado que elegimos para la simulación es el protocolo IP por la fiabilidad su estandarización que tiene con los dispositivos, y porque es un protocolo que es aplicable en los dispositivos CISCO.
- Estos protocolos han sido elegidos porque cumplen con los requerimientos de la UTPL que se explicó en este capítulo y las características que tienen estos protocolos son los más adecuados para la red WAN de la UTPL.

CAPÍTULO 4

ANÁLISIS DE USO DE ALGORITMOS DINÁMICOS EN EL ENRUTAMIENTO DE LA RED WAN MPLS DE LA UTPL

4. INTRODUCCIÓN

Para estar seguros de que el algoritmo de enrutamiento EIGRP es el adecuado para la red WAN de la UTPL se realizará un análisis de factibilidad de los algoritmos de enrutamiento, ventajas, desventajas y problemas que se pueden dar en la simulación. Teniendo claro los conceptos y características de cada protocolo de enrutamiento.

4.1 Análisis de factibilidad y simulación de algoritmo de enrutamiento RIP

- **Factibilidad de RIP**
  El algoritmo de enrutamiento RIP no es factible para la red WAN de la UTPL porque está diseñado para redes LAN, redes pequeñas de no más de 15 saltos. Esto significa que cuando la red WAN de la UTPL tiene cambios puede sobrepasar el número de saltos que soporta RIP y este protocolo quedaría inservible, además si supera el número de saltos se crea un bucle de enrutamiento y consumiría bastante ancho de banda y la red colapsaría. Otro punto a considerar es que utiliza tiempos de respuesta, lo cual hace que nuestra red se vuelva lenta en caso de que los paquetes se extravíen en la red.

- **Simulación de RIP**
  En la simulación este algoritmo de enrutamiento no tendría problemas con los dispositivos Cisco porque es de uso universal, puede ser configurado para cualquier dispositivo en la red WAN de la UTPL. Pero si tendría problemas con el tipo de red. En este caso, el tipo de red es WAN.

- **Problemas de RIP**
  Algunos de los problemas que pueden surgir en la red WAN de la UTPL son:

  - Diámetro pequeño.- no se puede extender más de 15 saltos.
  - Convergencia lenta: la tabla de rutas demora en reflejar como está actualmente la red porque las rutas se eliminan cada 180 segundos.[40]

4.2 Análisis de factibilidad y simulación de algoritmo de enrutamiento IGRP

- **Factibilidad de IGRP**
  Este protocolo es factible en la red WAN de la UTPL siempre y cuando los dispositivos de la red sean CISCO. Este protocolo es propietario de CISCO, por lo que no es compatible con otros dispositivos que no sean CISCO.

- **Simulación de IGRP**
  Este algoritmo de enrutamiento se puede simular en la red WAN de la UTPL. Pero no cubre todos los requerimientos que se vió en el capítulo 3 para la red WAN de la UTPL. Uno de estos requerimientos es que sea confiable y que converja de forma rápida, y existe un algoritmo de enrutamiento que es más confiable que este.

- **Problemas de IGRP**
  Algunos de los problemas que tiene IGRP son:

- Actualizaciones periódicas, se demora en actualizar las rutas de direccionamiento porque las rutas se eliminan cada 270 segundos por lo que no converge rápido.
- No tiene soporte para VLSM, es decir que existe desperdicio de host en la red porque no soporta el cambio de mascara de subred, lo que significa que existe una excesiva perdida de direcciones IP para los host.
- Consume un alto porcentaje de ancho de banda.

4.3 Análisis de factibilidad y simulación de algoritmo de enrutamiento EIGRP

- **Factibilidad de EIGRP**

  Este protocolo de enrutamiento de acuerdo al estudio que se realizó en el capítulo 3 cumple con los requerimientos de la red WAN de la UTPL porque es el más confiable de todos los algoritmos que se ha estudiado, no consume ancho de banda ni recursos exagerados, utiliza VLSM para no desperdiciar las direcciones IP, es compatible con los dispositivos CISCO que se utiliza en la red WAN de la UTPL y soporta redes grandes con más de 15 saltos.

- **Simulación de EIGRP**

  Este algoritmo de enrutamiento se puede simular porque es compatible con los dispositivos cisco que utiliza en la red WAN de la UTPL, es compatible con los IOS que se utiliza en cada dispositivo ya que soportan este algoritmo y el algoritmo enrutado IP en sus dos versiones, se adapta a los cambios de topología de la red, las actualizaciones las realiza solamente cuando ocurre un cambio en la topología o en los routers vecinos con lo que ahorra tiempo y esfuerzo.

- **Problemas de EIGRP**
  - No todos los IOS de los dispositivos CISCO son compatibles con este algoritmo de enrutamiento, por lo que hay que actualizar algunos IOS de los dispositivos si es necesario.
  - Si un dispositivo de la red WAN de la UTPL no es CISCO el protocolo de enrutamiento no es apto para simularlo.

4.4 Análisis de factibilidad y simulación de algoritmo de enrutamiento OSPF

- **Factibilidad de OSPF**

  Este protocolo es factible porque es un protocolo universal cumple con casi todos los requerimientos de la red WAN de la UTPL, excepto con la topología, para simular OSPF es necesario un modelo jerárquico, caso contrario no se puede simular, esto es una restricción porque no se puede simular OSPF en cualquier topología de red.

- **Simulación de OSPF**

  Es posible simularlo en la red WAN de la UTPL porque es un protocolo universal, y cumple con la mayoría de los requerimientos de la red WAN de la UTPL.

- **Problemas de OSPF**
  - Solo se puede adaptar a topologías jerárquicas.
  - Consume más ciclos de CPU, esto afecta a la capacidad de ampliación de la red.
  - Su configuración se complica, esto puede traer problemas en la simulación sobre todo en cuestión de tiempo.
  - Menor confiabilidad que EIGRP.

A continuación presentaremos una tabla resumen de los algoritmos de enrutamiento.

Tabla 6. Resumen de comparación de protocolos de enrutamiento

CARACTERÍSTICAS	RIP	IGRP	OSPF	EIGRP
Tipo	Vector distancia	Vector distancia	Estado de enlace	Dual
Convergencia	Lento	Lento	Rápido	Rápido
Soporta VLSM	No	No	Si	Si
Consumo de ancho de banda	Alto	Alto	Bajo	Bajo
Consumo de recurso de los equipos	Bajo	Bajo	Alto	Bajo
Escalamiento	No	Si	Si	Si
universal o propietario	Universal	Cisco	universal	Cisco

4.5 Factibilidad de la simulación de un nuevo protocolo enrutado.

En la actualidad la red WAN de la UTPL ha implementado enrutamiento estático en algunos dispositivos (Routers) con el protocolo enrutado IPv6. Esta transición se debe a que la Universidad es una institución que requiere ir creciendo por su cobertura a nivel nacional e internacional con sus extensiones (modalidad a distancia) en varios países y su requerimiento de mejores servicios con QoS (Datos, VoIP, video conferencia) y porque el protocolo enrutado IPv6 tiene mejoras con respecto a su versión anterior Ipv4 que son notables en rendimiento.

La factibilidad del protocolo IPv6 se debe a que la UTPL está en constante evolución y las direcciones IPv6 prestan grandes ventajas en cuanto a su rango de direcciones que es más amplio con respecto a su versión anterior que está agotando su rango de direcciones IP. IPv6 está diseñado para redes grandes (WAN) que es a lo que apunta la UTPL. IPv6 tiene más tipos de direcciones que su versión anterior lo cual nos permite una mejor distribución de las redes, también facilita la simulación de modelos para asegurar QoS sobre los servicios de Datos, VoIP y Video conferencia que presta la UTPL en los centros asociados.

Otro factor que beneficia la simulación de IPv6 como protocolo enrutado son los equipos CISCO que actualmente disponen en la red WAN en los centros asociados de la UTPL como los modelos de Routers CISCO 7200, 2901 y 1841 y modelos de Switch Catalyst 2960 que soportan IPv6.

El enrutamiento de IPv6 es eficaz y jerárquico porque utiliza varios tipos de direcciones entre las principales están las direcciones globales que tiene en cuenta múltiplos niveles de proveedores de servicios de internet (ISP). Sus tablas de enrutamiento son mucho más pequeñas que en su versión anterior. También realiza la configuración de direcciones con y sin estado para simplificar la configuración de los host. [39].

4.6 Factibilidad de la Simulación de un nuevo protocolo de enrutamiento.

Después de analizar cada algoritmo de enrutamiento (capítulo 3) y escoger EIGRP como el protocolo de enrutamiento más óptimo para la simulación en este proyecto, debemos justificar porque es factible el uso de este protocolo en la red WAN de la UTPL.

El protocolo de enrutamiento EIGRP fue escogido por una serie de características que son beneficiosas para aplicar QoS en los servicios que prestamos en los centros asociados, adaptabilidad a cambios de crecimiento que existan en la red, así también por su compatibilidad con los dispositivos CISCO que actualmente cuenta la UTPL. Una de las principales características que se tomó en cuenta fue la escalabilidad (crecimiento de la red y adaptabilidad a los cambios), la fiabilidad (distancia administrativa) y el balanceo de carga en los servicios que presta la UTPL.

Este protocolo de enrutamiento es factible porque nos permitirá mejorar el estado actual de la red WAN, dando servicios que son explotados para mejorar su funcionalidad y establecer conexiones con mejor prestación de servicios entre los centros asociados disminuyendo el retraso de la señal, la pixelación en el caso de la video conferencia, así como la perdida de paquetes en los tres servicios.

Este protocolo nos permite establecer una mejor comunicación cuando se transmite la señal o cuando tenemos una videoconferencia múltiple entre los distintos centros asociados.

En el ANEXO 21 se ha realizado una simulación del algoritmo de enrutamiento EIGRP básico y configuraciones de los dispositivos routers y Switch.

4.7 Discusión

- Es de gran importancia recalcar que el algoritmo de enrutamiento EIGRP se lo escogió porque los dispositivos de la red WAN de la UTPL son CISCO y estamos viéndolo del lado del cliente. Además cumple con las características de la red WAN de la UTPL vista en el capítulo 3 y 4.
- También se escogió EIGRP porque tiene algunas ventajas sobre OSPF, aunque los dos protocolos se pueden simular.

5 DIRECCIONAMIENTO IPV6

CAPÍTULO

5. INTRODUCCIÓN

En la UTPL se implementó IPv6 de forma estática, en algunas partes de la red como son el CORE, ASA y el Router de Borde, para comenzar a realizar un direccionamiento de nuestra red WAN en los centros asociados, nosotros debemos realizar una investigación acerca de las los tipos de direcciones ipv6 y del estado actual de la red WAN con direcciones IPv6, esto se lo realiza con el fin de afianzar nuestros conocimientos, poder realizar un direccionamiento y esquema en IPv6 y conocer como está actualmente implementado IPv6 en algunos dispositivos de la red.

5.1 TIPOS DE DIRECCIONES EN IPV6

En IPv6 tenemos un mayor número de tipos de direcciones, estas las describiremos a continuación para entender el protocolo IPv6.

- **Unicast:** En este tipo de direccionamiento se realiza una conexión uno a uno, los paquetes se envían a una sola interface. Entre los direccionamientos de tipo unicast más importantes tenemos:
  - **Global Unicast Addresses:** Es una dirección global única que identifica a una empresa o institución, es como una dirección publica en IPv4. actualmente la UTPL cuenta con una dirección global única que es asignada por LACNIC, es necesario aclarar que dentro de ICANN [16] [19], que es una corporación sin fines de lucro encargada de asignar nombres y números para internet, se encuentra una subdivisión de acuerdo al número de continentes, y para el continente de centro américa y sur américa esta LACNIC quien administra esta zona para el internet. La dirección que fue asignada por LACNIC y con la cual se identifica a nivel mundial la UTPL es 2800:130.1::/32. [11]. Por los general los tres primeros bits del prefijo de ruteo global de estas direcciones comienzan con 001, lo que quiere decir que el primer número hexadecimal siempre será dos. Este número lo identifica como dirección global única. El ID de la subred, identifica una subred dentro del sitio, es decir, identifica en que subred de la empresa o institución se encuentra conectado. El ID de la interface, lo que hace es utilizar los últimos 64 bits para identificar a un host (dispositivo o máquina conectada a la red) de forma única, con lo cual se sabe el lugar exacto del host. Por lo general este número hexadecimal esta dado automáticamente por el dispositivo o se lo puede configurar manualmente mediante EUI-64.

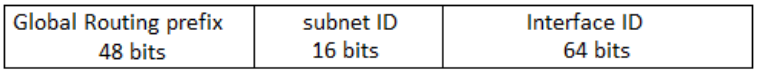


Figura 9. Formato de dirección única global. [5]

En la Figura 10, mostramos un ejemplo de cómo puede simularse una dirección global única en la red de la UTPL, este es un ejemplo ficticio en la cual tenemos tres

campus, el principal que sería la UTPL, los otros dos serian centros asociados en Quito y Guayaquil. De igual forma hemos puesto tres departamentos. Esto con la finalidad de un mejor entendimiento de las direcciones globales únicas.

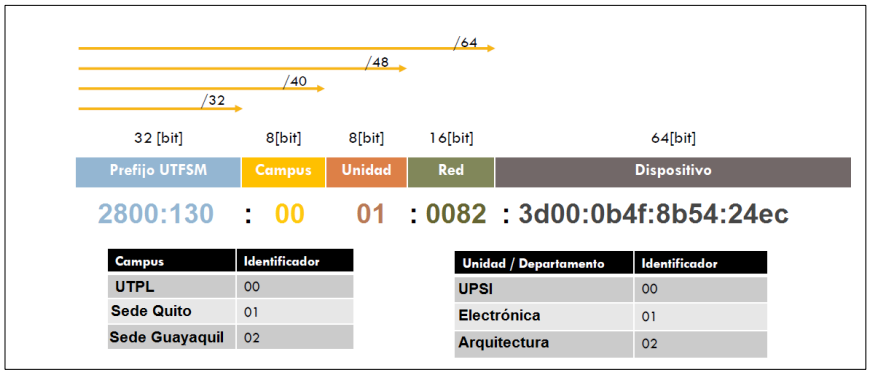


Figura 10. Ejemplo ficticio de dirección global única [14] [37]

- **Local al enlace (Link Local):** Es una dirección que se utiliza en redes dentro de la empresa, pero no pueden enrutarse entre routers, pueden existir direcciones link local iguales en segmentos diferentes de la red dentro de la empresa, el identificador de la máquina se lo puede realizar mediante EUI-64, pero en nuestra red interna de la UTPL el identificador esta dado automáticamente y aleatorio en cada nodo. Se puede decir que son como las direcciones privadas en IPV4 con formato IPV6. Estas direcciones solo se pueden utilizar en redes físicas en la que el nodo está conectado.

  El primer campo hexadecimal de la izquierda siempre comienza por 1111 1110 10 que es igual a FE80::. El formato de link local es el siguiente. [12][21]

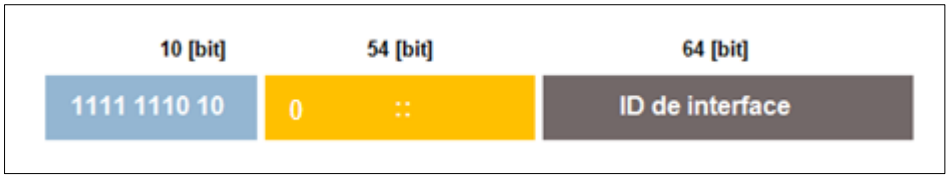


Figura 11. Formato Link Local [18] [19]

- **Local al sitio: (Site-Local):** Este tipo de direccionamiento se lo considera como privado, la diferencia que tiene con el link local, es que este no se repite dentro de una red interna, entre segmentos de una red no se repiten las direcciones. Esto quiere decir que se puede tener dos redes LAN[21], y las direcciones locales al sitio se pueden comunicar entre ellas, pero no se pueden re-encaminar hacia internet, es por esta razón que no necesita un prefijo global.[21]

[21] Red de área local

El primer campo hexadecimal de la izquierda siempre comienza por 1111 1110 11 que es igual a FEC0. El formato de "Site Local" es:

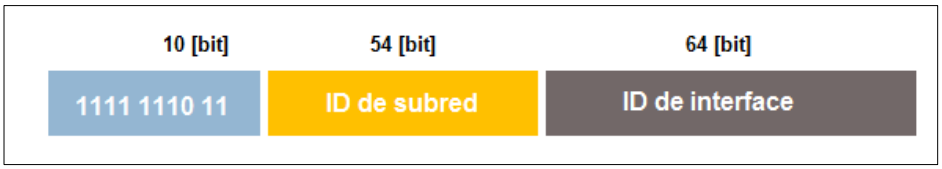


Figura 12. Formato Site Local [18] [19]

Otros tipos:

- **La dirección no especificada:** entre sus principales características tenemos:
  - Esta dirección es usada para especificar que no existen direcciones IPv6.
  - No debe ser asignada a ningún nodo.
  - No debe ser utilizada como dirección destino de paquetes IPv6.
  - No debe ser utilizada en cabeceras de enrutamiento IPv6
  - Si se asigna como dirección origen, nunca debe ser enviado por un routerIPv6.

  Se la identifica porque todos sus campos hexadecimales son ceros (0:0:0:0:0:0:0:0 = ::).

- **Dirección de Loopback:** esta dirección normalmente es usada por los nodos para enviarse paquetes así mismos, entre sus características principales tenemos:
  - Nunca debe asignarse a interfaces físicas
  - No debe ser utilizada como dirección IP origen en paquetes IPv6.
  - Nunca debe ser enviada fuera del nodo.
  - Nunca debe ser reenviado por un router IPv6.

  Se la identifica porque su último campo hexadecimal es uno (::1).

- **Direcciones IPv6 con IPv4 embebidas**

  Existen dos tipos:

  - **Compatibles con IPv4:** este tipo de direccionamiento es utilizado en la transición de IPv4 a IPv6, por lo general se lo utiliza para enviar paquetes enrutados dinámicamente mediante un tunelado que se crea a través de la infraestructura de enrutamiento establecida en IPv4. El formato que tiene es el siguiente.

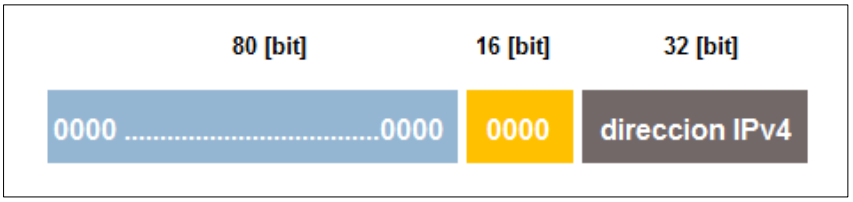


Figura 13. Formato compatible con IPv4 [18] [19]

- **IPv4 mapeadas a IPv6:** este tipo de direccionamiento se lo realizó para poner las direcciones IP en formato IPv6 a los nodos en el inicio de la transición de las direcciones IP. El formato es el siguiente.

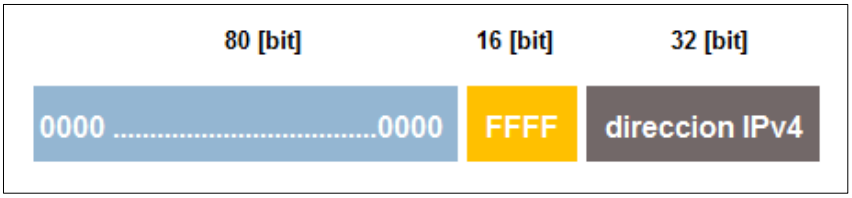


Figura 14.Formato IPv4 mapeadas a IPv6 [18] [19]

¿Cómo se pone la ID de interface manualmente?

Como lo indicamos anteriormente, mediante EUI-64, para entender esto lo explicare con un ejemplo:

Si tenemos una dirección IPV4 172.16.30.181 cuya dirección MAC es 00-26-22-AE-FE-C4. Para identificar nuestra dirección única IPV6 global, primero tendremos el prefijo de ruteo global, que es 2800:130:1, luego la ID de subred, que en nuestro caso sería la VLAN a la que pertenece, según la IPV4 nuestra VLAN es la 30, luego el identificador único que consta de 64 bits que lo sacamos de la siguiente manera:

Tomamos en cuenta la dirección MAC IPV4, y en la mitad le agregamos el numero hexadecimal FFFE, de la siguiente manera.

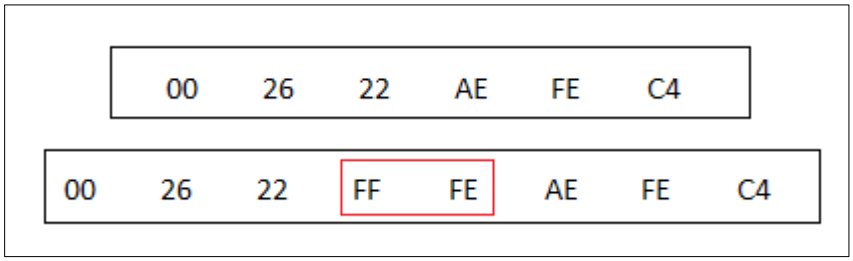


Figura 15.Agregando FFFE [20]

Luego de esto transformamos todo a binario y modificamos el séptimo bit por uno.

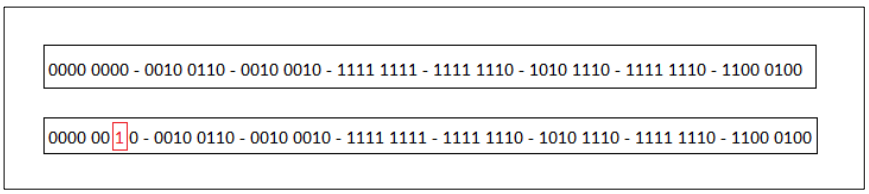


Figura 16.Modificamos el séptimo bit [20]

Ahora transformamos todo a código hexadecimal, para obtener la dirección MAC en IPV6

0226: 22FF: FEAE: FEC4

Entonces, la dirección global única nos queda de la siguiente manera.
2800: 130: 1: 30: 0226: 22FF: FEAE: FEC4
Esta parte en las direcciones IP por lo general es generado por los nodos (máquinas). [RFC 2373][RFC 2374]

- **Multicast:** este direccionamiento tiene variedad de usos en cuanto a sus direcciones IP**.** Identifica varias interfaces que se encuentran en diferentes nodos, su formato esta dado de la siguiente manera. Los primeros 8 bit corresponden a la identificación multicast que en hexadecimal se representa como "FF", los siguientes cuatro bit, de los cuales el último cambia y en este caso lo tenemos identificado con la letra "T" en la Figura 17.[21][22]

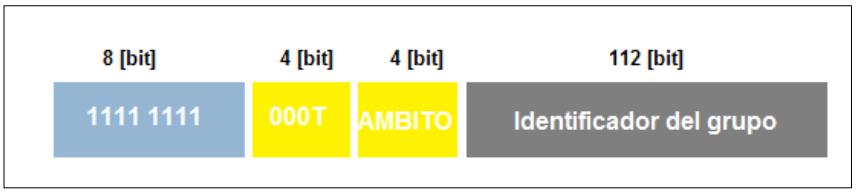


Figura 17.Formato Multicast [18] [19]

Cuando toma el valor de cero, identifican una dirección permanente, que la asigna la autoridad de numeración global de internet. Cuando toma el valor de uno, identifica que es una dirección temporal. Los siguientes cuatro bits, que corresponden al "ámbito" tienen los siguientes significados que se muestran en la tabla siguiente. [13][15][17]

Tabla 7. Significado de bit Ámbito en multicast [34]

0	Reservado
1	Ámbito local del nodo
2	Ámbito local del enlace
3	No asignado
4	No asignado
5	Ámbito local del sitio
6	No asignado
7	No asignado
8	Ámbito local de la organización
9	No asignado
A	No asignado
B	No asignado
C	No asignado
D	No asignado
E	Ámbito global
F	Reservado

En el direccionamiento Multicast, tenemos múltiples asignaciones de direcciones que tienen diferentes usos en el direccionamiento. Esto lo podemos ver en el ANEXO 22.

- **Anycast:** Este direccionamiento identifica a un conjunto de interfaces, cuando enviamos un paquete a una dirección Anycast, envía los paquetes a todas las interfaces que están conectadas a esta dirección, pero entrega el paquete a la interface más cercana, determinada utilizando OSPF o el estado de los enlaces (RIP). Es difícil distinguir una dirección Anycast de una Unicast debido a que utilizan la misma sintaxis, y son asignadas del espacio de dirección Unicast, por lo que pueden utilizar cualquier formato definido de las direcciones Unicast.
  Para poder diferenciar una dirección Anycast de una Unicast se debe revisar su configuración y observar si la dirección está asignada a más de una interface. Puesto que este tipo de direccionamiento es nuevo, se debe tomar algunas medidas preventivas de uso:
  - Las direcciones Anycast no se deben utilizar como direcciones origen en IPv6.
  - Tampoco pueden ser asignadas a un host, solo se las puede asignar a los Routers.

5.2 Análisis del enrutamiento de la red WAN MPLS

El enrutamiento de la red WAN MPLS esta implementado en parte, en la red interna y externa, en la actualidad todas las empresas están migrando a IPv6, es así que el 1% de las conexiones a internet están con IPv6, esto representa un avance significativo, debido a que las direcciones IPv4 están en declive, actualmente se estima que existe un 14% de direcciones IPv4 y se prevé que para el 2012 ya no existan direcciones IPv4 [10], lo que se está realizando en la red de la UTPL es una transición al nuevo protocolo IPv6, ya que esa es la tendencia a futuro. En la actualidad la red en IPv6 asignada por LACNIC para la UTPL es la 2800: 130::/32 y de acuerdo a este rango de redes debemos simular el resto de la red en los centros asociados, pero antes de eso revisaremos el enrutamiento actual de la red WAM MPLS.

5.2.1 Enrutamiento desde DMZ hacia Internet

La UTPL compro a LACNIC un prefijo de direcciones IPv6 que es 2800:130::/32 [52]. En la UTPL la red que tiene implementado IPv6 tiene la siguiente configuración para las direcciones IPv6.

Tabla 8. Configuración de Dirección Global

PREFIJO		VLAN		OCTETO IPV4
2800:130:1	:	222	:	156

Esto se hace con el objetivo de saber a qué VLAN pertenece dentro de la red de la UTPL y que dirección tiene en IPv4, ya que están en un proceso de transición.

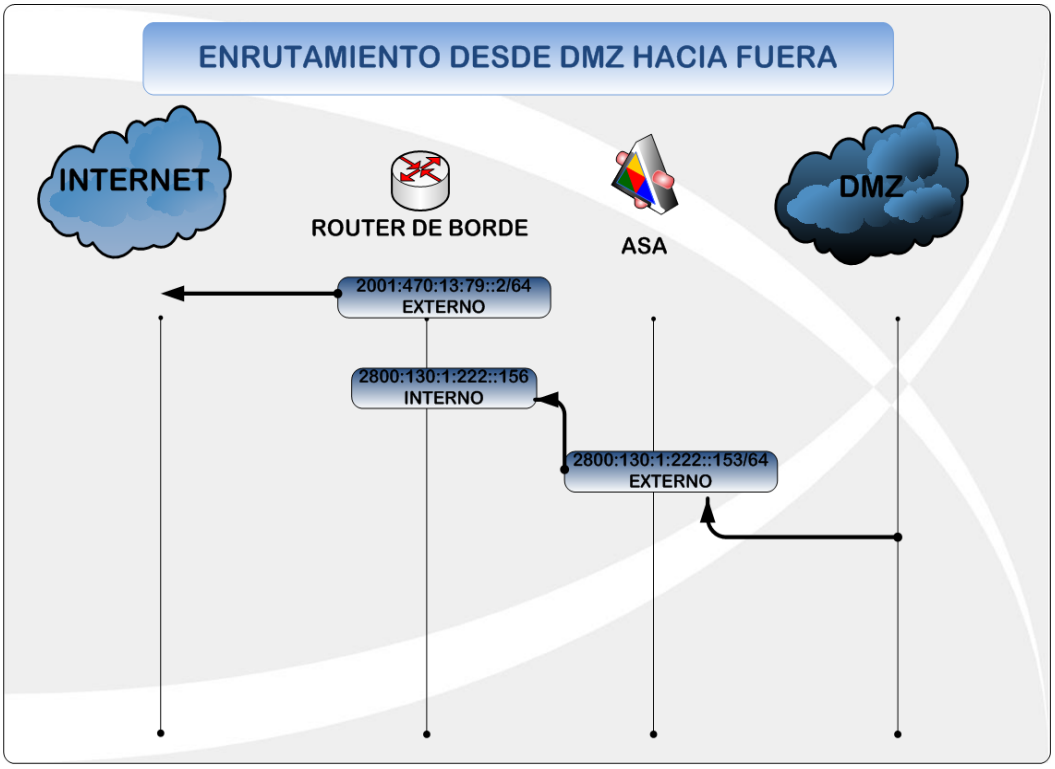


Figura 18. Enrutamiento desde DMZ hacia internet

La DMZ[22][10], por lo general se encuentra entre una red LAN y WAN, sirve para mostrar aplicaciones de los servidores internos pero sin permitir el ingreso a la parte interna de la red desde la parte externa. A la DMZ se puede ingresar desde la parte interna y externa.

La DMZ está compuesta por diferentes servidores que nos permiten mostrar el frontal de la UTPL, el mail, y trabajar con otros servidores que prestan diferentes utilidades.

La DMZ se conecta directamente al ASA[23], esto quiere decir que no pasa por capa 3 del modelo OSI[24], (capa de red) y no es necesario enrutar. En la Figura 18, se ilustra como salen los paquetes de datos hacia el internet, para esto debemos conocer que cada dispositivo tiene varias interfaces, y que cada interface tiene configurado una dirección en IPv6. A las interfaces que reciben los paquetes les he denominado INTERNO, mientras las que entregan, les denomine EXTERNO. La DMZ por estar conectado directamente al ASA entrega la información sin ninguna configuración de capa 3, el ASA enruta estos paquetes hacia el router de borde, quien a su vez se encargara de que los paquetes se enrutan hacia el internet. La configuración del ASA la podemos ver en el ANEXO 23 y ANEXO 24.

[22] Zona desmilitarizada
[23] Dispositivos de Seguridad Adaptativos de Cisco
[24] Open System Interconnection

5.2.2 Enrutamiento desde Internet hacia la DMZ

Para el enrutamiento desde el Internet hacia la DMZ se utiliza las mismas rutas de direccionamiento que vemos en la Figura 18, pero de forma inversa. Aquí nos encontramos con dos niveles de seguridad en dispositivos como son el Router de Borde, que realiza un primer control con las listas de acceso, esto permite que algunas direcciones no tengan permisos de ingresar hacia el siguiente dispositivo. Luego tenemos un control en el servidor ASA, desde el cual se puede ingresar a los servidores externos, DMZ o al CORE.

5.2.3 Enrutamiento desde el CORE hacia Internet

El enrutamiento para enviar paquetes de datos desde la red interna de la UTPL hacia el internet, comienza con el CORE, el cual esta enrutado hacia el servidor ASA, este a su vez está apuntando hacia el ROUTER DE BORDE, y de aquí se envía los datos hacia la parte externa. De igual manera el direccionamiento en IPv6 se lo puede visualizar en la Figura 19, En el cual, el CORE consta de una interfaz con direccionamiento externo, que apunta hacia la interfaz interna del servidor ASA, dentro del servidor ASA se realiza una conmutación para enviar los datos por la interfaz externa del mismo, hacia el ROUTER DE BORDE que recibe la información mediante la interfaz interna y luego se conmuta para direccionarla hacia la interfaz externa que sale al internet.

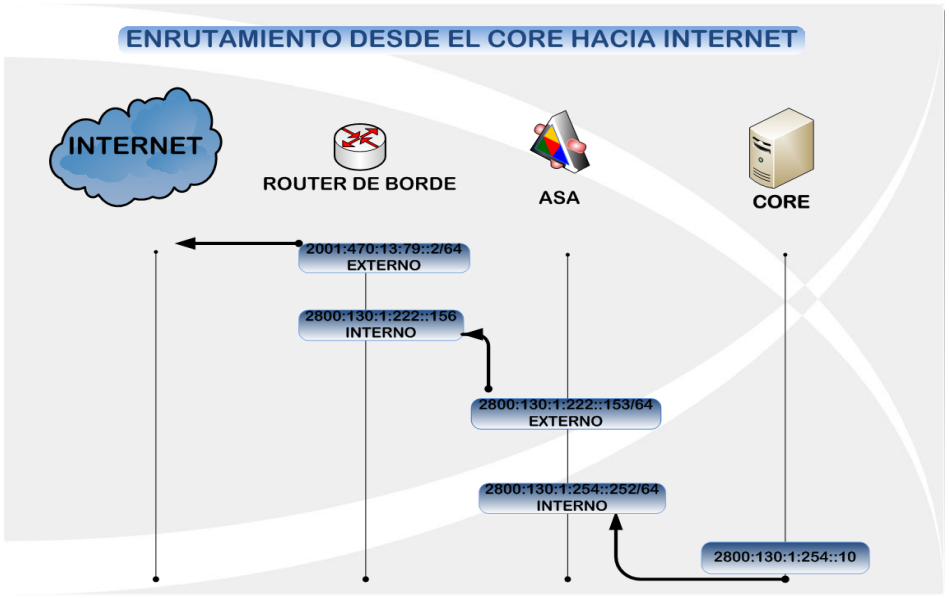


Figura 19.Enrutamiento desde el CORE hacia Internet

5.2.4 Enrutamiento desde Internet hacia el CORE.

En el CORE, se encuentran todas los dispositivos y redes internas de la UTPL, además tenemos cuatro niveles de seguridad que se pueden identificar. El primer nivel de seguridad se encuentra en las máquinas, las cuales están provistas de un antivirus, el

segundo nivel se lo identifica en el CORE, el cual mediante listas de control de acceso puede permitir el ingreso o bloqueo de direcciones IP, luego está el servidor ASA, que aplica ACLs en forma más restrictiva y finalmente el Router de Borde, que da la cara hacia el internet.

Generalmente el enrutamiento de entrada hacia el CORE, está dado desde el router de borde hacia el servidor ASA, luego se realiza el enrutamiento hacia el CORE, en donde se distribuye la información hacia la parte interna de la red. El direccionamiento se lo puede ver en la Figura19. Utiliza el mismo direccionamiento de entrada como de salida de datos.

En la Figura 20, se ilustra el estado actual del enrutamiento IPV6 en la UTPL hasta donde esta implementado. Como se puede ver, la parte de centros asociados esta por implementarse IPV6 con enrutamiento dinámico, que es lo que corresponde realizar en este proyecto.

5.2.5 Enrutamiento actual de la red con IPv6 en la UTPL

Ya hemos explicado el enrutamiento de forma separada, como se puede llegar de la DMZ hacia el internet y como se llega desde el CORE hacia el internet. Ahora se muestra el esquema en su totalidad. Como se puede observar en la Figura 20, muestra el enrutamiento actual implementado en IPv6 en la red de la UTPL. Se puede observar que dentro del CORE se encuentran varias interfaces lógicas, cada una con una dirección IPv6 (Gateway), cada interface lógica tiene asignada una VLAN (red lógica independiente dentro de una red física) que por lo general pertenece o identifica un departamento. Esto corresponde a la red interna de la UTPL, este CORE se enruta con el ASA, que a su vez también tiene varias interfaces lógicas, en donde tiene configurados algunos servidores que muestran la parte externa, como son, las páginas de la UTPL, como pueden ser el E.V.A, mail, utpl.net, entre otros. El ASA es una especie de firewall interno de la red, que a su vez esta enrutado con el Router de Borde, que es el que da la cara hacia el internet.

En el ANEXO 25. Podemos ver la lista completa de las VLANs que se ven en la gráfica siguiente.

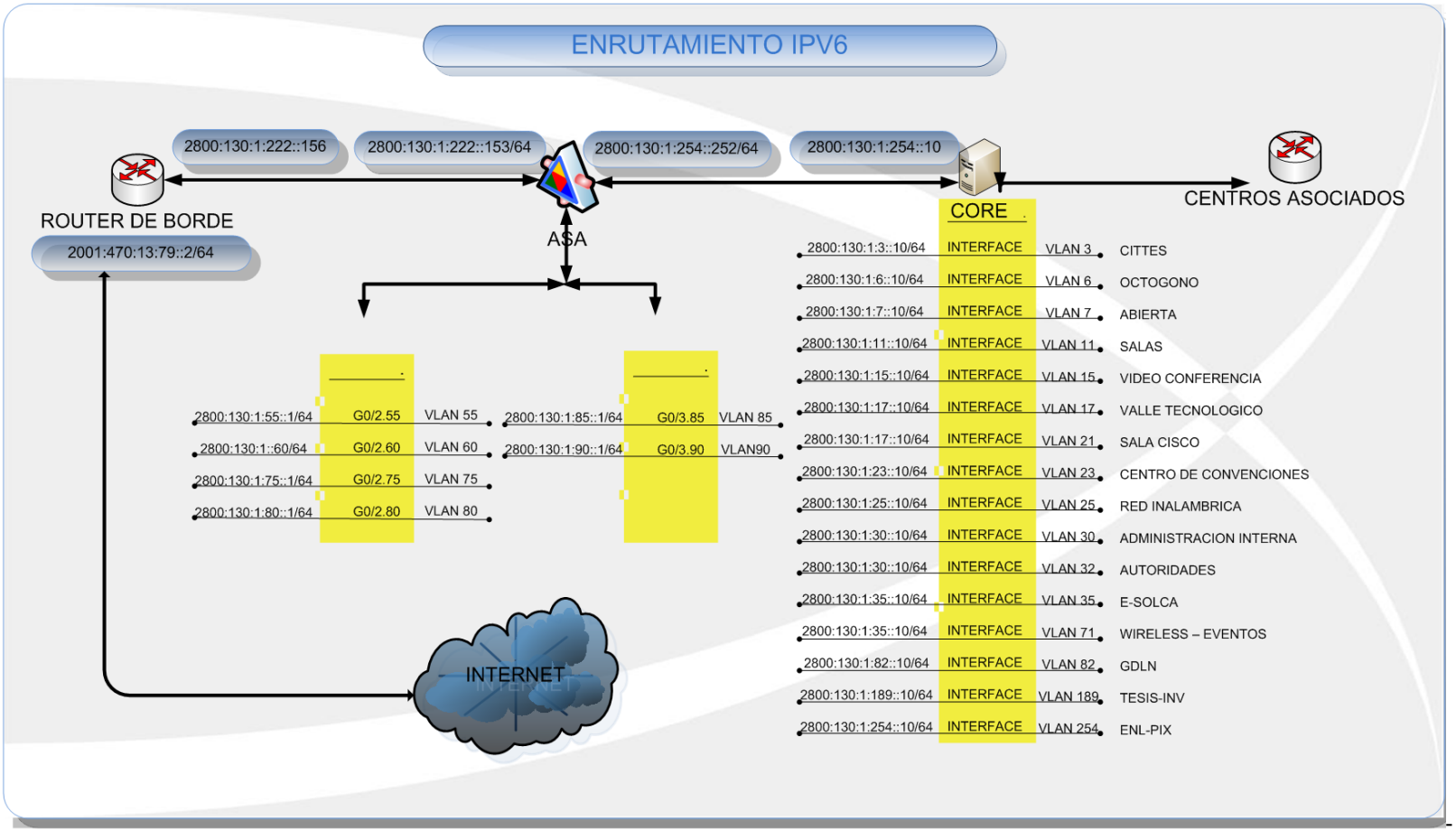


Figura 20.Enrutamiento Actual IPv6 en la UTPL

Este análisis de cómo está actualmente implementado ipv6 en la UTPL nos introduce al tema de ipv6 aunque esta implementación es estática.Se muestra que sectores ya están cubiertas con ipv6. Como se puede ver en la Figura 20, los centros asociados no tienen implementado IPv6.

5.3 Tabla de direccionamiento en IPv6

En este capítulo se establecerá el enrutamiento ipv6 para realizar la simulación en GNS3 para esto lo primero que se ha realizado un direccionamiento de acuerdo a la red que se tiene disponible en ipv6, de acuerdo a esta red nosotros procedemos a realizar un subneteo en ipv6.

Para esto hemos tomado la red 2800:130:1::/32 que está asignada a la UTPL, esta red tenemos que transformarla a un /56 para poder obtener 256 subredes que nos servirán en el direccionamiento de nuestra red. Es importante recordar que los primeros 64 bits están asignados a la red, y estos se subdividen en 48 bits de red y 16 bits de subred, los siguientes 64 bits están asignados a hosts.

Aclarado este punto procedemos a obtener la nueva red que sería la siguiente 2800:139:1:0000::/56, como nos podemos dar cuenta existen 8 bits que se los puede utilizar para subredes, estos 8 bits se transforman en 256 subredes que salen de las combinaciones que existen entre los números del 1-9 y las letras de la A-F. Estas subredes se las puede subnetear para sacar nuestras redes para integrarlas a los routers. Podemos utilizar el /64, /112, /126, y /128, el /127 no se lo utiliza por cuestiones de seguridad.

En caso de que se obtenga algún enlace punto a punto o punto host, se utilizará las dos últimas subredes para poder identificar de que se trata de un tunelado. En este caso se tendrá que utilizar las subredes 2800:139:1:00FF::/64 y 2800:139:1:00FE::/64 respectivamente y luego subnetear para obtener direcciones reservadas para esos routers o hosts. De modo que tendríamos direcciones reservadas a /128 para este tipo de tunelado. [42], [43], [44], [45]

En la tabla 9, se ha creado un direccionamiento para implementarlo en la red WAN, la cual tiene direcciones de red para los Routers que se utilicen con el protocolo de enrutamiento EIGRP.

Estas direcciones de red están relacionadas directamente con la Figura 21, que también se creó para implementarlo en un simulador.

Tabla 9. Propuesta de Direccionamiento IPv6 para los centros regionales.

RED	2800:130:1::/32
RED A SUBNETEAR	2800:130:1:0100::/56

CENTROS ASOCIADOS	**DISPOSITIVOS**	**DIRECCIONES DE RED**	**INTERFACES**	**DIRECCIONES**
QUITO	R2 CISCO 2691	2800:130:1:0101::/64	F0/0	2800:130:1:0101::1/64
		2800:130:1:0108::/64	S0/0	2800:130:1:0108::1/64
	R1 CISCO 2691	2800:130:1:0108::/64	S0/0	2800:130:1:0108::2/64
		2800:130:1:0114::/64	F0/0	2800:130:1:0114::2/64
GUAYAQUIL	R6 CISCO 2691	2800:130:1:0102::/64	F0/0	2800:130:1:0102::1/64
		2800:130:1:0109::/64	S0/0	2800:130:1:0109::1/64
	R5 CISCO 2691	2800:130:1:0109::/64	S0/0	2800:130:1:0109::2/64
		2800:130:1:0114::/64	F0/0	2800:130:1:0114::3/64
CUENCA	R8 CISCO 2691	2800:130:1:0103::/64	F0/0	2800:130:1:0103::1/64
		2800:130:1:0110::/64	S0/0	2800:130:1:0110::1/64
	R7 CISCO 2691	2800:130:1:0110::/64	S0/0	2800:130:1:0110::2/64
		2800:130:1:0114::/64	F0/0	2800:130:1:0114::4/64
LOJA	R4 CISCO 2691	2800:130:1:0100::/64	F0/0	2800:130:1:0100::1/64
		2800:130:1:0107::/64	S0/0	2800:130:1:0107::1/64
	R3 CISCO 2691	2800:130:1:0107::/64	S0/0	2800:130:1:0107::2/64
		2800:130:1:0114::/64	F0/0	2800:130:1:0114::1/64
SANTO DOMINGO	R10 CISCO 2691	2800:130:1:0104::/64	F0/0	2800:130:1:0104::1/64
		2800:130:1:0111::/64	S0/0	2800:130:1:0111::1/64
	R11 CISCO 2691	2800:130:1:0111::/64	S0/0	2800:130:1:0111::2/64
		2800:130:1:0114::/64	F0/0	2800:130:1:0114::5/64
MANTA	R16 CISCO 2691	2800:130:1:0105::/64	F0/0	2800:130:1:0105::1/64
		2800:130:1:0112::/64	S0/0	2800:130:1:0112::1/64
	R17 CISCO 2691	2800:130:1:0112::/64	S0/0	2800:130:1:0112::2/64
		2800:130:1:0114::/64	F0/0	2800:130:1:0114::6/64
SAN RAFAEL	R15 CISCO 2691	2800:130:1:0106::/64	F0/0	2800:130:1:0106::1/64
		2800:130:1:0113::/64	S0/0	2800:130:1:0113::1/64
	R14 CISCO 2691	2800:130:1:0113::/64	S0/0	2800:130:1:0113::2/64
		2800:130:1:0114::/64	F0/0	2800:130:1:0114::7/64

En el ANEXO 43 también se puede visualizar la propuesta para la configuración de las VLANs en IPv6

5.4 Esquema de red en Simulador

Una vez obtenido este direccionamiento nosotros tendremos que construir un esquema de red para poder simular nuestra red en un simulador como es el caso del simulador GNS3, aquí lo que se realiza primeramente es la configuración tanto de los IOS de cada router como del Quemu, que viene hacer una especie de PC en Linux para hacer más real la simulación, en caso de no consumir muchos recursos es aconsejable utilizar VPCS, pero solo se puede simular nueve máquinas y a veces sale un error de estética del programa que molesta al momento de trabajar. Otra solución es convertir los routers en PCs.

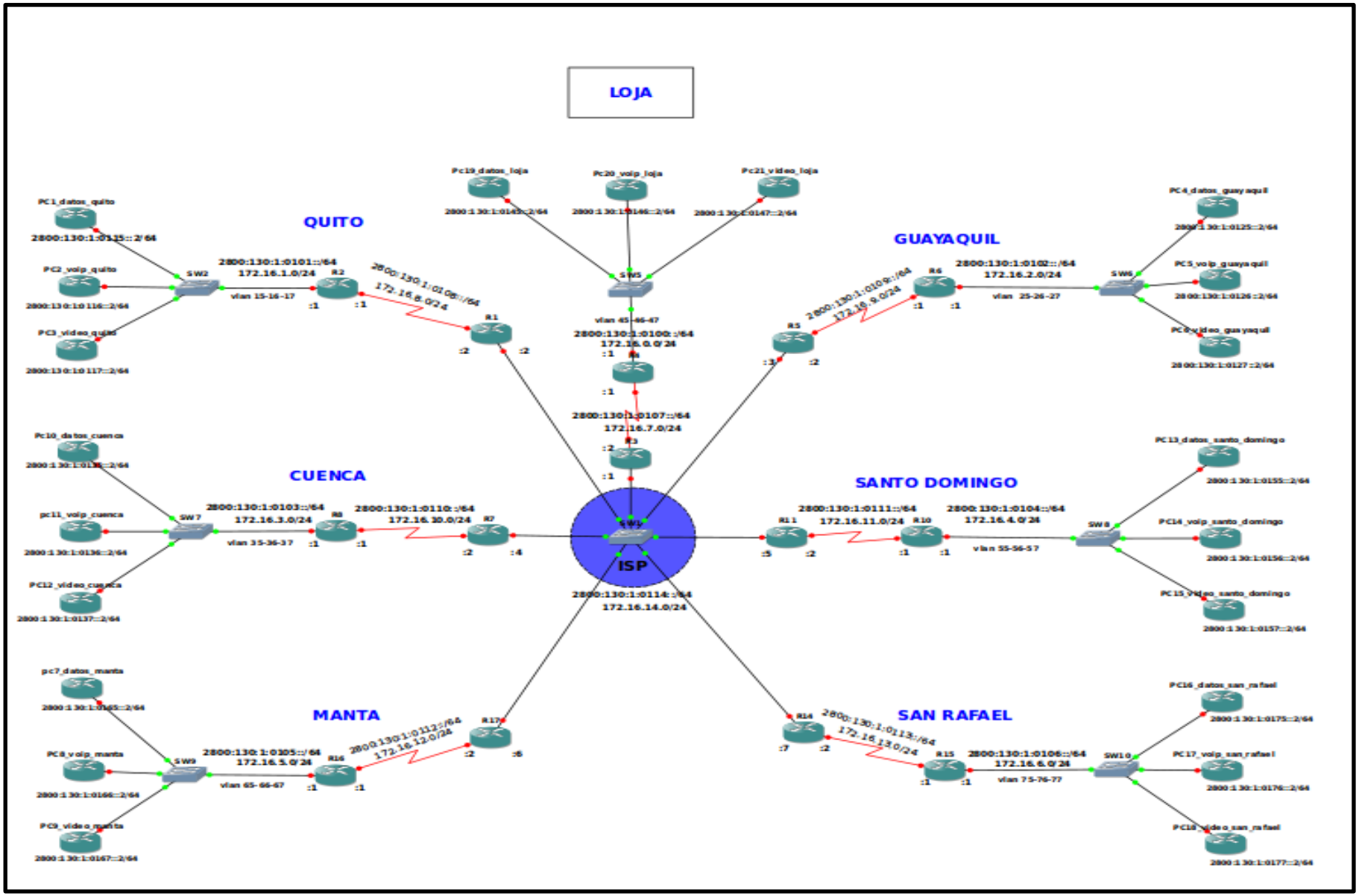


Figura 21.Esquema de simulación para la red WAN MPLS

5.5 Discusión

El análisis de enrutamiento de la red WAN de la UTPL sirvió para entender como está actualmente configurado IPv6 en la red, y esto nos introdujo a la investigación de direccionamiento IPv6, como resultado de esta investigación, se pudo apreciar que el direccionamiento en esta parte de la red está de forma estática y que las direcciones ipv6 están relacionadas con las direcciones ipv4 para poder identificarlas fácilmente.

En este capítulo se ha desarrollado con éxito una tabla de direccionamiento en ipv6 para implementarla en un simulador de pruebas. El direccionamiento se lo realizó en base a la investigación que se hizo acerca subneteo IPv6 y los tipos de direcciones ipv6 que se investigó.

En el simulador GNS3 se encontró algunos problemas de compatibilidad al momento de realizar el esquema ya que el simulador utiliza IOS reales de los dispositivos de la red WAN MPLS, por lo que es recomendable asegurarse de que el IOS que se va a utilizar en el dispositivo tenga los puertos suficientes para trabajar en lo que se quiere hacer.

CAPÍTULO 6

SIMULACIÓN DE ALGORITMO DE ENRUTAMIENTO

6. INTRODUCCIÓN

En este capítulo ya se tiene información necesaria para simular el algoritmo de enrutamiento escogido, como es el algoritmo de enrutamiento EIGRP, por lo que se procederá a simular en GNS3 parte o toda la red que está en el esquema, dependiendo de los requerimientos del simulador, se procederá a realizar la configuración y mostrar resultados de la configuración del protocolo de enrutamiento, lo cual quedará como constancia del trabajo realizado, la configuración se la realizará con IOS reales de los dispositivos CISCO por lo que es necesario un computador moderno. Se detallará las configuraciones para una mejor comprensión de la aplicación de EIGRP con IPv4 e IPv6.

6.1 Recomendaciones

Antes de realizar la práctica es recomendable tener un mínimo de 4GB de memoria RAM en el computador ya que el IOS del router ocupa como mínimo de 128 Mb a 164 Mb de memoria por cada dispositivo. Se debe tomar en cuenta que se utilizará como mínimo 20 dispositivos routers simulados, lo cual nos ocupa una considerable parte de la memoria que puede traer consecuencias en la parte de rendimiento del computador y posiblemente el reinicio de la misma.

La simulación se está realizando en Ubuntu 10.10 ya que en Windows XP y Windows 7 se registró errores de compatibilidad y mal uso de la memoria RAM. También se está utilizando un IOS (c2691-advipservicesk9-mz.124-15.T6.bin) [49] compatible con EIGRP para que se reconozcan todos los comandos de EIGRP como los de IPv6.

6.2 Pasos para simulación de EIGRP con IPV4

*Se tomará como ejemplo el **router R2 de la red de Quito** (ver Figura 21) para realizar los pasos de la configuración. Los pasos que se siguieron para la realización de la simulación de este proyecto son:*

6.2.1 Direccionamiento IPv4

Se estableció un direccionamiento adecuado de acuerdo al direccionamiento IPv6 que se realizó en el capítulo 5 para que no exista confusión y seguir con la misma dirección.

Tabla 10. Configuración de dirección IPv4 en las interfaces de los routers

Comandos de Configuración para el direccionamiento	
Comando o Acción	**Propósito**
Quito> enable	Modo privilegiado EXEC
Quito# configure terminal	Modo de configuración global
Quito#(config) interface fa0/0	Ingresa a la interface
Quito#(config-if) IP address 172.16.1.1 255.255.255.0	Dirección local al enlace

Esta configuración se debe realizar en todos los dispositivos routers de la red con su respectiva dirección de red y dirección IP.

6.2.2 Configuración de algoritmo de enrutamiento EIGRP con IPv4.

Ahora vamos a configurar EIGRP en los dispositivos routers de la red, para esto estamos tomando como ejemplo el Router R2 de Quito (ver Figura 21). Lo que se realiza mediante comandos es la activación del algoritmo de enrutamiento EIGRP y se configura las redes adyacentes a este dispositivo router, en la tabla siguiente se muestra la configuración.

Tabla 11. Comandos de Activación de EIGRP para IPv4

Activación de EIGRP para IPv4	
Comando o acción	Propósito
Quito> enable	Modo privilegiado EXEC
Quito# configure terminal	Modo de configuración global
Quito #(config) interface fa0/0	Escogemos la interfaz en la cual se configurara EIGRP
Quito #(config-if) ip router eigrp 10	Entra en el modo de configuración del router y crea un proceso de enrutamiento IPv4 EIGRP
Quito #(config-router)network 172.16.1.1 0.0.0.255	Identificador de redes adyacentes
Quito #(config-router)network 172.16.8.1 0.0.0.255	Identificador de redes adyacentes
Quito#(config-router)no shutdown	Activación de la interface

Esta configuración se realiza en todos los dispositivos de la red con sus respectivas redes adyacentes.

6.2.3 Creación de VLANs y encapsulamiento dot1Q para enrutar IPv4

Primero se realiza la identificación de los Routers en donde se debe crear las VLANs, en este caso los routers que están más cerca de los Switch donde están conectadas las máquinas que tiene los servicios de Datos, VoIP y Video conferencia. Un vez identificados se procede crear las VLANs y a encapsularlas. En la siguiente tabla están ilustrados los comandos utilizados para esta configuración.

Tabla 12. configuración para las VLANs

Comandos para creación de VLANs en las interfaces	
Comando o acción	**Propósito**
Quito> enable	Modo privilegiado EXEC
Quito# configure terminal	Modo de configuración global
Quito #(config) interface fa0/0	Interface fa0/0
Creación de VLAN de datos	
Quito #(config-if) interface fa0/0.15	Crear sub-interface
Quito #(config-subif) description datos_quito	Descripción para identificar la sub-interface
Quito #(config-subif) encapsulation dot1Q	Modo de encapsulamiento
Quito #(config-subif) ip address 172.16.15.1 255.255.255.0	Dirección IPv4 global única
Quito #(config-subif) ip router eigrp 10	Entra en el modo de configuración del router y crea un proceso de enrutamiento IPv4 EIGRP
Quito#(config-router)no shutdown	Activación de la interface
Creación de VLAN de VOIP	
Quito #(config-if) interface fa0/0.16	Creamos sub-interface para VoIP
Quito #(config-subif) description voip_quito	Ponemos una descripción para identificar la sub-interface
Quito #(config-subif) encapsulation dot1Q	Modo de encapsulamiento
Quito #(config-subif) ip address 172.16.16.1 255.255.255.0	Dirección IPv4 global única
Quito #(config-subif) ip router eigrp 10	Entra en el modo de configuración del router y crea un proceso de enrutamiento IPv4 EIGRP
Quito#(config-router)no shutdown	Activación de la interface

6.2.1 Encapsulamiento dot1Q en las interfaces de los Switch

En el simulador GNS3 se puede realizar una configuración gráfica a nivel de los Switch, porque nos permite escoger el puerto, VLAN y el tipo de acceso o encapsulamiento. En esta parte se configuró la VLAN 99 como dot1Q para todos los Switch, y las otras interface que dan la cara a las PCs se las configuró con la VLAN de acuerdo al servicio que pertenecen y de tipo Access.

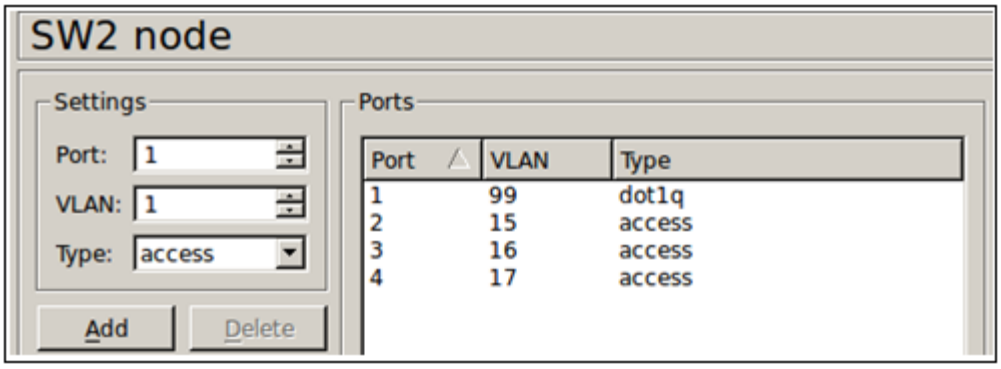


Figura 22. Configuración de un Switch

Se puede visualizar que la configuración del encapsulamiento en el Switch está realizada de forma gráfica.

6.2.2 Lista de control de Acceso ACLs

Las listas de control de acceso nos sirven para controlar el ingreso a los dispositivos por parte de otros dispositivos, en este caso se ha configurado para que una red específica de Quito que cuenta con un servicio igual al que se encuentra en la red de Guayaquil pueda ingresar, pero no podrá ingresar a otro servicio diferente.

Tabla 13. Configuración de ACLs

Comandos para Configuración de ACLs con IPv6	
Comando o acción	**Propósito**
Quito> enable	Modo privilegiado EXEC
Quito# configure terminal	Modo de configuración global
Quito# (config)# ipv6 access-list extended quito	Nombra a la ACL
Quito# (config-ipv6-acl)# permit ip 172.16.15.2 0.0.0.255 host 172.16.25.2 permit ip 172.16.16.2 0.0.0.255 host 172.16.26.2 permit ip 172.16.17.2 0.0.0.255 host 172.16.27.2 deny any any	Conexión de servicio de datos_quito con datos_guayaquil
Quito# (config)#interface se0/0	Abrir interface se0/0
Quito# (config-if)#ip access-group quito1 out	Controla tráfico de salida

Existe conectividad entre servicios iguales entre las dos redes pero no sobre servicios diferentes.

6.3 Pruebas realizadas sobre la Simulación en IPv4.

Estas pruebas están realizadas sobre la simulación que se ha creado a partir del algoritmo de enrutamiento EIGRP y el algoritmo enrutado IPv4.

Algunas de las pruebas que se realizaron se describen a continuación:

- **Configuración de las interfaces.-** lo que se realiza es una consulta para ver las interfaces configuradas. El objetivo es ver las rutas configuradas en las interfaces del router que se está analizando.
- **Interfaces configuradas con EIRGP.-** El objetivo es mostrar lo que está pasando en la interfaz. A continuación se detalla lo que se evalúa:
  - Identificar la interface sobre cual se configuró EIGRP.
  - Número de vecinos que están directamente conectados.
  - Verificar paquetes poco confiables y transmisión de colas confiables.
  - El intervalo de tiempo de ida y vuelta que toma en milisegundos.
  - Regulación del tiempo utilizado para determinar cuando los paquetes se envían a la interface.
  - Número máximo en segundos en los que el router envié los paquetes de multidifusión EIGRP.
  - Número de rutas en los paquetes en la en la transmisión de espera de cola para ser enviados.
- **Vecinos de los routers configurados con EIGRP.-** El objetivo es la verificación del funcionamiento de la tabla de vecinos de EIGRP para poder realizar la simulación de EIGRP dinámicamente. A continuación se detalla lo que se evalúa:
  - Tiempo que transcurre desde que se escucha al router vecino.
  - Tiempo necesario para que un paquete viaje hasta el router vecino.
  - Tiempo que espera para enviar otro paquete al router vecino.
  - Número de paquetes EIGRP en espera para ser enviados.
- **Protocolo en uso para el enrutamiento dinámico.-** El objetivo es Verificar:
  - Que algoritmo de enrutamiento se está utilizando.
  - Cuál es el número de sistema autónomo que se está utilizando.
  - Cuáles son las métricas que se utiliza.
  - Gateway configurado.
  - Distancia administrativa.
  - Tiempo de mantenimiento.
- **Traza de la ruta con EIGRP.-** El objetivo es verificar el funcionamiento de los algoritmos de enrutamiento y enrutado IPv4.

El desarrollo completo de las pruebas de la simulación del algoritmo de enrutamiento EIGRP y algoritmo enrutado IPv4 está en el ANEXO 34.

6.4 Pasos para simulación de EIGRP con IPV6

Se tomará como ejemplo el **router R2 de la red de Quito** (ver Figura 21) para realizar los pasos de la configuración. Los pasos que se siguieron para la realización de la simulación de este proyecto son:

6.4.1 Direccionamiento IPv6

Se realizó previamente un estudio de direccionamiento ipv6 el cual nos sirvió para conocer como esta direccionada la red.

Para que se puedan enlazar con el algoritmo de enrutamiento EIGRP nosotros tenemos que configurar ese direccionamiento con las direcciones Globales y link local, para esto existe una relación de las direcciones globales con las direcciones link local para poder identificarlas. Por ejemplo si tenemos la siguiente dirección global 2800:130:1:0101::1, la dirección link-local se escribirá de la siguiente manera fe80::0101:1. La cuarta y la octava porción de la dirección global se ubican en la séptima y octava posición de la dirección link-local para poder identificar a que red pertenece y cuál es el host según la dirección global.

Tabla 14. Configuración de dirección ipv6 global única y dirección local al enlace

Comandos de Configuración para el direccionamiento	
Comando o Acción	**Propósito**
Quito> enable	Modo privilegiado EXEC
Quito# configure terminal	Modo de configuración global
Quito#(config) interface fa0/0	Ingreso a la interface
Quito#(config-if)ipv6 address fe80::0101:1 link-local	Dirección local al enlace
Quito#(config-if)ipv6 address 2800:130:1:0101::1	Dirección Global única

Esta configuración se la realiza en todos los dispositivos router de la red de acuerdo al Direccionamiento IPv6 y el esquema de simulación (Figura 21).Ver ANEXO 44 para revisar la configuración de todos los router.

6.4.2 Configuración de algoritmo de enrutamiento EIGRP con IPv6.

Una vez realizado todo el direccionamiento en los dispositivos router se procede a configurar el algoritmo de enrutamiento, para lo cual se escoge un número de sistema autónomo que sirve para gestionar tráfico con políticas de rutas propias, en este caso el AS que se escogió es diez y los comandos que se utilizó para la configuración son los siguientes.

Tabla 15. Comandos de Activación de EIGRP para IPv6 [47] [48]

Activación de EIGRP para IPv6	
Comando o acción	**Propósito**
Quito> enable	Modo privilegiado EXEC
Quito# configure terminal	Modo de configuración global
Quito#(config) ipv6 unicast-routing	Envío de datagramas de unidifusión IPv6.
Quito #(config) interface fa0/0	Interfaz en la cual se configura EIGRP
Quito #(config-if) ipv6 enable	Procesamiento de IPv6 en una interface.
Quito #(config-if) ipv6 eigrp 10	Permite EIGRP para IPv6 en una interface
Quito #(config-if) ipv6 router eigrp 10	Entra en el modo de configuración del router y crea un proceso de enrutamiento IPv6 EIGRP
Quito #(config-router)router-id 2.2.2.2	Identificador de Router fijo.
Quito#(config-router)no shutdown	Activación de la interface

Esta configuración se realizó en todos los router, menos en aquellos routers que están funcionando como PCs (ver Figura 21). Una vez que se activa EIGRP para IPv6 y ya teniendo configurado el enrutamiento IPv6, se puede descubrir las rutas dinámicamente, de esto estaremos hablando más adelante en la parte de las pruebas de funcionamiento. Ver ANEXO 45 para revisar la configuración en todos los routers.

6.4.3 Creación de VLANs y encapsulamiento dot1Q

Para la creación de las VLANs debemos identificar cuáles son los routers en los cuales se debe crear las VLANs, en este caso se configura a todos los routers que están conectados a los Switch a excepción de los routers PCs y los routers que se conectan al ISP (ver Figura 21). Como estamos tomando como ejemplo el R2 de la red de Quito, la interface que se configura es la F0/0. Las VLANs estarán configuradas con números como 15, 16, 17 hasta 75, 76, 77 solo cogiendo como número terminal el 5, 6, 7.

En esta parte las VLANs que terminan en el número cinco pertenecen al servicio de Datos, los que terminan en seis pertenecen al servicio de VoIP y los que terminan en siete pertenecen al servicio de Video conferencia, esto se realiza con el fin de

identificar los servicios en diferentes redes. Los comandos que se utiliza se deben aplicar en todos los router que están identificados para crear VLANs.

El encapsulamiento dot1Q es muy importante ya que mediante una sola interface se puede configurar diferentes sub-interfaces (VLANs) que nos pueden servir para transmitir servicios diferentes por una sola interface. En el encapsulamiento lo que se realiza es la creación de tres sub-interfaces para transmitir tres servicios específicos como son Datos, VoIP y Video.

En la siguiente tabla se muestra la configuración para las interfaces de las VLANs de Datos y VoIP. La configuración de la VLAN de Video es similar a las de los otros servicios.

A continuación describimos los comandos utilizados para la creación de VLANs.

Tabla 16. Comandos para VLANs

Comandos para creación de VLANs en las interfaces	
Comando o acción	**Propósito**
Quito> enable	Modo privilegiado EXEC
Quito# configure terminal	Modo de configuración global
Quito #(config) interface fa0/0	Escoger la interface
Creación de VLAN de datos	
Quito #(config-if) interface fa0/0.15	Crear sub-interface para Datos
Quito #(config-subif) description datos_quito	Descripción para identificar la sub-interface
Quito #(config-subif) encapsulation dot1Q	Modo de encapsulamiento
Quito #(config-subif) ipv6 address 2800:130:1:0115::1/64	Dirección IPv6 global única
Quito #(config-subif) ipv6 enable	Permite el procesamiento de IPv6 en una interface.
Quito #(config-subif) ipv6 eigrp 10	Permite EIGRP para IPv6 en una interface
Quito #(config-subif) ipv6 router eigrp 10	Entra en el modo de configuración del router y crea un proceso de enrutamiento IPv6 EIGRP
Quito #(config-router)router-id 2.2.2.2	Identificador de Router fijo.
Quito#(config-router)no shutdown	Activación de la interface

Creación de VLAN de VOIP	
Quito #(config-if) interface fa0/0.16	Crear sub-interface para VoIP
Quito #(config-subif) description voip_quito	Descripción para identificar la sub-interface
Quito #(config-subif) encapsulation dot1Q	Modo de encapsulamiento
Quito #(config-subif) ipv6 address 2800:130:1:0116::1/64	Dirección IPv6 global única
Quito #(config-subif) ipv6 enable	Procesamiento de IPv6 en una interface.
Quito ##(config-subif) ipv6 eigrp 10	EIGRP para IPv6 en una interface
Quito #(config-subif) ipv6 router eigrp 10	Entra en el modo de configuración del router y crea un proceso de enrutamiento IPv6 EIGRP
Quito #(config-router)router-id 2.2.2.2	Identificador de Router fijo.
Quito#(config-router)no shutdown	Activación de la interface

Ver ANEXO 46 para revisar la configuración en todos los routers

6.4.4 Encapsulamiento dot1Q en las interfaces de los Switch

En el simulador GNS3 se puede realizar una configuración gráfica a nivel de los Switch, ya que permite escoger el puerto, VLAN y el tipo de acceso o encapsulamiento. En esta parte se configuró la VLAN 99 como dot1Q para todos los Switch, y las otras interface que dan la cara a las PCs se las configuró con la VLAN de acuerdo al servicio que pertenecen y de tipo Access. Por ejemplo en el R2 de la red Quito tenemos configurado en la interface fa0/0 tres VLAN (15-16-17), entonces en el Switch también debemos configurar las tres interfaces que dan la cara a las PCs con esos mismos números de VLANs y la dirección de las máquinas debe ir de acuerdo a la VLAN a la que pertenecen.

En la Figura 22 se ha configurado el Switch en el puerto 1 con un encapsulamiento dot1Q, y las VLAN 15, 16, 17 son interfaces a las cuales se conectan las máquinas. El número de puerto es el número de la interface.

6.4.5 Lista de control de Acceso ACLs

Las ACLs sirven para controlar tráfico, en nuestro caso debemos controlar que solo las máquinas que tengan servicios iguales se conecten y que el resto se bloquee para ese host. Para este tipo de control nosotros utilizamos ACLs en los routers que están conectados a los Switch a excepción de los routers PCs y los routers que se conectan al

ISP. En los Routers que se tiene que configurar las listas de control de acceso, se lo realiza en la interface serial, debido a que estamos trabajando con una ACL nombrada que es extendida. Eso quiere decir que se evalúa el origen y destino. Este tipo de ACL nombradas extendidas se coloca lo más cerca del origen para optimizar las rutas.

A continuación se explicará los comandos que se utiliza y se tomará como ejemplo el R2 de la red de Quito.

Tabla 17 Configuración de ACLs [51]

Comandos para Configuración de ACLs con IPv6	
Comando o acción	**Propósito**
Quito> enable	Modo privilegiado EXEC
Quito# configure terminal	Modo de configuración global
Quito# (config)# ipv6 access-list quito	Nombre a la ACL
Quito# (config-ipv6-acl)#permit host 2800:130:1:0115::2 host 2800:130:1:0125:2	Conexión de servicio de datos_quito con datos_guayaquil
Quito# (config-ipv6-acl)#deny any any	Negar todo el resto del trafico
Quito# (config)#interface se0/0	Abrir la interface se0/0
Quito# (config-if)#ipv6 traffic filter quito out	Controla tráfico de salida

Las listas de control de acceso se las pone para todos los host que están conectados para controlar el tráfico de salida. En este caso solo se puso una lista de control de acceso pero en realidad son muchísimos más que se irán mostrando en los anexos. Ver ANEXO 47 para revisar la configuración en todos los routers

6.4.6 QoS

Para la calidad de servicio tenemos que aplicar anchos de banda con prioridad en este caso la prioridad será el servicio de VoIP. Cuando se aplica QoS en la red se está aprovechando la tecnología MPLS. Esta parte está configurada pero debido a que estamos trabajando con un simulador, el cual utiliza imágenes reales de los sistemas operativos para emularlos y en vista de que la memoria utilizada para este proyecto es de 4GB no es posible realizar pruebas reales de la calidad de servicio que presta, sin embargo quedan los archivos de configuración que se ha realizado para mejorar la calidad de servicio de los servicios prestados.

Para realizar la configuración de calidad de servicio se debe tomar algunos puntos en cuenta, como son: ¿Cuál será el servicio que tenga prioridad sobre el resto?, ¿Cuál será la precedencia de cada servicio, los anchos de banda que se asignaran a cada servicio, y las políticas que se asignaran para la salida y lo que sé queda adentro?. En los archivos de configuración de los routers se podrá apreciar de mejor manera la implementación en el simulador.

Tabla 18 Archivo de configuración de Calidad de Servicio [50]

```
QUITO
conf ter
class-map match-any APLICACIONES
match access-group name quito
match precedence 3
EXIT
class-map match-any VIDEO
match access-group name quito
match precedence 4
EXIT
class-map match-any VOICE
match access-group name quito
match precedence 5
exit
conf ter
policy-map QoS_nested
class VOICE
priority 384
class VIDEO
bandwidth 1500
class APLICACIONES
bandwidth 512
exit
exit
policy-map QoS_parent
class class-default
shape average 2400000
service-policy QoS_nested
interface se0/0
description enlace_wan
service-policy output QoS_parent
bandwidth 3300
end
```

Hasta aquí llega la simulación del algoritmo de enrutamiento dinámico para la red WAN MPLS. Ahora nos concentraremos en las pruebas correspondientes para ver si en verdad está funcionando el algoritmo de enrutamiento y el protocolo enrutado IPv6. Ver ANEXO 48 para revisar la configuración en todos los routers.

6.5 Pruebas realizadas sobre la Simulación con IPv6

Estas pruebas están realizadas sobre la simulación que se ha creado a partir del algoritmo de enrutamiento EIGRP y el algoritmo enrutado IPv6. Algunas pruebas son las siguientes:

- **Configuración de las interfaces.-** el objetivo de esta prueba es verificar los diferentes tipos de direcciones IPv6 que se configuraron en las diferentes interfaces y las direcciones que se generan dinámicamente.
- **Interfaces configuradas con EIGRP.-** El objetivo principal es describir las interfaces que están configuradas con EIGRP. En este caso se tomará en cuenta los siguientes puntos:

    - Routers vecinos
    - Intervalos de tiempo
    - Paquetes multidifusión

- **Vecinos de los routers configurados con EIGRP.-** El objetivo es revisar que los routers vecinos están siendo identificados por el router R2 de Quito y los tiempos que tardan los paquetes en ir a los routers vecinos y venir.
- **Protocolo en uso para el enrutamiento dinámico.-** El objetivo es identificar las características principales de EIGRP.
- **Métricas configuradas en IPv6.-** El objetivo principal es identificar el uso de las ACLs.
- **Políticas de mapeo de la calidad de servicio.-** El objetivo es aplicar QoS en los servicios de los centros asociados.
- **Reconocimiento de rutas con EIGRP.-** El objetivo principal es mostrar las rutas aprendidas por el Router R2 de Quito.
- **Prueba de conexión del servicio de datos de la red de Quito.-** El objetivo es comprobar que se está realizando la conexión del servicio de datos de la red de Quito.
- **Prueba de conexión del servicio de VoIP de la red de Quito-** El objetivo es comprobar que se está realizando la conexión del servicio de VoIP de la red de Quito.
- **Prueba de conexión del servicio de Video de la red de Quito-** El objetivo es comprobar que se está realizando la conexión del servicio de Video de la red de Quito.
- **Tabla de topología.-** El objetivo es identificar la ruta que recorre los paquetes cuando viajan de un origen a un destino para identificar las posibles rutas que puede tomar una dirección.
- **Tráfico de red.-** El objetivo es identificar los mensajes *Hello,* actualizaciones, consultas y paquetes recibidos y enviados.

El desarrollo completo de las pruebas de la simulación del algoritmo de enrutamiento EIGRP y algoritmo enrutado IPv4 está en el ANEXO 35

6.6 Comparaciones con el estado actual de la red WAN MPLS

Para poder realizar la comparación del estado actual con la simulación que tenemos, debemos tomar en cuenta, que los dispositivos que están actualmente funcionando en la

red WAN de la UTPL cumplen una función específica, mientras que en la simulación se utiliza un solo equipo anfitrión y esto puede afectar el rendimiento y la apreciación de los datos.

Para la comparación de resultados se toma como muestras 5 centros, de los 7 que cuentan con la tecnología MPLS. Para obtener valores aproximados a los reales se realizó una prueba del impacto que tiene la simulación sobre el tiempo en milisegundos. (Ver ANEXO 49, 50). Aclarado esto procedemos a realizar las comparaciones de la simulación con el estado actual.

6.6.1 Comparación del retardo del canal de Datos

Para realizar esta comparación se ejecutó las pruebas desde el router de Quito, tanto en la simulación como en el estado actual. Los datos obtenidos del canal de Datos se muestran en la tabla siguiente.

Tabla 19. Tabla de retardo del canal de datos

PRUEBA DE RETARDO CANAL DE DATOS			
CIUDAD	**IPV6 SIMULADO (ms) Avg**	**IPV4 SIMULADO (ms) Avg**	**IPV4 ACTUAL (ms) Avg**
GUAYAQUIL	22	18	11
CUENCA	22	18	0
STO. DOMINGO	92	25	8
MANTA	43	23	12
SAN RAFAEL	15	41	0

El promedio (avg) es el retardo que se genera cuando se transmite desde un router a otro, cuando este promedio es igual que el tiempo mínimo (Min) y el tiempo máximo (Max), quiere decir que no existe retardo en la comunicación, en la siguiente gráfica ilustramos los datos que se obtuvo de la comparación entre lo simulado y lo que esta implementado actualmente.

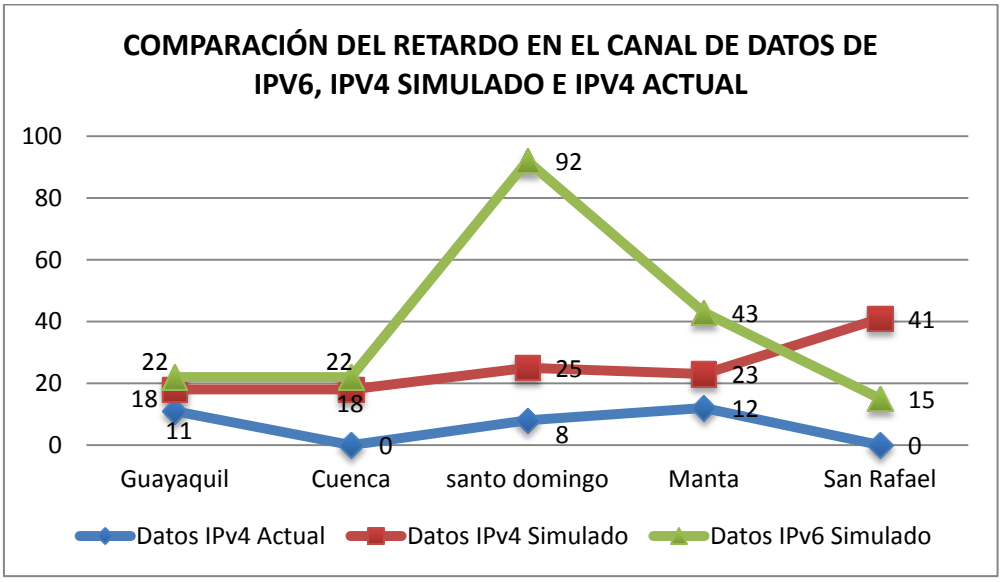


Figura 23. Comparación del retardo del canal de datos

En la gráfica se puede observar que la simulación IPv4 tiene un poco más de retardo en cuanto a lo que actualmente está implementado, pero este retardo no es muy significativo, mientras que la simulación IPv6, dobla el tiempo de retardo en comparación con lo que esta implementado actulamente.

6.6.2 Comparación del retardo del canal de VoIP

Las pruebas de retardo del canal de VoIP se realizan en cinco centros asociados las cuales nos reflejan los datos que se muestran en la tabla siguiente.

Tabla 20. Prueba de retardo canal de VoIP

PRUEBA DE RETARDO CANAL DE VoIP			
CIUDAD	IPV6 SIMULADO (ms) avg	IPV4 SIMULADO (ms) Avg	IPV4 ACTUAL (ms) Avg
GUAYAQUIL	10	11	12
CUENCA	28	19	21
STO DOMINGO	34	7	5
MANTA	35	15	234* Se omite este valor por congestion de canal
SAN RAFAEL	16	3	* Se omite el valor por saturación del dispositivo

L

Los datos que se obtuvo de la implementación actual, no son datos que se mantienen en un rango, sino que se pueden alterar drásticamente. Esto es debido al uso del dispositivo. En el caso de Manta, existe un mayor retardo debido a que se está utilizando más ese canal de VoIP (esto no se refleja en la gráfica siguiente, porque no nos permite apreciar el resto de valores, sin embargo se encuentra ilustrado en la tabla anterior).

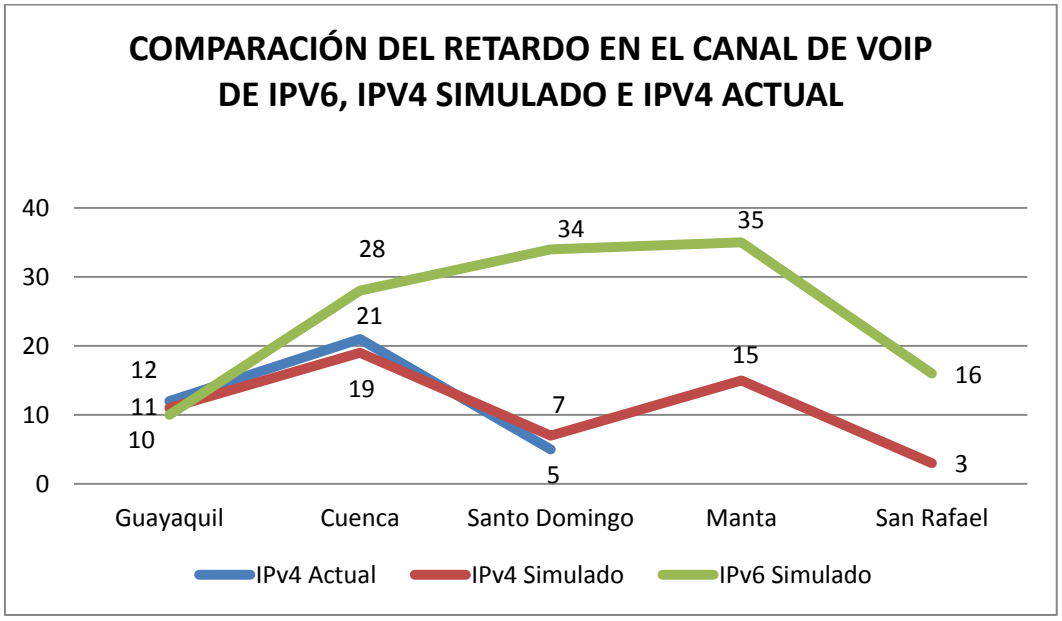


Figura 24. Comparación del retardo en el canal de VoIP

Sin embargo como se puede observar en la gráfica, los valores de la simulación dinámica IPv4 se mantiene en un rango constante, y similar a lo que está implementado, en cambio lo simulado dinámicamente en IPv6 tiene un rango mas elevado que lo implementado actualmente.

6.6.3 Comparación del retardo del canal de Video

En esta tabla tenemos los datos que se obtuvo en el canal de video, donde se puede observar las variaciones que se encuentran en la parte estática que actualmente está implementada.

Tabla 21. Prueba de retardo canal de video

PRUEBA DE RETARDO CANAL DE VIDEO			
CIUDAD	DATOS IPV6 SIMULADO (ms) Avg	DATOS IPV4 SIMULADO (ms) Avg	DATOS IPV4 ACTUAL (ms) Avg
GUAYAQUIL	16	33	13
CUENCA	37	21	13
SANTO DOMINGO	7	8	6
MANTA	26	14	213* Se omite por saturación del dispositivo
SAN RAFAEL	27	47	186* Se omite por saturación del dispositivo

En esta gráfica se puede apreciar que la simulación de algoritmo dinámico mantiene una secuencia en el retraso de la señal. Es mas alto que lo que esta implementado actualmente, la simulación de IPv4 no tiene un retardo de consideración con respecto a IPv4 actual.

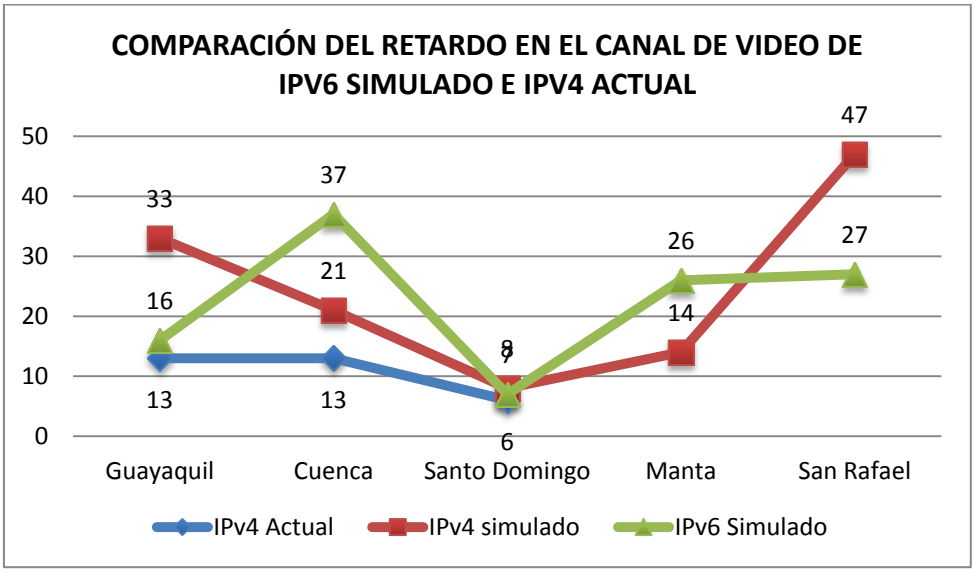


Figura 25. Retartdo de la señal en el canal de video

En la parte que actualmente esta implementado estáticamente en la red WAN de la UTPL se puede apreciar que aunque en algunos centros asociados el retraso de la señal es bajo en otros centros asociados sobrepasa el retardo que hay en la parte simulada. Esto se debe a que se están utilizando en gran medida.

6.6.4 Comparación de número de saltos

El número de saltos que se puede observar en la parte de la simulación es igual para todos los centros asociados, lo que hace que se tenga un rango de retardo similar en cada uno de los canales de los centros asociados.

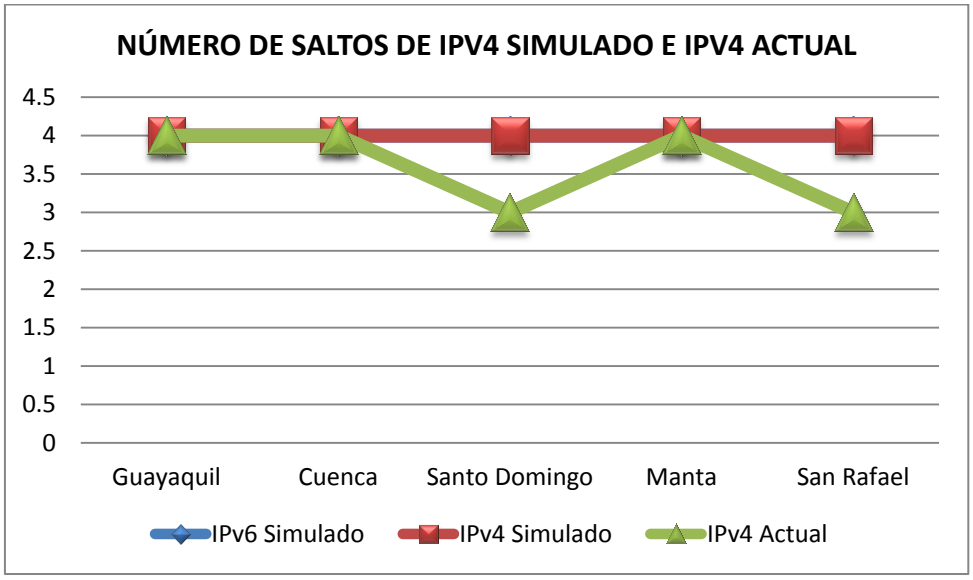


Figura 26 Número de saltos

En cambio el número de saltos de lo que esta implementado de forma estática varia, lo cual también hace que varíe el retardo en los diferentes servicios de datos, video conferencia y VoIP.

6.6.5 Comparación General

De acuerdo a los conceptos, pruebas y observaciones se puede definir las ventajas que tiene la configuración simulada de la red WAN de la UTPL con respecto a la configuración actual, y viceversa. Esta comparación se la efectúa en base a toda la investigación que se ha realizado hasta el momento.

Tabla 22. Comparacion General

CONSIDERACIONES	ACTUAL	SIMULADO
Rutas a difundir	Depende del administrador notificar a los demás la nueva ruta (Proceso manual)	Nueva ruta a difundir (Proceso automático.)
Soporte de VLSM	Soportado	Soportado
Escalabilidad	No factible para redes grandes y cambiantes	Se adapta rápidamente a los cambios realizados en la red.
Rapidez	Depende de las rutas estáticas.	Depende de la rapidez de convergencia del algoritmo dinámico y de la versión del protocolo enrutado IPv4 o IPv6. (un poco lento con relación al estático)
Direccionamiento	Estático, depende en todo momento del administrador (cuando se añade un dispositivo se debe configurar todos los dispositivos implicados)	Dinámico, se difunde en toda la red (solo se configura el dispositivo añadido)

Como se puede observar en el Tabla 22, la única desventaja que tiene la simulación con respecto a la configuración actual de la red WAN de la UTPL, es que su tiempo de respuesta es un poco lento, esto se puede justificar, porque cuando se está manejando una configuración Dinámica, esta deberá revisar sus tablas (tablas de vecinos, topología y encaminamiento) y escoger cual es la dirección que se necesita para realizar la conexión de la red. En cuanto a la administración de las redes, la simulación es mucho más rápida con relación a la configuración que se encuentra actualmente en la red WAN de la UTPL.

CAPÍTULO 7

ENTREGABLES Y PROPUESTA DE IMPLEMENTACIÓN

7. INTRODUCCIÓN

En el presente capítulo se procede a detallar los entregables y el proceso para la implementación , esto se evaluó en un laboratorio de pruebas. Se deja entregables los cuales serán valorados por los administradores de la red WAN de la UTPL.

7.1 Entregables

Los entegables se empaquetan en un DVD para que los administradoes de la red puedan revisarlos cuando sea necesario.

Dentro de los entregables tenemos:

- Archivos de configuración de los dispositivos.
  Aquí se puede encontrat todas los archivos de configuración que son necesarios para levantar el laboratorio de pruebas con la herramienta GNS3.
- Esquema de red IPv4 e IPv6.
  Todo el esquema con su direccionamiento para realizar revisiones y observaciones sobre la red que se trabajó.
- Direccionamiento de IPv6 Propuesto.
  El direccionamiento IPv6 con el que se trabajó durante la investigación.
- Manual de implementación IPv4 e IPv6.
  Aquí se explica paso a paso todas las configuraciones que se realiza para levantar la información de los dispositivos configuados.

7.2 Propuesta de implementación

Una vez que se ha validado la factibilidad de simulación exitosa, el proceso para implementarlo debe ser el siguiente:

1. Levantamiento de Información (CAPITULO 1, CAPITULO 2)
2. Requerimientos del a red WAN de la UTPL, Criterios de selección y análisis del algoritmo adecuado (Capitulo 3, Capitulo 4)
3. Tabla de direccionamiento propuesto para el algoritmo enruta IPv6 (CAPITULO 5, TABLA 9)
4. Tabla de direcciones propuesta para la configuración de las VLANs para los servicios de Datos, VoIP y Video Conferencia (ANEXO 43)
5. Esquema propuesto para la implementación con enrutamiento dinámico EIGRP y algoritmo enrutado IPv6. (CAPITULO 5, FIGURA 21)
6. Configuración del algoritmo de enrutamiento con algoritmo enrutado IPv6
    a. Configuración de direccionamiento IPv6 (CAPITULO 6, TABLA 14, ANEXO 44)
    b. Configuración de algoritmo de enrutamiento EIGRP con IPv6 (CAPITULO 6, TABLA 15, ANEXO 45)

   c. Creación de VLANs para los servicios de Datos, VoIP y Video (CAPITULO 6, TABLA 16, ANEXO 46)
   d. Configuración de ACLs (CAPITULO 6, TABLA 17, ANEXO 47)
   e. Configuración de calidad de servicio (CAPITULO 6, TABLA 18, ANEXO 48)
7. Pruebas (CAPITULO 6, ANEXO 35)

CONCLUSIÓNES

Conclusiones generales

- En el entorno simulado con IPv4 se puede apreciar que los canales de datos, voz y video son análogos con un error de (2 - 20 ms) lo que nos permite validar el modelo de simulación.
- En el entorno simulado con IPv6, es análogo con la implementación actual de la red WAN MPLS de la UTPL pero con un error de 2 – 40 ms.
- En base a la verificación del modelo simulado se pude concluir que el modelo IPv6 trabajará eficientemente en el entorno real. Aunque los tiempos de transferencia sean un poco elevados en cuanto al enrutamiento estático que esta implementado actualmente.
- Al implementar el algoritmo de enrutamiento dinámico la convergencia o anuncio de nuevas rutas en la red WAN MPLS de la UTPL es mucho más rápida que un modelo estático.
- El simulador trabaja con IOS reales por lo que se puede tener una experiencia más real por los inconvenientes que se tiene tanto en hardware como en software.
- El algoritmo de enrutamiento EIGRP es compatible con la red actual debido a que los IOS de los equipos de redes, están actualizados para que puedan ser compatibles.
- Al momento de revisar las rutas se pudo evidenciar que el algoritmo EIGRP con el comando ***traceroute IPV6 direccion_global*** muestra todas las posibles rutas que se pueden recorrer desde el origen, cosa que no evidenciaba con un enrutamiento estàtico. Esto se puede evidenciar en el ANEXO 35.
- Al momento de tener los servicios ya configurados se estableció que se necesitaba implementar ACLs debido a que todo se conectaba con todo y no existía un control en los servicios prestados.
- Se pudo evidenciar en las pruebas que el algoritmo enrutado IPV4 e IPv6 son aptos para configurarlos con el algoritmo de enrutamiento EIGRP y que pueden convivir ambos protocolos porque al momento de realizar la simulación se realizó ambas configuraciones en el mismo esquema de red.
- La configuración del algoritmo de enrutamiento con IPv6 es más tediosa que con IPv4 porque se necesita configurar más direcciones de red y permisos para que se acepte el protocolo de enrutamiento en los dispositivos.

RECOMENDACIONES

Recomendaciones Generales

- Se debe implementar el proyecto propuesto por parte del administrador de la red WAN debido a que mejorará el servicio, rendimiento, disponibilidad y administración de la red WAN de la UTPL.
- Antes de probar una nueva configuración de la red WAN se debe tener un laboratorio de experimentación con GNS-3 que tenga replicada la configuración de la red WAN de la UTPL lo cual ayudará a los administradores a su gestión y cambios.
- Se debe implementar IPv6 ya que estamos en una etapa de transición y los proveedores ya están trabajando sobre este protocolo, de tal forma que la UTPL ya tiene acceso a ipv6 de forma nativa.
- Es recomendable tener el enrutamiento de IPv6 en base a lo que ya se tiene implementado con IPv4 para que el administrador pueda reconocer inmediatamente las redes que están configuradas sobre la red WAN de la UTPL y realizar una correcta administración**.**
- Para evitar inconvenientes al momento de realizar cambios sobre la red WAN de la UTPL, se debe respaldar los datos de los dispositivos en caso de que se requiera volver a la configuración anterior o en caso de que alguna configuración no se realice correctamente.
- Para implementar las configuraciones del algoritmo de enrutamiento EIGRP y algoritmos enrutados IPv4 o IPv6 se debe actualizar los IOS de los equipos para que soporten las configuraciones.
- Al realizar las comparaciones de la simulación con la situación actual de la red WAN de la UTPL, se debe tener en cuenta que los dispositivos conectados a la red WAN de la UTPL están activos en sus diferentes centros asociados, para lograr datos confiables.
- La máquina en la cual se va a simular la red debe tener como mínimo un procesador Core i5 o i7 para no tener problemas en la simulación.
- En el equipo anfitrión de la simulación se recomienda tener de 6 a 8 Gb de memoria RAM, debido a que los dispositivos utilizan IOS reales y la memoria que utiliza cada dispositivo simulado es de 128 a 180 Mb y se debe tomar en cuenta que son 35 dispositivos simulados.

BIBLIOGRAFÍA

BIBLIOGRAFIA:

[1] Miguel Candía, (2007). Planta externa: Última milla. Chile: La Revista de Tecnologías de Información para la Gerencia, [On-line] Disponible en: http://www.emb.cl/gerencia/articulo.mv?sec=3&num=366&cmtok=1&rxx=656#coment

Citado: Diciembre 2009

[2] Compañía Global Crossing, (2010). One Planet. One Network. Infinite Possibilities, [On-line] Disponible en: http://www.globalcrossing.com/language/espanol.aspx

Citado: Enero 2010

[3] Compañía Telconet, (2010). Transmisión de datos, [On-line] Disponible en: http://www.telconet.net/?lang=es&section=solutions&content=03

Citado: Enero 2010

[4] Ibiblio the public's library and digital archive (2010). Routing avanzado con el núcleo Linux. http://www.ibiblio.org/pub/linux/docs/LuCaS/Presentaciones/200103hispalinux/eric/html/tuneles.html

Citado: Febrero 2010

[5] Emagister (2008). Diferencia en modos trunking allowed y native, [On-line] Disponible en: http://grupos.emagister.com/debate/diferencia_en_modos_trunking_allowed_y_native/6980-523501

Citado: Febrero 2010

[6] SAF (2009). Customized Microwave Solutions, [On-line] Disponible en: https://www.saftehnika.com/

Citado: Febrero 2010

[7] Informativo UTPL (2008.) La fibra Óptica, una oportunidad de desarrollo para Loja, [On-line] Disponible en: http://www.scribd.com/doc/7434324/Informativo-via-Marzo08

Citado: Febrero 2010

[8] Wikipedia (2010). E1, [On-line] Disponible en: http://es.wikipedia.org/wiki/E1

Citado: Febrero 2010

[9] Comisión Nacional de Comunicaciones CNC (2010). Homologaciones, [On-line] Disponible en: http://www.cnc.gov.ar/homologaciones/equipos.asp?offset=8500

Citado: Marzo 2010

[10] DEMUSAN, Que es una DMZ, [On-line] Disponible en: http://www.solusan.com/que-es-una-dmz.html

Citado: Marzo 2010

[11] LACNIC, Registro de direcciones de internet para América Latina y el Caribe, [On-line] Disponible en: http://lacnic.net/cgi-bin/lacnic/whois?lg=SP

Citado: Marzo 2010

[12] RFC 3513, Internet Protocol Version 6 (IPv6) Addressing Architecture, [On-line] Disponible en: http://www.ietf.org/rfc/rfc3513.txt

Citado: Marzo 2010

[13] EVELIUX, IPv6: El protocolo del Internet de la nueva generación - IPv6 parte 2, [On-line] Disponible en: http://www.eveliux.com/mx/ipv6-el-protocolo-del-internet-de-la-nueva-generacion/page-2.php

Citado: Marzo 2010

[14] IPv6.br, Guía didáctica de direccionamiento IPv6, [On-line] Disponible en: http://www.ipv6.br/pub/IPV6/MenuIPv6CursoPresencial/enderec-v6.pdf

Citado: Abril 2010

[15] MSDN, IPv6, [On-line] Disponible en: http://msdn.microsoft.com/es-es/library/95c9d312(VS.80).aspx

Citado: Abril 2010

[16] Verónica Xhardez, Internet: Redes Informáticas y jerarquías, [On-line] Disponible en: http://docs.hipatia.net/verox/internet_redes_informaticas_y_jerarquias.pdf

Citado: Abril 2010

[17] David Fernández, Introducción a IPv6, [On-line] Disponible en: http://www.6sos.org/pdf/introduccion_a_ipv6_v1.pdf

Citado: Abril 2010

[18] Eloy Aguiano Rey, IPv6, [On-line] Disponible en: http://memnon.ii.uam.es/~eloy/media/REDES/Tema11-ipv6.pdf

Citado: Mayo 2010

[19] IPv6, [On-line] Disponible en: http://www.arcesio.net/ipv6/IPv6.ppt

Citado: Mayo 2010

[20] Alberto G. Martínez, Depto. de Telemática, Universidad Carlos III, Introducción a IPv6, [On-line] Disponible en: http://www.it.uc3m.es/rromeral/arc/arc-files/05-ipv6.pdf

Citado: Mayo 2010

[21] RFCs de IPv6, IPv6 Fórum, [On-line] Disponible en: http://www.consulintel.es/html/ForoIPv6/RFCs.htm.

Citado: Mayo 2010

[22] RFC 2375, IPv6 Multicast Address Assignments, [On-line] Disponible en: http://tools.ietf.org/html/rfc2375

Citado: Mayo 2010

[23] Simón Mudd, Ángel Moncada "c4n", Joaquín Bójar "ShuoData". (2002) Organización de las Redes Wireless - v1.2, [On-line] Disponible en: http://www.wl0.org/~sjmudd/wireless/network-structure/html/index.html

Citado: Mayo 2010

[24] José María Barceló. Protocolos de encaminamiento, [On-line] Disponible en: http://beta.redes-linux.com/manuales/routing/PIAM-Routing-OSPF.pdf

Citado: Mayo 2010

[25]ICE (2008) Protocolos de Enrutamiento y Tráfico Soportado por la RAI, [On-line] Disponible en: https://www.grupoice.com/PEL/docsAdq/CD20081742CAR-078.doc

Citado: Mayo 2010

[26] NEO-University of Málaga (2008).Herramientas WEB para la enseñanza de protocolos de Comunicación. Protocolos RIP/OSPF/BGP, [On-line] Disponible en: http://neo.lcc.uma.es/evirtual/cdd/tutorial/red/protocols.html

Citado: Mayo 2010

[27] Info bits **(2008).** Autonomous Systems and BGPv4, [On-line] Disponible en: www.scribd.com/doc/2926414/piamroutingbgpv4

Citado: Junio 2010

[28] UNITEC. Ing. Jorge Álvarez. (2005). Capa de red, protocolos, [On-line] Disponible en: http://members.fortunecity.es/unitec/resumen10.htm

Citado: Junio 2010

[29] Mitecnologico, [On-line] Disponible en: http://www.mitecnologico.com/Main/ProtocolosEnrutadosYDeEnrutamiento

Citado: Junio 2010

[30] ESPOL. Diseño de una red troncal en anillo de fibra óptica para el transporte de tráfico IP sobre MPLS entre las ciudades de Guayaquil, Quito y Cuenca. , [On-line] Disponible en: http://www.dspace.espol.edu.ec/bitstream/123456789/2547/1/5023.pdf

Citado: Junio 2010

[31] Néstor García Fernández. Introducción a IPX/SPX, [On-line] Disponible en: http://petra.euitio.uniovi.es/asignaturas/adm.ent.mul/curso0304/AEMRedes2.pdf

Citado: Junio 2010

[32] gobiernodecanarias.org, [On-line] Disponible en: http://www.gobiernodecanarias.org/educacion/conocernos_mejor/paginas/protocol1.htm

Citado: Junio 2010

[33] Ing. Jorge Álvarez, Resumen módulo 10, CCNA 1 v 3.1. , [On-line] Disponible en: http://members.fortunecity.es/unitec/resumen10.htm

Citado: Junio 2010

[34]6SOS, El protocolo IPv6, [On-line] Disponible en: http://www.6sos.org/documentos/6SOS_El_Protocolo_IPv6_v4_0.pdf

Citado: Julio 2010

[35] Configuración EIGRP, [On-line] Disponible en: http://aprenderedes.com/2006/10/configuracion-de-eigrp/

Citado: Julio 2010

[36] Francisco Hernandis Gil, introducción al OSPF, [On-line] Disponible en: www.uv.es/~montanan/redes/trabajos/OSPF.doc

Citado: Julio 2010

[37]Ing. Felipe Jara Saba, Estudio e Implementación de una red IPv6 en la UTFSM, [On-line] Disponible en: http://portalipv6.lacnic.net/files/documentos/ImplementacionIPv6_UTFSM_presentacion.pdf

Citado: Julio 2010

[38] Insude, Protocolos de red, [On-line] Disponible en: http://www.ignside.net/man/redes/protocolos.php

Citado: Julio 2010

[39] Microsoft TechNet, IPv6, [On-line] Disponible en: http://technet.microsoft.com/es-es/library/cc780593(WS.10).aspx

Citado: Agosto 2010

[40] I Taller RUDAC en Tecnología de Redes Internet, José A. Domínguez [On-line] Disponible en: www.redhucyt.oas.org/webesp/PRESENTATIONS/RUDAC99/Routing.ppt

Citado: Agosto 2010

[41] CCNA2, Routing protocols and concepts 4.0

Citado: Agosto 2010

[42]LAC-TF IPv6 Subnetting, [On-line] Disponible en: http://mail.lacnic.net/pipermail/lactf/2006-January/001204.html

Citado: Agosto 2010

[43] RFC3177 - IAB/IESG Recommendations on IPv6 Address Allocations, [On-line] Disponible en: http://www.faqs.org/rfcs/rfc3177.html

Citado: Agosto 2010

[44] RFC3627 - Use of /127 Prefix Length Between Routers Considered, [On-line] Disponible en: http://www.faqs.org/rfcs/rfc3627.html

Citado: Agosto 2010

[45] The ISP Column, Just how big is IPv6?
- or Where did all those addresses go?, Geoff Huston, [On-line] Disponible en:
http://www.potaroo.net/ispcol/2005-07/ipv6size.html

Citado: Agosto 2010

[46] Portal GuilleSQL, Cap. 2. Protocolos de Enrutamiento, [On-line] Disponible en:
http://www.guillesql.es/Articulos/Manual_Cisco_CCNA_Protocolos_Enrutamiento.aspx

Citado: Septiembre 2010

[47] CCIE, CCIE, the beginning!, IPv6 EIGRP [On-line] Disponible en:
http://cciethebeginning.wordpress.com/2008/06/13/ipv6-eigrp/

Citado: octubre 2010

[48] CISCO, Implementing EIGRP for IPv6, [On-line] Disponible en:
http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-eigrp.html#wp1056488

Citado: Octubre 2010

[49] General search, c2691-advipservicesk9-mz.124-15.T6.bin, [On-line] Disponible en:
http://www.general-search.net/fileinfo/gs34b2f07h1i0

Citado: Octubre 2010

[50] CISCO, Implementing QoS for IPv6, [On-line] Disponible en:

http://www.cisco.com/en/US/docs/ios/ipv6/configuration/guide/ip6-qos.html#wp1054057
Citado: Octubre 2010

[51] CISCO, Configuring IPv6 ACLs, [On-line] Disponible en:
http://www.ciscosystems.info/en/US/docs/switches/lan/catalyst3750e_3560e/software/release/12.2_46_se/configuration/guide/swv6acl.pdf

Citado: Octubre 2010

[52] LACNIC, Servicios de Registro, [On-line] Disponible en: http://lacnic.net/cgi-bin/lacnic/whois?lg=SP&stkey=3589942-2667963734

Citado: Octubre 2010

ANEXOS

ANEXO 1 ANCHO DE BANDA DE LA TECNOLOGÍA WAN MPLS EN LOS DIFERENTES CENTROS ASOCIADOS

WAN MPLS			
UBICACIÓN	**DESCRIPCIÓN**	BANDWIDTH	PROVEEDOR
QUITO	Datos	512 Kb 1:1	**Global Crossing**
	Video	1.5 Mb 1:1	
	VoIP	384 Kb 1:1	
GUAYAQUIL	Datos	256 Kb 1:1	**Global Crossing**
	Video	640 Kb 1:1	
	VoIP	128 Kb 1:1	
CUENCA	Datos	256 Kb 1:1	**Global Crossing**
	Video	640KB 1:1	
	VoIP	128 Kb 1:1	
MANTA	Datos	256 Kb 1:1	**Global Crossing**
	Video	320 Kb 1:1	
	VoIP	128 Kb 1:1	
SANTO DOMINGO	Datos	256 Kb 1:1	**Global Crossing**
	Video	320 Kb 1:1	
	VoIP	128 Kb 1:1	
VILLA FLORA	Datos	256 Kb 1:1	**Global Crossing**
	Video	320 Kb 1:1	
	VoIP	128 Kb 1:1	
SAN RAFAEL	Datos	256 Kb 1:1	**Global Crossing**
	Video	320 Kb 1:1	
	VoIP	128 Kb 1:1	

ANEXO 2 PRUEBAS DE CALIDAD DE SERVICIO EN LOS DIFERENTES CENTROS ASOCIADOS ANTES DE LA SIMULACIÓN

Estas pruebas están realizadas sobre la configuración actual de la red WAN de la UTPL, antes de realizar la simulación de algoritmos de enrutamiento dinamico sobre la red WAN de la UTPL.

En los enlaces de los centros asociados se realizó algunas pruebas de calidad de servicio en los servicios de video conferencia con todos los centros asociados para comprobar que tipos de inconvenientes se producen al momento de realizar una conexión simultánea.

Se probó con tres medidas de anchos de banda al momento de realizar conexiones simultaneas, en el siguiente cuadro se puede visualizar los resultados que se obtuvo.

	CENTROS ASOCIADOS								RESULTADOS		
	QUITO	GUAYAQUIL	CUENCA	LOJA	MANTA	SANTO DOMINGO	SN RAFAEL	VILLAFLORA	RETRASO DE SEÑAL	PIXELACIÓN	EXELENTE
ANCHO DE BANDA	256 Kbps								✓		
	384 Kbps									✓	
	512 Kbps										✓

- En la primera prueba realizada con 256 Kbps se revelo que la señal llegaba entrecortada, por lo que no existía una señal óptima.
- En la segunda prueba realizada con 256 Kbps se revelo que la señal perdía algunos bytes en la transferencia lo cual hacia que la imagen se distorsione un poco al llegar al receptor, pero el sonido llegaba en plenitud al receptor.
- En la tercera prueba se constató que se podía realizar video conferencia sin problemas.

ANEXO 3 ARCHIVO DE CONFIGURACIÓN QUITO (ACTUAL)

Las contraseñas han sido borradas por cuestiones de seguridad.
Using 4716 out of 196600 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-CR-QUITO
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
class-map match-any APLICACIONES
match access-group 102
class-map match-any VIDEO
match access-group 101
class-map match-any VOICE
match access-group 100
policy-map QoS_nested
class VOICE

priority 384

set ip precedence 5
class VIDEO
bandwidth 1500
set ip precedence 4
class APLICACIONES
bandwidth 512
set ip precedence 3
policy-map QoS_parent
class class-default
shape average 2400000
service-policy QoS_nested
interface FastEthernet0/0
description ENLACE WAN RED GC
no ip address
no ip redirects
no ip proxy-arp
ip route-cache flow
duplex auto
speed auto
arp timeout 300
interface FastEthernet0/0.354
description ENLACE WAN RED GC
bandwidth 3300
encapsulation dot1Q 354
ip address 10.111.134.38 255.255.255.248
no snmp trap link-status
arp timeout 300
service-policy output QoS_parent
interface FastEthernet0/1
no ip address
no ip route-cache cef
ip route-cache flow
duplex auto
speed auto
interface FastEthernet0/1.15
description VC
bandwidth 1500
encapsulation dot1Q 15
ip address 200.0.30.1 255.255.255.240
no snmp trap link-status
interface FastEthernet0/1.40
description DATOS
bandwidth 512
encapsulation dot1Q 40
ip address 172.16.40.10 255.255.255.0
no snmp trap link-status
interface FastEthernet0/1.46
description VOIP
bandwidth 384
encapsulation dot1Q 46
ip address 172.16.46.65 255.255.255.0
no snmp trap link-status
interface FastEthernet0/1.100
encapsulation dot1Q 1 native
ip address 172.16.100.10 255.255.255.0
no snmp trap link-status
ip classless
ip route 0.0.0.0 0.0.0.0 10.111.134.37
ip route 172.16.41.0 255.255.255.0 172.16.40.1 name LANQUITO
ip flow-export source FastEthernet0/1.40
ip flow-export version 5
ip flow-export destination 172.16.85.15 9996
ip http server
ip access-list extended DATOS
permit tcp 172.16.40.0 0.0.0.255 host 172.16.50.54 eq 3128
permit udp 172.16.40.0 0.0.0.255 host 172.16.50.55 eq domain
permit udp 172.16.40.0 0.0.0.255 host 172.16.50.58 eq domain
permit ip 172.16.40.0 0.0.0.255 host 172.16.50.43
permit ip 172.16.40.0 0.0.0.255 host 172.16.3.132
permit ip 172.16.40.0 0.0.0.255 host 172.16.50.64
permit ip 172.16.40.0 0.0.0.255 host 172.16.50.60
permit ip 172.16.40.0 0.0.0.255 host 172.16.31.17
permit ip 172.16.40.0 0.0.0.255 host 172.16.50.62
permit ip 172.16.40.0 0.0.0.255 host 172.16.31.50
permit ip 172.16.40.0 0.0.0.255 host 172.16.13.7

```
permit ip 172.16.40.0 0.0.0.255 host 172.16.50.46
permit ip 172.16.40.0 0.0.0.255 host 172.16.50.41
permit ip 172.16.40.0 0.0.0.255 host 172.16.50.40
permit ip 172.16.40.0 0.0.0.255 host 172.16.50.42
permit ip 172.16.40.0 0.0.0.255 host 172.16.50.81
permit ip 172.16.40.0 0.0.0.255 host 172.16.90.12
permit ip 172.16.40.0 0.0.0.255 host 172.16.50.73
ip access-list extended VC
deny   ip any 172.16.0.0 0.0.255.255
permit ip 200.0.30.0 0.0.0.15 any
ip access-list extended VOIP
permit ip 172.16.46.0 0.0.0.255 host 172.16.50.34
access-list 100 remark VOICE
access-list 100 permit ip 172.16.46.64 0.0.0.31 any
access-list 101 remark VIDEO
access-list 101 permit ip 200.0.30.0 0.0.0.15 any
access-list 102 remark APLICACIONES
access-list 102 permit ip 172.16.40.0 0.0.0.255 any
snmp-server community utpl RO
snmp-server host 172.16.50.57 utpl
snmp-server host 172.16.85.15 utpl
control-plane
banner motd ^C
privilege exec level 10 copy startup-config tftp
privilege exec level 10 copy startup-config
privilege exec level 10 copy
privilege exec level 10 traceroute
privilege exec level 10 ping
privilege exec level 10 show startup-config
privilege exec level 10 show
line con 0
exec-timeout 5 0
login local
line aux 0
line vty 0 4
session-timeout 1
exec-timeout 5 0
login local
line vty 5 15
session-timeout 1
exec-timeout 5 0
login local
end
```

ANEXO 4 TABLA DE ENRUTAMIENTO QUITO (ACTUAL)

```
R-QUITO#show ip route
Gateway of last resort is 10.111.134.37 to network 0.0.0.0
     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.46.0 is directly connected, FastEthernet0/1.46
C       172.16.40.0 is directly connected, FastEthernet0/1.40
S       172.16.41.0 [1/0] via 172.16.40.1
C       172.16.100.0 is directly connected, FastEthernet0/1.100
     10.0.0.0/29 is subnetted, 1 subnets
C       10.111.134.32 is directly connected, FastEthernet0/0.354
     200.0.30.0/28 is subnetted, 1 subnets
C       200.0.30.0 is directly connected, FastEthernet0/1.15
S*      0.0.0.0/0 [1/0] via 10.111.134.37
R-CR-QUITO#
```

ANEXO 5 ARCHIVO DE CONFIGURACIÓN GUAYAQUIL (ACTUAL)

R-CR-GUAYAQUIL#show startup-config
Using 4384 out of 196600 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-CR-GUAYAQUIL
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
class-map match-any APLICACIONES
match access-group 102
class-map match-any VIDEO
match access-group 101
class-map match-any VOICE
match access-group 100
policy-map QoS_nested
class VOICE
priority 128
set ip precedence 5
class VIDEO
bandwidth 640
set ip precedence 4
class APLICACIONES
bandwidth 256
set ip precedence 3
policy-map QoS_parent
class class-default
shape average 1024000
service-policy QoS_nested
interface FastEthernet0/0
description ENLACE WAN RED GC
no ip address
ip route-cache flow
duplex auto
speed auto
interface FastEthernet0/0.354
description ENLACE WAN RED GC
bandwidth 1000
encapsulation dot1Q 354
ip address 10.112.115.110 255.255.255.252
no snmp trap link-status
service-policy output QoS_parent
interface FastEthernet0/1
no ip address
ip route-cache flow
duplex auto
speed auto
interface FastEthernet0/1.15
description VC
bandwidth 640
encapsulation dot1Q 15
ip address 200.0.30.17 255.255.255.248
no snmp trap link-status
interface FastEthernet0/1.42
description DATOS
bandwidth 256
encapsulation dot1Q 42
ip address 172.16.42.10 255.255.255.0
no snmp trap link-status
interface FastEthernet0/1.48
description VOIP
bandwidth 128
encapsulation dot1Q 48
ip address 172.16.48.10 255.255.255.0
no snmp trap link-status
interface FastEthernet0/1.100
encapsulation dot1Q 1 native
ip address 172.16.100.10 255.255.255.0
no snmp trap link-status
ip classless
ip route 0.0.0.0 0.0.0.0 10.112.115.109
ip flow-export source FastEthernet0/1.42
ip flow-export version 5
ip flow-export destination 172.16.85.15 9996
ip http server
ip access-list extended DATOS
permit tcp 172.16.42.0 0.0.0.255 host 172.16.50.54 eq 3128
permit udp 172.16.42.0 0.0.0.255 host 172.16.50.55 eq domain
permit udp 172.16.42.0 0.0.0.255 host 172.16.50.58 eq domain
permit ip 172.16.42.0 0.0.0.255 host 172.16.50.43
permit ip 172.16.42.0 0.0.0.255 host 172.16.3.132
permit ip 172.16.42.0 0.0.0.255 host 172.16.50.64
permit ip 172.16.42.0 0.0.0.255 host 172.16.50.60
permit ip 172.16.42.0 0.0.0.255 host 172.16.31.17
permit ip 172.16.42.0 0.0.0.255 host 172.16.50.62
permit ip 172.16.42.0 0.0.0.255 host 172.16.31.50
permit ip 172.16.42.0 0.0.0.255 host 172.16.13.7
permit ip 172.16.42.0 0.0.0.255 host 172.16.50.46
permit ip 172.16.42.0 0.0.0.255 host 172.16.50.41
permit ip 172.16.42.0 0.0.0.255 host 172.16.50.40
permit ip 172.16.42.0 0.0.0.255 host 172.16.50.42
permit ip 172.16.42.0 0.0.0.255 host 172.16.50.81
permit ip 172.16.42.0 0.0.0.255 host 172.16.90.12

```
permit ip 172.16.42.0 0.0.0.255 host 172.16.50.73
ip access-list extended VC
permit ip 200.0.30.16 0.0.0.7 any
ip access-list extended VOIP
permit ip 172.16.48.0 0.0.0.255 host 172.16.50.34
access-list 100 remark VOICE
access-list 100 permit ip 172.16.48.0 0.0.0.255 any
access-list 101 remark VIDEO
access-list 101 permit ip 200.0.30.16 0.0.0.7 any
access-list 102 remark APLICACIONES
access-list 102 permit ip 172.16.42.0 0.0.0.255 any
snmp-server community utpl RO
snmp-server host 172.16.50.57 utpl
snmp-server host 172.16.85.15 utpl
control-plane
privilege exec level 10 traceroute
privilege exec level 10 ping
privilege exec level 10 show startup-config
privilege exec level 10 show
line con 0
exec-timeout 5 0
login local
line aux 0
line vty 0 4
session-timeout 1
exec-timeout 5 0
password 7 094F471A1A0A
login local
line vty 5 15
session-timeout 1
exec-timeout 5 0
login local
end
```

ANEXO 6 TABLA DE ENRUTAMIENTO GUAYAQUIL (ACTUAL)

```
R-CR-GUAYAQUIL#show ip route
Gateway of last resort is 10.112.115.109 to network 0.0.0.0
      172.16.0.0/24 is subnetted, 3 subnets
C       172.16.48.0 is directly connected, FastEthernet0/1.48
C       172.16.42.0 is directly connected, FastEthernet0/1.42
C       172.16.100.0 is directly connected, FastEthernet0/1.100
      10.0.0.0/30 is subnetted, 1 subnets
C       10.112.115.108 is directly connected, FastEthernet0/0.354
      200.0.30.0/29 is subnetted, 1 subnets
C       200.0.30.16 is directly connected, FastEthernet0/1.15
S*      0.0.0.0/0 [1/0] via 10.112.115.109
R-CR-GUAYAQUIL#
```

ANEXO 7 CONFIGURACIÓN ROUTER CUENCA (ACTUAL)

```
R-CR-CUENCA#show startup-config
Using 4541 out of 196600 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-CR-CUENCA
boot-start-marker
boot-end-marker
enable secret 5 $1$esDl$nez1.TX6tdM7.BJQJbc61/
no aaa new-model
resource policy
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
class-map match-any APLICACIONES
match access-group 102
class-map match-any VIDEO
match access-group 101
class-map match-any VOICE
match access-group 100
policy-map QoS_nested
class VOICE
priority 128
set ip precedence 5
class VIDEO
bandwidth 640
set ip precedence 4
class APLICACIONES
bandwidth 256
set ip precedence 3
policy-map QoS_parent
class class-default
shape average 1024000
service-policy QoS_nested
interface FastEthernet0/0
description ENLACE WAN RED GC
no ip address
no ip redirects
no ip proxy-arp
ip route-cache flow
duplex auto
speed auto
arp timeout 300
interface FastEthernet0/0.354
description ENLACE WAN RED GC
bandwidth 1400
encapsulation dot1Q 354
ip address 10.113.114.122 255.255.255.248
no snmp trap link-status
arp timeout 300
service-policy output QoS_parent
interface FastEthernet0/1
no ip address
ip route-cache flow
duplex auto
speed auto
interface FastEthernet0/1.15
description VC
bandwidth 640
encapsulation dot1Q 15
ip address 200.0.30.25 255.255.255.248
no snmp trap link-status
interface FastEthernet0/1.44
description DATOS
bandwidth 256
encapsulation dot1Q 44
ip address 172.16.44.10 255.255.255.0
no snmp trap link-status
interface FastEthernet0/1.47
description VOIP
bandwidth 128
encapsulation dot1Q 47
ip address 172.16.47.10 255.255.255.0
no snmp trap link-status
interface FastEthernet0/1.100
encapsulation dot1Q 1 native
ip address 172.16.100.10 255.255.255.0
no snmp trap link-status
ip classless
ip route 0.0.0.0 0.0.0.0 10.113.114.121
ip route 172.16.45.0 255.255.255.0 172.16.44.254
name InternetCCA
ip flow-export source FastEthernet0/1.44
ip flow-export version 5
ip flow-export destination 172.16.85.15 9996
ip http server
ip access-list extended DATOS
permit tcp 172.16.44.0 0.0.0.255 host 172.16.50.54
eq 3128
permit udp 172.16.44.0 0.0.0.255 host 172.16.50.55
eq domain
permit udp 172.16.44.0 0.0.0.255 host 172.16.50.58
eq domain
permit ip 172.16.44.0 0.0.0.255 host 172.16.50.43
permit ip 172.16.44.0 0.0.0.255 host 172.16.3.132
permit ip 172.16.44.0 0.0.0.255 host 172.16.50.64
permit ip 172.16.44.0 0.0.0.255 host 172.16.50.60
permit ip 172.16.44.0 0.0.0.255 host 172.16.31.17
permit ip 172.16.44.0 0.0.0.255 host 172.16.50.62
permit ip 172.16.44.0 0.0.0.255 host 172.16.31.50
permit ip 172.16.44.0 0.0.0.255 host 172.16.13.7
permit ip 172.16.44.0 0.0.0.255 host 172.16.50.46
permit ip 172.16.44.0 0.0.0.255 host 172.16.50.41
permit ip 172.16.44.0 0.0.0.255 host 172.16.50.40
```

```
permit ip 172.16.44.0 0.0.0.255 host 172.16.50.42
permit ip 172.16.44.0 0.0.0.255 host 172.16.50.81
permit ip 172.16.44.0 0.0.0.255 host 172.16.90.12
ip access-list extended VC
permit ip 200.0.30.24 0.0.0.7 any
ip access-list extended VOIP
permit ip 172.16.47.0 0.0.0.255 host 172.16.50.34
access-list 100 remark VOICE
access-list 100 permit ip 172.16.47.0 0.0.0.255 any
access-list 101 remark VIDEO
access-list 101 permit ip 200.0.30.24 0.0.0.7 any
access-list 102 remark APLICACIONES
access-list 102 permit ip 172.16.44.0 0.0.0.255 any
access-list 102 permit ip 172.16.45.0 0.0.0.255 any
snmp-server community utpl RO
snmp-server host 172.16.50.57 utpl
snmp-server host 172.16.85.15 utpl
control-plane
privilege exec level 10 traceroute
privilege exec level 10 ping
privilege exec level 10 show startup-config
privilege exec level 10 show
line con 0
exec-timeout 5 0
login local
line aux 0
line vty 0 4
session-timeout 1
exec-timeout 5 0
login local
line vty 5 15
session-timeout 1
exec-timeout 5 0
login local
End
```

ANEXO 8 TABLA DE ENRUTAMEINTO CUENCA (ACTUAL)

R-CR-CUENCA#show ip route

Gateway of last resort is 10.113.114.121 to network 0.0.0.0

```
     172.16.0.0/24 is subnetted, 4 subnets
C       172.16.44.0 is directly connected, FastEthernet0/1.44
S       172.16.45.0 [1/0] via 172.16.44.254
C       172.16.47.0 is directly connected, FastEthernet0/1.47
C       172.16.100.0 is directly connected, FastEthernet0/1.100
     10.0.0.0/29 is subnetted, 1 subnets
C       10.113.114.120 is directly connected, FastEthernet0/0.354
     200.0.30.0/29 is subnetted, 1 subnets
C       200.0.30.24 is directly connected, FastEthernet0/1.15
S*   0.0.0.0/0 [1/0] via 10.113.114.121
R-CR-CUENCA#
```

ANEXO 9 CONFIGURACIÓN ROUTER MANTA (ACTUAL)

```
R-UTPL-MANTA#show startup-config
Using 4450 out of 196600 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-UTPL-MANTA
boot-start-marker
boot-end-marker
no aaa new-model
resource policy
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
ip domain name utpl.edu.ec
class-map match-any APLICACIONES
match access-group 102
class-map match-any VIDEO
match access-group 101
class-map match-any VOICE
match access-group 100
policy-map QoS_nested
class VOICE
priority 128
set ip precedence 5
class VIDEO
bandwidth 320
set ip precedence 4
class APLICACIONES
bandwidth 256
set ip precedence 3
policy-map QoS_parent
class class-default
shape average 704000
service-policy QoS_nested
interface FastEthernet0/0
description ENLACE WAN RED GC
no ip address
no ip redirects
no ip proxy-arp
ip route-cache flow
duplex auto
speed auto
arp timeout 300
interface FastEthernet0/0.354
description ENLACE WAN RED GC
encapsulation dot1Q 354
ip address 10.114.113.146 255.255.255.248
no snmp trap link-status
arp timeout 300
service-policy output QoS_parent
interface FastEthernet0/1
no ip address
ip route-cache flow
duplex auto
speed auto
interface FastEthernet0/1.1
encapsulation dot1Q 1 native

ip address 172.16.100.10 255.255.255.0
no snmp trap link-status
interface FastEthernet0/1.12
interface FastEthernet0/1.15
description VC
encapsulation dot1Q 15
ip address 200.0.30.81 255.255.255.248
no snmp trap link-status
interface FastEthernet0/1.77
encapsulation dot1Q 77
ip address 172.16.77.10 255.255.255.0
no snmp trap link-status
interface FastEthernet0/1.78
description VOIP
encapsulation dot1Q 78
ip address 172.16.78.10 255.255.255.0
no snmp trap link-status
ip classless
ip route 0.0.0.0 0.0.0.0 10.114.113.145
ip flow-export source FastEthernet0/1.77
ip flow-export version 5
ip flow-export destination 172.16.85.15 9996
ip http server
ip access-list extended DATOS
permit tcp 172.16.77.0 0.0.0.255 host 172.16.50.54
eq 3128
permit udp 172.16.77.0 0.0.0.255 host 172.16.50.55
eq domain
permit udp 172.16.77.0 0.0.0.255 host 172.16.50.58
eq domain
permit ip 172.16.77.0 0.0.0.255 host 172.16.50.43
permit ip 172.16.77.0 0.0.0.255 host 172.16.3.132
permit ip 172.16.77.0 0.0.0.255 host 172.16.50.64
permit ip 172.16.77.0 0.0.0.255 host 172.16.50.60
permit ip 172.16.77.0 0.0.0.255 host 172.16.31.17
permit ip 172.16.77.0 0.0.0.255 host
172.16.50.62permit ip 172.16.77.0 0.0.0.255 host
172.16.31.50

permit ip 172.16.77.0 0.0.0.255 host 172.16.13.7
permit ip 172.16.77.0 0.0.0.255 host 172.16.50.46
permit ip 172.16.77.0 0.0.0.255 host 172.16.50.41
permit ip 172.16.77.0 0.0.0.255 host 172.16.50.40
permit ip 172.16.77.0 0.0.0.255 host 172.16.50.42
permit ip 172.16.77.0 0.0.0.255 host 172.16.50.81
permit ip 172.16.77.0 0.0.0.255 host 172.16.90.12
```

```
permit ip 172.16.77.0 0.0.0.255 host 172.16.50.73
ip access-list extended VC
permit ip 200.0.30.80 0.0.0.7 any
ip access-list extended VOIP
permit ip 172.16.78.0 0.0.0.255 host 172.16.50.34
access-list 100 remark VOICE
access-list 100 permit ip 172.16.78.0 0.0.0.255 any
access-list 101 remark VIDEO
access-list 101 permit ip 200.0.30.80 0.0.0.7 any
access-list 102 remark APLICACIONES
access-list 102 permit ip 172.16.77.0 0.0.0.255 any
snmp-server community utpl RO
snmp-server host 172.16.50.57 utpl
snmp-server host 172.16.85.15 utpl
control-plane
privilege exec level 10 traceroute
privilege exec level 10 ping
privilege exec level 10 show startup-config
privilege exec level 10 show
line con 0
exec-timeout 5 0
password 7 045802150C2E
login local
line aux 0
line vty 0 4
session-timeout 1
exec-timeout 5 0
password 7 121A0C041104
login local
line vty 5 15
session-timeout 1
exec-timeout 5 0
login local
End
```

ANEXO 10 TABLA DE ENRUTAMIENTO MANTA (ACTUAL)

```
R-UTPL-MANTA#show ip route

Gateway of last resort is 10.114.113.145 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.100.0 is directly connected, FastEthernet0/1.1
C       172.16.77.0 is directly connected, FastEthernet0/1.77
C       172.16.78.0 is directly connected, FastEthernet0/1.78
     10.0.0.0/29 is subnetted, 1 subnets
C       10.114.113.144 is directly connected, FastEthernet0/0.354
     200.0.30.0/29 is subnetted, 1 subnets
C       200.0.30.80 is directly connected, FastEthernet0/1.15
S*   0.0.0.0/0 [1/0] via 10.114.113.145
R-UTPL-MANTA#
```

ANEXO 11 CONFIGURACIÓN ROUTER SANTO DOMINGO (ACTUAL)

```
R-CR-SNT-DOMINGO#show startup-config
Using 4629 out of 196600 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-CR-SNT-DOMINGO
boot-start-marker
boot-end-marker
enable secret 5
$1$GFwu$DPgIiXN4JwSjEKuHXHAvq1
no aaa new-model
resource policy
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
class-map match-any APLICACIONES
match access-group 102
class-map match-any VIDEO
match access-group 101
class-map match-any VOICE
match access-group 100
policy-map QoS_nested
class VOICE
priority 128
set ip precedence 5
class VIDEO
bandwidth 320
set ip precedence 4
class APLICACIONES
bandwidth 256
set ip precedence 3
policy-map QoS_parent
class class-default
shape average 704000
service-policy QoS_nested
interface FastEthernet0/0
description ENLACE WAN RED GC
no ip address
no ip redirects
no ip proxy-arp
ip route-cache flow
duplex auto
speed auto
arp timeout 300
interface FastEthernet0/0.1883
description ENLACE WAN RED GC
bandwidth 704
encapsulation dot1Q 1883
ip address 10.117.113.114 255.255.255.248
no snmp trap link-status
arp timeout 300
service-policy output QoS_parent
interface FastEthernet0/1
bandwidth 704
no ip address
ip route-cache flow
duplex auto
speed auto
interface FastEthernet0/1.15
description VC
bandwidth 320
encapsulation dot1Q 15
ip address 200.0.30.73 255.255.255.248
ip accounting output-packets
no snmp trap link-status
interface FastEthernet0/1.67
description DATOS
bandwidth 256
encapsulation dot1Q 67
ip address 172.16.67.10 255.255.255.0
ip accounting output-packets
no snmp trap link-status
interface FastEthernet0/1.68
description VOIP
bandwidth 128
encapsulation dot1Q 68
ip address 172.16.68.10 255.255.255.0
ip accounting output-packets
no snmp trap link-status
interface FastEthernet0/1.100
encapsulation dot1Q 1 native
ip address 172.16.100.10 255.255.255.0
no snmp trap link-status
ip classless
ip route 0.0.0.0 0.0.0.0 10.117.113.113
ip flow-export source FastEthernet0/1.67
ip flow-export version 5
ip flow-export destination 172.16.50.57 9996
ip flow-export destination 172.16.85.15 9996
ip http server
ip access-list extended DATOS
permit tcp 172.16.67.0 0.0.0.255 host 172.16.50.54
eq 3128
permit udp 172.16.67.0 0.0.0.255 host 172.16.50.55
eq domain
permit udp 172.16.67.0 0.0.0.255 host 172.16.50.58
eq domain
permit ip 172.16.67.0 0.0.0.255 host 172.16.50.43
permit ip 172.16.67.0 0.0.0.255 host 172.16.3.132
permit ip 172.16.67.0 0.0.0.255 host 172.16.50.64
permit ip 172.16.67.0 0.0.0.255 host 172.16.50.60
permit ip 172.16.67.0 0.0.0.255 host 172.16.31.17
permit ip 172.16.67.0 0.0.0.255 host 172.16.50.62
permit ip 172.16.67.0 0.0.0.255 host 172.16.31.50
```

```
permit ip 172.16.67.0 0.0.0.255 host 172.16.13.7
permit ip 172.16.67.0 0.0.0.255 host 172.16.50.46
permit ip 172.16.67.0 0.0.0.255 host 172.16.50.41
permit ip 172.16.67.0 0.0.0.255 host 172.16.50.40
permit ip 172.16.67.0 0.0.0.255 host 172.16.50.42
permit ip 172.16.67.0 0.0.0.255 host 172.16.50.81
permit ip 172.16.67.0 0.0.0.255 host 172.16.90.12
permit ip 172.16.67.0 0.0.0.255 host 172.16.50.73
ip access-list extended VC
permit ip 200.0.30.72 0.0.0.7 any
ip access-list extended VOIP
permit ip 172.16.68.0 0.0.0.255 host 172.16.50.34
access-list 100 remark VOICE
access-list 100 permit ip 172.16.68.0 0.0.0.255 any
access-list 101 remark VIDEO
access-list 101 permit ip 200.0.30.72 0.0.0.7 any
access-list 102 remark APLICACIONES
access-list 102 permit ip 172.16.67.0 0.0.0.255 any
snmp-server community utpl RO
snmp-server host 172.16.50.57 utpl
snmp-server host 172.16.85.15 utpl
control-plane
privilege exec level 10 traceroute
privilege exec level 10 ping
privilege exec level 10 show startup-config
privilege exec level 10 show
line con 0
exec-timeout 5 0
password 7 104D000A0618
login local
line aux 0
line vty 0 4
session-timeout 1
exec-timeout 5 0
password 7 110A1016141D
login local
line vty 5 15
session-timeout 1
exec-timeout 5 0
login local
End
```

ANEXO 12 TABLA DE ENRUTAMIENTO SANTO DOMINGO (ACTUAL)

```
R-CR-SNT-DOMINGO#show ip route
Gateway of last resort is 10.117.113.113 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.100.0 is directly connected, FastEthernet0/1.100
C       172.16.68.0 is directly connected, FastEthernet0/1.68
C       172.16.67.0 is directly connected, FastEthernet0/1.67
     10.0.0.0/29 is subnetted, 1 subnets
C       10.117.113.112 is directly connected, FastEthernet0/0.1883
     200.0.30.0/29 is subnetted, 1 subnets
C       200.0.30.72 is directly connected, FastEthernet0/1.15
S*   0.0.0.0/0 [1/0] via 10.117.113.113
R-CR-SNT-DOMINGO#
```

ANEXO 13 CONFIGURACIÓN ROUTER SAN RAFAEL (ACTUAL)

```
R-CR-SAN_RAFAEL#show start
R-CR-SAN_RAFAEL#show startup-config
Using 4991 out of 196600 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-CR-SAN_RAFAEL
boot-start-marker
boot-end-marker
enable secret 5
$1$okYP$bZXpmlR1o1/Ex2S73MTxM/
no aaa new-model
resource policy
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
class-map match-any APLICACIONES
match access-group 102
class-map match-any VIDEO
match access-group 101
class-map match-any VOICE
match access-group 100
policy-map QoS_nested_video
class VIDEO
bandwidth 320
set ip precedence 4
policy-map QoS_parent_video
class class-default
shape average 320000
service-policy QoS_nested_video
policy-map QoS_nested_datos
class VOICE
priority 128
set ip precedence 5
class APLICACIONES
bandwidth 256
set ip precedence 3
policy-map QoS_parent_datos
class class-default
shape average 384000
service-policy QoS_nested_datos
interface FastEthernet0/0
description ENLACE WAN RED GC
no ip address
no ip redirects
no ip proxy-arp
ip route-cache flow
duplex auto
speed auto
arp timeout 300
interface FastEthernet0/0.120
description ENLACE-WAN-VC
bandwidth 320
encapsulation dot1Q 120
ip address 193.169.5.38 255.255.255.252
no snmp trap link-status
arp timeout 300
service-policy output QoS_parent_video
interface FastEthernet0/0.1883
description ENLACE-WAN-VOIP Y DATOS
bandwidth 384
encapsulation dot1Q 1883
ip address 10.111.134.130 255.255.255.248
no snmp trap link-status
arp timeout 300
service-policy output QoS_parent_datos
interface FastEthernet0/1
no ip address
ip route-cache flow
duplex auto
speed auto
interface FastEthernet0/1.15
description VC
bandwidth 320
encapsulation dot1Q 15
ip address 200.0.30.89 255.255.255.248
no snmp trap link-status
interface FastEthernet0/1.87
description VOIP
bandwidth 128
encapsulation dot1Q 87
ip address 172.16.87.10 255.255.255.0
no snmp trap link-status
interface FastEthernet0/1.100
encapsulation dot1Q 1 native
ip address 172.16.100.10 255.255.255.0
no snmp trap link-status
interface FastEthernet0/1.250
description DATOS
bandwidth 256
encapsulation dot1Q 250
ip address 172.16.250.1 255.255.255.0
no snmp trap link-status
ip classless
ip route 0.0.0.0 0.0.0.0 193.169.5.37
ip route 172.16.0.0 255.255.0.0 10.111.134.129
ip flow-export source FastEthernet0/1.250
ip flow-export version 5
ip flow-export destination 172.16.85.15 9996
ip http server
ip access-list extended DATOS
permit tcp 172.16.250.0 0.0.0.255 host 172.16.50.54
eq 3128
```

```
permit tcp 172.16.250.0 0.0.0.255 host 172.16.40.1
eq 3128
permit udp 172.16.250.0 0.0.0.255 host
172.16.50.55 eq domain
permit udp 172.16.250.0 0.0.0.255 host
172.16.50.58 eq domain
permit ip 172.16.250.0 0.0.0.255 host 172.16.50.43
permit ip 172.16.250.0 0.0.0.255 host 172.16.3.132
permit ip 172.16.250.0 0.0.0.255 host 172.16.50.64
permit ip 172.16.250.0 0.0.0.255 host 172.16.50.60
permit ip 172.16.250.0 0.0.0.255 host 172.16.31.17
permit ip 172.16.250.0 0.0.0.255 host 172.16.50.62
permit ip 172.16.250.0 0.0.0.255 host 172.16.31.50
permit ip 172.16.250.0 0.0.0.255 host 172.16.13.7
permit ip 172.16.250.0 0.0.0.255 host 172.16.50.46
permit ip 172.16.250.0 0.0.0.255 host 172.16.50.41
permit ip 172.16.250.0 0.0.0.255 host 172.16.50.40
permit ip 172.16.250.0 0.0.0.255 host 172.16.50.42
permit ip 172.16.250.0 0.0.0.255 host 172.16.50.81
permit ip 172.16.250.0 0.0.0.255 host 172.16.90.12
permit ip 172.16.250.0 0.0.0.255 host 172.16.50.73
ip access-list extended VC
permit ip 200.0.30.88 0.0.0.7 any
ip access-list extended VOIP
permit ip 172.16.87.0 0.0.0.255 host 172.16.50.34
access-list 100 remark VOICE
access-list 100 permit ip 172.16.87.0 0.0.0.255 any
access-list 101 remark VIDEO
access-list 101 permit ip 200.0.30.88 0.0.0.7 any
access-list 102 remark APLICACIONES
access-list 102 permit ip 172.16.86.0 0.0.0.255 any
snmp-server community utpl RO
snmp-server host 172.16.50.57 utpl
snmp-server host 172.16.85.15 utpl
control-plane
privilege exec level 10 traceroute
privilege exec level 10 ping
privilege exec level 10 show startup-config
privilege exec level 10 show
line con 0
exec-timeout 5 0
password 7 060506324F41
login local
line aux 0
line vty 0 4
session-timeout 1
exec-timeout 5 0

login local

line vty 5 15
session-timeout 1
exec-timeout 5 0
login local
end
```

ANEXO 14 TABLA DE ENRUTAMENTO SAN RAFAEL (ACTUAL)

```
R-CR-SAN_RAFAEL#show ip route
Gateway of last resort is 193.169.5.37 to network 0.0.0.0

     172.16.0.0/16 is variably subnetted, 4 subnets, 2 masks
C       172.16.250.0/24 is directly connected, FastEthernet0/1.250
S       172.16.0.0/16 [1/0] via 10.111.134.129
C       172.16.100.0/24 is directly connected, FastEthernet0/1.100
C       172.16.87.0/24 is directly connected, FastEthernet0/1.87
     193.169.5.0/30 is subnetted, 1 subnets
C       193.169.5.36 is directly connected, FastEthernet0/0.120
     10.0.0.0/29 is subnetted, 1 subnets
C       10.111.134.128 is directly connected, FastEthernet0/0.1883
     200.0.30.0/29 is subnetted, 1 subnets
C       200.0.30.88 is directly connected, FastEthernet0/1.15
S*   0.0.0.0/0 [1/0] via 193.169.5.37
R-CR-SAN_RAFAEL#
```

ANEXO 15 CONFIGURACIÓN ROUTER VILLAFLORA (ACTUAL)

```
R-CR-VILLAFLORA#show startup-config
Using 4634 out of 196600 bytes
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
hostname R-CR-VILLAFLORA
boot-start-marker
boot-end-marker
enable secret 5
$1$D7Qu$aduy6thPtAXpDH9JZdkUo0
no aaa new-model
resource policy
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
ip subnet-zero
ip cef
class-map match-any APLICACIONES
match access-group 102
class-map match-any VIDEO
match access-group 101
class-map match-any VOICE
match access-group 100
policy-map QoS_nested
class VOICE
priority 128
set ip precedence 5
class VIDEO
bandwidth 320
set ip precedence 4
class APLICACIONES
bandwidth 256
set ip precedence 3
policy-map QoS_parent
class class-default
shape average 704000
service-policy QoS_nested
interface FastEthernet0/0
description ENLACE WAN RED GC
bandwidth 704
no ip address
no ip redirects
no ip proxy-arp
ip route-cache flow
load-interval 30
speed auto
full-duplex
arp timeout 300
interface FastEthernet0/0.354
description ENLACE WAN RED GC
bandwidth 704
encapsulation dot1Q 354
ip address 10.111.130.66 255.255.255.248
no snmp trap link-status
arp timeout 300
service-policy output QoS_parent
interface FastEthernet0/1
no ip address
ip accounting output-packets
ip route-cache flow
duplex auto
speed auto
!
interface FastEthernet0/1.15
description VIDEOCONFERENCIA
bandwidth 320
encapsulation dot1Q 15
ip address 200.0.30.65 255.255.255.248
no snmp trap link-status
interface FastEthernet0/1.58
description VOIP
bandwidth 128
encapsulation dot1Q 58
ip address 172.16.58.10 255.255.255.0
no snmp trap link-status
interface FastEthernet0/1.100
encapsulation dot1Q 1 native
ip address 172.16.100.10 255.255.255.0
no snmp trap link-status
interface FastEthernet0/1.249
description DATOS
bandwidth 256
encapsulation dot1Q 249
ip address 172.16.249.10 255.255.255.0
no snmp trap link-status
ip classless
ip route 0.0.0.0 0.0.0.0 10.111.130.65
ip flow-export source FastEthernet0/1.249
ip flow-export version 5
ip flow-export destination 172.16.85.15 9996
ip http server
ip access-list extended DATOS
permit tcp 172.16.249.0 0.0.0.255 host 172.16.50.54
eq 3128
permit udp 172.16.249.0 0.0.0.255 host
172.16.50.55 eq domain
permit udp 172.16.249.0 0.0.0.255 host
172.16.50.58 eq domain
permit ip 172.16.249.0 0.0.0.255 host 172.16.50.43
permit ip 172.16.249.0 0.0.0.255 host 172.16.3.132
permit ip 172.16.249.0 0.0.0.255 host 172.16.50.64
permit ip 172.16.249.0 0.0.0.255 host 172.16.50.60
permit ip 172.16.249.0 0.0.0.255 host 172.16.31.17
permit ip 172.16.249.0 0.0.0.255 host 172.16.50.62
permit ip 172.16.249.0 0.0.0.255 host 172.16.31.50
permit ip 172.16.249.0 0.0.0.255 host 172.16.13.7
```

```
permit ip 172.16.249.0 0.0.0.255 host 172.16.50.46
permit ip 172.16.249.0 0.0.0.255 host 172.16.50.41
permit ip 172.16.249.0 0.0.0.255 host 172.16.50.40
permit ip 172.16.249.0 0.0.0.255 host 172.16.50.42
permit ip 172.16.249.0 0.0.0.255 host 172.16.50.81
permit ip 172.16.249.0 0.0.0.255 host 172.16.90.12
permit tcp 172.16.249.0 0.0.0.255 host 172.16.40.1
eq 3128
permit ip 172.16.249.0 0.0.0.255 host 172.16.50.73
ip access-list extended VC
permit ip 200.0.30.64 0.0.0.7 any
ip access-list extended VOIP
permit ip 172.16.58.0 0.0.0.255 host 172.16.50.34
access-list 100 remark VOICE
access-list 100 permit ip 172.16.58.0 0.0.0.255 any
access-list 101 remark VIDEO
access-list 101 permit ip 200.0.30.64 0.0.0.7 any
access-list 102 remark APLICACIONES
access-list 102 permit ip 172.16.249.0 0.0.0.255 any
snmp-server community utpl RO
snmp-server host 172.16.50.57 utpl
snmp-server host 172.16.85.15 utpl
control-plane
privilege exec level 10 traceroute
privilege exec level 10 ping
privilege exec level 10 show startup-config
privilege exec level 10 show
line con 0
exec-timeout 5 0
password 7 104D000A0618
login local
line aux 0
line vty 0 4
session-timeout 1
exec-timeout 5 0
password 7 110A1016141D
login local
line vty 5 15
session-timeout 1
exec-timeout 5 0
login local
end

R-CR-VILLAFLORA#
```

ANEXO 16 TABLA DE ENRUTAMIENTO VILLAFLORA (ACTUAL)

```
R-CR-VILLAFLORA#show ip route

Gateway of last resort is 10.111.130.65 to network 0.0.0.0

     172.16.0.0/24 is subnetted, 3 subnets
C       172.16.249.0 is directly connected, FastEthernet0/1.249
C       172.16.58.0 is directly connected, FastEthernet0/1.58
C       172.16.100.0 is directly connected, FastEthernet0/1.100
     10.0.0.0/29 is subnetted, 1 subnets
C       10.111.130.64 is directly connected, FastEthernet0/0.354
     200.0.30.0/29 is subnetted, 1 subnets
C       200.0.30.64 is directly connected, FastEthernet0/1.15
S*   0.0.0.0/0 [1/0] via 10.111.130.65
R-CR-VILLAFLORA#
```

ANEXO 17 RESUMEN CONFIGURACIÓN DE LOS ROUTERS (ACTUAL)

CIUDAD	FAST ETHERNET	DIRECCIONES	SERVICIOS	ANCHO DE BANDA	PRESEDENCIA QoS	PROTOCOLO ENRUTADO	IOS COMPATIBLE ALGORITMOS DE ENRUTAMIENTO	ARCHIVOS DE CONFIGURACIÓN
QUITO	F0/1.15	200.0.30.1/28	VIDEO	512kbps	4	IPv4	Si	ANEXO 3 ANEXO 4
	F0/1.40	172.16.40.10/24	DATOS	384kbps	3			
	F0/1.46	172.16.46.65/24	VOZ	1500kbps	5			
	F0/1.100	172.16.100.10/24	ADMINISTRACIÓN					
	F0/0	10.111.134.38/29						
GUAYAQUIL	F0/1.15	200.0.30.17/29	VIDEO	640kbps	4	IPv4	Si	ANEXO 5 ANEXO 6
	F0/1.42	172.16.42.10/24	DATOS	256kbps	3			
	F0/1.48	172.16.48.10/24	VOZ	128kbps	5			
	F0/1.100	172.16.100.10/24	ADMINISTRACION					
	F0/0.354	10.112.115.110	ENLACE WAN	1000kbps				
CUENCA	F0/1.15	200.0.30.25/29	VIDEO	640kbps	4	IPv4	Si	ANEXO 7 ANEXO 8
	F0/1.44	172.16.44.10/24	DATOS	256kbps	3			
	F0/1.47	172.16.47.10/24	VOZ	128kbps	5			
	F0/1.100	172.16.100.10/24	ADMINISTRACION					
	F0/0.354	10.113.114.122/29	ENLACE WAN	1400kbps				
MANTA	F0/1.15	200.0.30.81/29	VIDEO	640kbps	4	IPv4	Si	ANEXO 9 ANEXO 10
	F0/1.77	172.16.77.10/24	DATOS	256kbps	3			
	F0/1.78	172.16.78.10/24	VOZ	128kbps	5			
	F0/1.1	172.16.100.10/24	ADMINISTRACION					
	F0/0.354	10.113.114.146/29	ENLACE WAN	1400kbps				
SANTO DOMINGO	F0/1.15	200.0.30.73/29	VIDEO	320kbps	4	IPv4	Si	ANEXO 11 ANEXO 12
	F0/1.67	172.16.67.10/24	DATOS	256kbps	3			
	F0/1.68	172.16.68.10/24	VOZ	128kbps	5			
	F0/1.100	172.16.100.10/24	ADMINISTRACION					
	F0/0.1883	10.117.113.114./29	ENLACE WAN	704kbps				

SAN RAFAEL	F0/1.15	200.0.30.89/29	VIDEO	320kbps	4	IPv4	Si	ANEXO 13 ANEXO 14
	F0/1.87	172.16.87.10/24	VOZ	128kbps	5			
	F0/1.250	172.16.250.1/24	DATOS	256kbps	3			
	F0/1.100	172.16.100.10/24	ADMINISTRACION					
	F0/0.120	193.169.5.38/30	ENLACE WAN VIDEO	320kbps				
	F0/0.1883	10.111.134.130/29	ENLACE WAN VOIP Y DATOS	384kbps				
	F0/1.15	200.0.30.89/29	VIDEO	320kbps	4			
VILLAFLORA	F0/1.15	200.0.30.65/29	VIDEO	320kbps	4	IPv4	Si	ANEXO 15 ANEXO 16
	F0/1.249	172.16.249.10/24	DATOS	256kbps	3			
	F0/1.58	172.16.58.10/24	VOZ	128kbps	5			
	F0/1.100	172.16.100.10/24	ADMINISTRACION					
	F0/0.354	10.111.130.66/29	ENLACE WAN	704kbps				

ANEXO 18 RESUMEN DE LOS PROTOCOLOS DE ENRUTAMIENTO

PROTOCOLOS DE ENRUTAMIENTO (RESUMEN)											
PROTOCOLO	*VECTOR DISTANCIA*	*ESTADO DE ENLACE*	*# SALTOS*	*ACTUALIZACIÓN EN SEGUNDOS*	*DESACTIVACIÓN EN SEGUNDOS*	*TIEMPO DE BORRADO EN SEG.*	*DISTANCIA ADMINISTRATIVA*	*DESARROLLADO POR*	*METRICAS*	*ALGORITMO*	*CREADO*
RIP	✓		15	30	180	300	120	UNIVERSAL	Conteo de saltos	BELLMAN FORD	1957
IGRP	✓		255	90	270	630	100	CISCO	Métrica compuesta ✓ ANCHO DE BANDA (POR DEFECTO) ✓ RETRASO (POR DEFECTO) ✓ CONFIABILIDAD ✓ CARGA	BELLMAN FORD	1984
EIGRP	DUAL		224	CUANDO HAY CAMBIOS EN LA RED (5 segundos con saludo Hello)	15 (con saludo Hello)		90	CISCO	Métrica compuesta ✓ ANCHO DE BANDA (POR DEFECTO) ✓ RETRASO (POR DEFECTO) ✓ CONFIABILIDAD ✓ CARGA	BELLMAN FORD Y DIJKSTRA	1994
OSPF		✓	SIN LIMITE	CUANDO HAY CAMBIOS EN LA RED			110	UNIVERSAL	✓ ANCHO DE BANDA	DIJKSTRA	1988
IS-IS		✓	SIN LIMITE	CUANDO HAY CAMBIOS EN LA RED			115	UNIVERSAL	✓ CON VALOR MÁXIMO DE 1024 ✓ RETARDO DE ENLACE ✓ COSTO DE ENLACE ✓ ERRORES DE ENLACE	DIJKSTRA	1990

ANEXO 19 RESUMEN DE LOS PROTOCOLOS ENRUTADOS IP

PROTOCOLOS ENRUTADOS (RESUMEN)							
PROTOCOLO	**TAMAÑO DE DIRECCIÓN**	**FORMATO DE DIRECCIONES**	**SEGURIDAD**	**SIMPLIFICA ENCABEZADO**	**AUTOCONFIGURACIÓN**	**CREADO PARA**	**CREADO**
IPV4	2^{32}	DECIMAL	X	X	X	CONEXIÓN	1981
IPV6	2^{128}	HEXADECIMAL	IPSEC	✓	✓	CONEXIÓN Y MOVILIDAD	1999

ANEXO 20 COMPARACIÓN DE LOS PROTOCOLOS DE ENRUTAMIENTO [46]

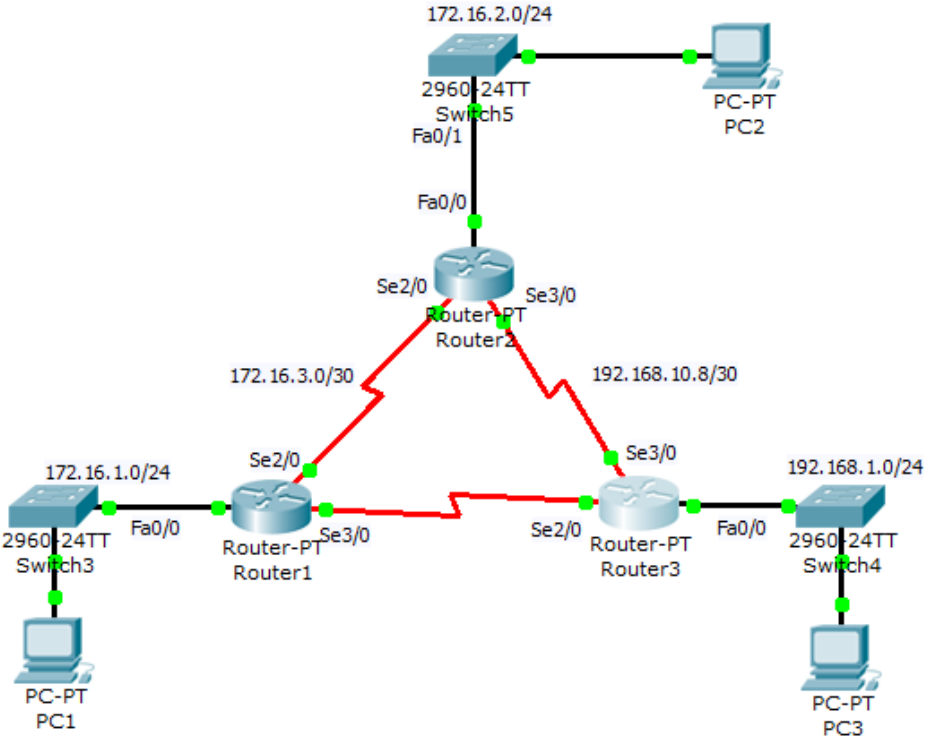
CARACTERISTICAS DE LOS PROTOCOLOS DE ENRUTAMIENTO									
PROTOCOLO	**PROPIETARIO CISCO**	**REDES GRANDES**	**ALGORITMO DUAL**	**MAYOR ESCALABILIDAD**	**SEGURIDAD**	**VELOCIDAD DE CONVERGENCIA**	**MENOR DISTANCIA ADMINISTRATIVA**	**DEPENDE DE TOPOLOGIA**	**SOPORTE PARA VLSM**
RIP									
IGRP	✓	✓				✓			
EIGRP	✓	✓	✓	✓	✓	✓	✓		✓
OSPF		✓		✓	✓			✓	✓
IS-IS				✓				✓	✓
BGP				✓					✓
DESCRIPCIÓN	Quien lo diseño	Mayores a 15 saltos	Estado de enlace y vector distancia	Crecimiento de la red y adaptacion	MD5	Varias métricas	Mayor grado de confiabilidad	Cambios de la red	Mascara de subred de tamaño variable

ANEXO 21 EJERCICIO DE CONFIGURACIÓN BÁSICA DE EIGRP Y DE DISPOSITIVOS ROUTERS Y SWITCH

En la investigación se ha revisado algunos comandos utilizados en el enrutamiento dinámico que se utiliza para configurar los dispositivos Routers y Switch estos comandos nos sirven para realizar varias tareas dentro de los dispositivos Routers. De una mejor manera quedará explicado con un ejemplo en el cual utilizaremos la configuración estática de EIGRP con una tabla de direcciones dada. Cabe recalcar que estos ejemplos aunque realizado con una configuración sobre los protocolos enrutados IPv4 nos sirven para ir afianzando los conocimientos y tener las bases para el entendimiento y entrenamiento del funcionamiento del enrutamiento dinámico, configuraciones de Routers y Switch que se realizará en un capítulo posterior.

Ejemplo de configuración básica de EIGRP

Para este ejemplo tendremos que visualizar el ANEXO 36, donde las direcciones IP que se usaran en cada interface.



Configuración básica de EIGRP [41]

A medida que vamos desarrollando el ejercicio nos daremos cuenta de los comandos que son necesarios para una configuración básica del protocolo de enrutamiento EIGRP.

Como primer paso configuramos los enlaces seriales de los Routers R1, R2, R3 su configuración se puede visualizar en el ANEXO 37, luego configuramos las interfaces Ethernet en cada Router, como vemos en la Figura 18, las Ethernet son las Fa0/0 en cada

Router, la configuración de estas interfaces se puede ver en el ANEXO 38, luego colocamos la dirección IP, la máscara de subred y el Gateway para cada PC, con los valores que están en el ANEXO 36. Una vez que ya hemos configurado esto junto con las configuraciones básicas de los Routers, procedemos a configurar el protocolo de enrutamiento en los Routers. Para esto utilizamos el comando "Router eigrp 1" en el modo de configuración global para permitir EIGRP en el Router. El numero 1 significa un identificador de procesos para parámetros de sistema autónomos (ver ANEXO 39). Luego configuramos el "Classful Network" (arquitectura de la red) (ver ANEXO 39), una vez configurado el Classful Network, el Router podrá enviar mensajes de actualización de EIGRP a cada interface Ethernet o serial que pertenezca a la red que se establece en Classful Network. En este caso envía las actualizaciones a Fa0/0 y serial2/0 del Router1.

Luego configuramos la Wildcard-mask para anunciar la subred de la interface serial3/0 del router 1, la Wildcard-mask solo anuncia la subred, no toda la red de Classful **N**etwork, y para hacer esto se toma la parte inversa de la máscara de subred (ver ANEXO 39). Luego de esto se guarda la configuración realizada en el router1.

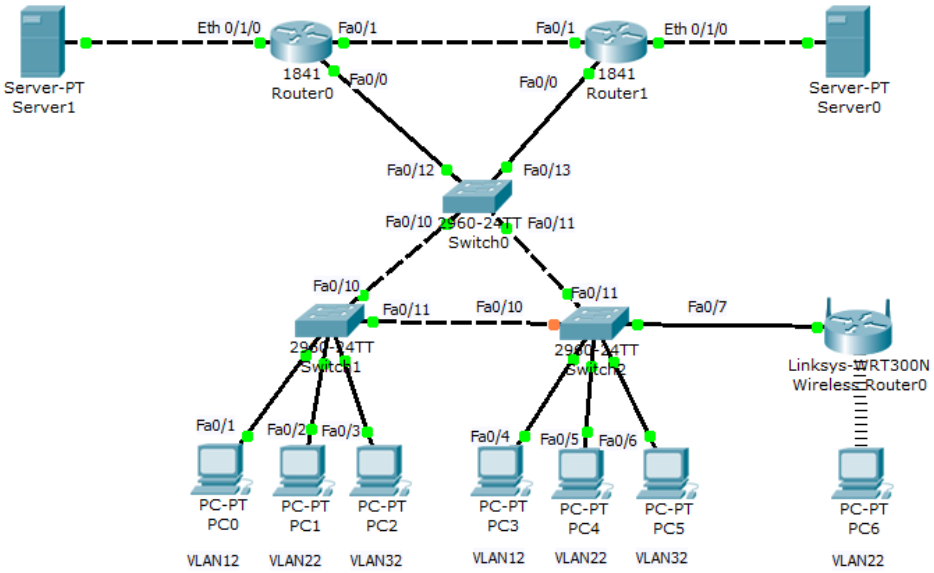
En el R2 y el R3 se realiza la misma configuración con diferentes datos (ver ANEXO 40), cuando se está configurando la Classful Network se llega a identificar la relación con los Routers EIRGP vecinos.

Algunos comandos que se utiliza para visualizar los datos de la configuración son los siguientes:

- **Show IP eigrp neighbors:** Para ver los vecinos de los Routers que están configurados con EIGRP. (ver ANEXO 41).
- **Show IP protocols:** Para ver información acerca de las operaciones del protocolo de enrutamiento (ver ANEXO 41).
- **Show IP route:** Eigrp denota con la letra "D" (doble), cual es el algoritmo de enrutamiento utilizado por EIGRP.
- **Show interface serial n/n:** para ver las métricas de EIGRP. (ANEXO 41)

Para modificar las métricas lo único que se hace es entrar a la interface y utilizar los comandos "Bandwidth xx".

Ejemplo de configuración básica de Switch y Routers



Configuración de Switch y Routers

En este ejercicio nosotros hemos realizado configuraciones de Routers y Switch, así como las configuraciones de interfaces VLAN y Sub-interfaces, además se configuró un Router Wireless con el objetivo de afianzar los conocimientos y aplicarlos en el enrutamiento dinámico, el objetivo de esta práctica es realizar conexiones simultaneas entre VLANS diferentes utilizando dispositivos de capa dos (Switch) y capa tres (routers) del modelo OSI.

ANEXO 22 DIRECCIONAMIENTO MULTICAST

NODO LOCAL SCOPE		ALL SCOPE MULTICAST ADDRESSES		ALL SCOPE MULTICAST ADDRESSES	
FF01:0:0:0:0:0:0:1	All Nodes Address	FF0X:0:0:0:0:0:0:0	Reserved Multicast Address	FF0X:0:0:0:0:0:0:118	microsoft-ds
FF01:0:0:0:0:0:0:2	All Routers Address	FF0X:0:0:0:0:0:0:100	VMTP Managers Group	FF0X:0:0:0:0:0:0:119	nbc-pro
SITE-LOCAL SCOPE		FF0X:0:0:0:0:0:0:101	Network Time Protocol (NTP)	FF0X:0:0:0:0:0:0:11A	nbc-pfn
FF05:0:0:0:0:0:0:2	All Routers Address	FF0X:0:0:0:0:0:0:102	SGI-Dogfight	FF0X:0:0:0:0:0:0:11B	lmsc-calren-1
FF05:0:0:0:0:0:1:3	All-dhcp-servers	FF0X:0:0:0:0:0:0:103	Rwhod	FF0X:0:0:0:0:0:0:11C	lmsc-calren-2
FF05:0:0:0:0:0:1:4	All-dhcp-relays	FF0X:0:0:0:0:0:0:104	VNP	FF0X:0:0:0:0:0:0:11D	lmsc-calren-3
FF05:0:0:0:0:0:1:1000	Service Location	FF0X:0:0:0:0:0:0:105	Artificial Horizons – Aviator	FF0X:0:0:0:0:0:0:11E	lmsc-calren-4
FF05:0:0:0:0:0:1:13FF		FF0X:0:0:0:0:0:0:106	NSS - Name Service Server	FF0X:0:0:0:0:0:0:11F	ampr-info
LINK LOCAL SCOPE		FF0X:0:0:0:0:0:0:107	AUDIONEWS - Audio News Multicast	FF0X:0:0:0:0:0:0:120	mtrace
FF02:0:0:0:0:0:0:1	All Nodes Address	FF0X:0:0:0:0:0:0:108	SUN NIS+ Information Service	FF0X:0:0:0:0:0:0:121	RSVP-encap-1
FF02:0:0:0:0:0:0:2	All Routers Address	FF0X:0:0:0:0:0:0:109	MTP Multicast Transport Protocol	FF0X:0:0:0:0:0:0:122	RSVP-encap-2
FF02:0:0:0:0:0:0:3	Unassigned	FF0X:0:0:0:0:0:0:10ª	IETF-1-LOW-AUDIO	FF0X:0:0:0:0:0:0:123	SVRLOC-DA
FF02:0:0:0:0:0:0:4	DVMRP Routers	FF0X:0:0:0:0:0:0:10B	IETF-1-AUDIO	FF0X:0:0:0:0:0:0:124	rln-server
FF02:0:0:0:0:0:0:5	OSPFIGP	FF0X:0:0:0:0:0:0:10C	IETF-1-VIDEO	FF0X:0:0:0:0:0:0:125	proshare-mc
FF02:0:0:0:0:0:0:6	OSPFIGP Designated Routers	FF0X:0:0:0:0:0:0:10D	IETF-2-LOW-AUDIO	FF0X:0:0:0:0:0:0:126	dantz
FF02:0:0:0:0:0:0:7	ST Routers	FF0X:0:0:0:0:0:0:10E	IETF-2-AUDIO	FF0X:0:0:0:0:0:0:127	cisco-rp-announce
FF02:0:0:0:0:0:0:8	ST Host	FF0X:0:0:0:0:0:0:10F	IETF-2-VIDEO	FF0X:0:0:0:0:0:0:128	cisco-rp-discovery
FF02:0:0:0:0:0:0:9	RIP Routers	FF0X:0:0:0:0:0:0:110	MUSIC-SERVICE	FF0X:0:0:0:0:0:0:129	gatekeper
FF02:0:0:0:0:0:0:A	EIGRP Routers	FF0X:0:0:0:0:0:0:111	SEANET-TELEMETRY	FF0X:0:0:0:0:0:0:12A	iberiagames
FF02:0:0:0:0:0:0:B	Mobile-Agents	FF0X:0:0:0:0:0:0:112	SEANET-IMAGE	FF0X:0:0:0:0:0:0:201	"rwho" Group (BSD) (unofficial)
FF02:0:0:0:0:0:0:D	All PIM Routers	FF0X:0:0:0:0:0:0:113	MLOADD	FF0X:0:0:0:0:0:0:202	SUN RPC PMAPPROC_CALLIT
FF02:0:0:0:0:0:0:E	RSVP-ENCAPSULATION	FF0X:0:0:0:0:0:0:114	any private experiment	-FF0X:0:0:0:0:0:2:7FFD	Multimedia Conference Calls
FF02:0:0:0:0:0:1:1	Link Name	FF0X:0:0:0:0:0:0:115	DVMRP on MOSPF	FF0X:0:0:0:0:0:2:7FFE	SAPv1 Announcements
FF02:0:0:0:0:0:1:2	All-dhcp-agents	FF0X:0:0:0:0:0:0:116	SVRLOC	FF0X:0:0:0:0:0:2:7FFF	SAPv0 Announcements
FF02:0:0:0:0:1:FFXX:XXXX	Solicited-Node Address	FF0X:0:0:0:0:0:0:117	XINGTV	-FF0X:0:0:0:0:0:2:FFFF	SAP Dynamic Assignments

ANEXO 23 CONFIGURACIÓN DEL ASA (ACTUAL)

```
interface GigabitEthernet0/0
description Conexion a f0/5 (f0/6) del Cat2950 de borde.
speed 100
duplex full
nameif outside
security-level 0
ip address 200.0.31.153 255.255.255.224 standby 200.0.31.154
ipv6 address 2800:130:1:222::153/64 (PUBLICA)
ipv6 address fe80::21b:cff:fe38:f67a link-local
ipv6 nd suppress-ra
interface GigabitEthernet0/1
description Conexión a g3/9 (g3/1) del Cat6509 de core.
speed 1000
duplex full
nameif campus
security-level 100
ip address 192.168.254.252 255.255.255.0 standby 192.168.254.251
ipv6 address 2800:130:1:254::252/64
ipv6 address fe80::21b:cff:fe38:f67b link-local
ipv6 nd dad attempts 0
interface GigabitEthernet0/2.55
description VLAN de frontales55.
vlan 55
nameif frontales55
security-level 55
ip address 172.16.55.1 255.255.255.0 standby 172.16.55.2
ipv6 address 2800:130:1:55::1/64
ipv6 address fe80::21b:cff:fe38:f67c link-local
interface GigabitEthernet0/2.60
description VLAN de frontales60.
 vlan 60
nameif frontales60
security-level 60
ip address 172.16.60.1 255.255.255.0 standby 172.16.60.2
ipv6 address 2800:130:1::60/64
ipv6 address fe80::21b:cff:fe38:f67c link-local
interface GigabitEthernet0/2.75
description VLAN de frontales75.
vlan 75
nameif frontales75
security-level 75
ip address 172.16.75.1 255.255.255.0 standby 172.16.75.2
ipv6 address 2800:130:1:75::1/64
ipv6 address fe80::21b:cff:fe38:f67c link-local
interface GigabitEthernet0/2.80
description VLAN de frontales80.
vlan 80
nameif frontales80
security-level 80
ip address 172.16.80.1 255.255.255.0 standby 172.16.80.2
ipv6 address 2800:130:1:80::1/64
ipv6 address fe80::21b:cff:fe38:f67c link-local
interface GigabitEthernet0/3.85
description VLAN de frontales85.
vlan 85
nameif frontales85
security-level 85
ip address 172.16.85.1 255.255.255.0 standby 172.16.85.2
interface GigabitEthernet0/3.90
description VLAN de frontales90.
vlan 90
nameif frontales90
security-level 90
ip address 172.16.90.1 255.255.255.0 standby 172.16.90.2
!
```

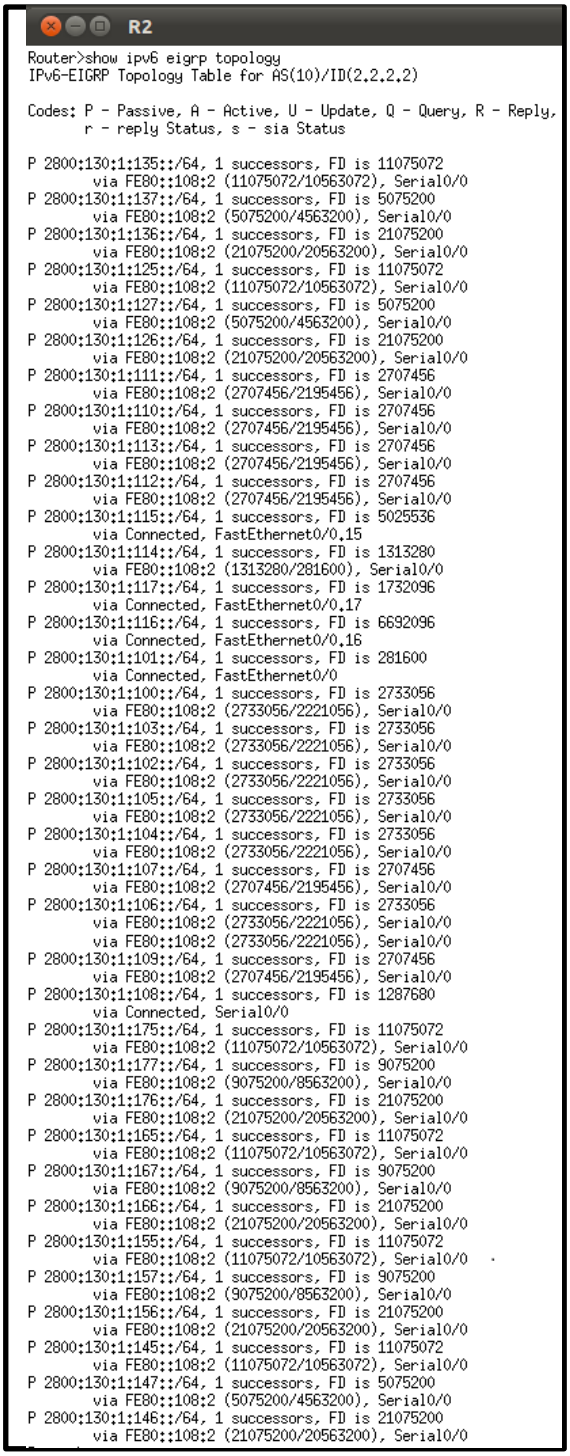
ANEXO 24 RUTAS ASA (ACTUAL)

ipv6 route campus 2800:130::/32 2800:130:1:254::10
ipv6 route outside ::/0 2800:130:1:222::156

ANEXO 25 INFORMACIÓN DE VLANS (ACTUAL)

INFORMACION VLANs					
VLAN	**DEPARTAMENTO**	**INTERFACES**	**VLAN**	**DEPARTAMENTO**	**INTERFACES**
1	Default	Gi1/3, Gi1/4, Gi1/5, Gi1/6 Gi4/4, Gi5/2	50	SERVIDORES	Gi3/14
2	ADM	Activo	51	VLAN-PROXY	Activo
3	CITTES	Activo	52	Servers_Inside	Activo
4	CENTRAL	Activo	55	ISP	Activo
5	LABII	Activo	60	FRONTUTPL	Activo
6	OCTOG	Activo	65	MARISTAS	Activo
7	ABIERTA	Activo	66	CAMARAS-SEG	Activo
8	SISABI	Activo	67	STO-DOMINGO-DATOS	Activo
9	CENTROEVALUACIONES	Activo	68	STO-DOMINGO-VOIP	Activo
10	TELE-IP	Activo	69	GALAPAGOS	Activo
11	SALAS	Activo	70	TELEFONIA	Activo
12	SALAS-2	Activo	71	WIRELESS-EVENTOS	Activo
13	H-CASA-LOJAN	Activo	75	Servers_voip	Activo
14	CONTABILIDAD	Activo	77	CR_MANTA	Activo
15	VIDEOC	Activo	80	Frontales_80	Activo
16	EDITORIAL	Activo	81	r-coca	Activo
17	VALLE-TEC	Activo	82	GDLN	Activo
18	CITTES-B	Activo	83	ISUMMIT	Activo
19	DOCENTES	Activo	84	IEEE	Activo
20	TAME	Activo	85	Vpn_ssl	Activo
21	SALA-CISCO	Activo	86	BARCAMP2	Activo
22	ECOLAC	Activo	88	LAB-INGLES	Activo
23	CENTROCONVEN	Activo	89	CAMARAS	Activo
24	BCOLOJA	Activo	90	FRONTALES-BD	Activo
25	REDINALAMBRICA	Activo	97	Centros	Activo
26	CLUSTER-UCG	Activo	98	Contabilidad	Activo
27	MATRICULAS	Activo	189	TESIS-INV	Gi3/15
29	IMPRESORAS	Activo	200	INTERNET_2	Activo
30	ADM-INT	Activo	222	ZONA_BORDE	Activo
31	DESARROLADORES	Activo	223	PUBLIC-TELCO	Activo
32	AUTORIDADES	Activo	225	RADIO_VIRTUAL	Activo
33	AP-BIBLIOTECA	Activo	226	PSTM	Activo
34	WEBCONTENT	Activo	243	VIDEOMULTICAST	Activo
35	E-SOLCA	Activo	244	VIDEOMULTICASTRX	Activo
37	EVA-CAL	Activo	254	ENL-PIX	Activo
43	GY	Activo	300	CONEXION_TELCONET_DIRECTA	Activo
45	CRC	Activo			

ANEXO 26 TOPOLOGÍA DE RED IPv6 (SIMULADO)



ANEXO 27 ARCHIVOS DE CONFIGURACIÓN DE LA RED DE QUITO IPV6 (SIMULADO)

ARCHIVO DE CONFIGURACIÓN DE R1 QUITO

```
12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::114:2 link-local
 ipv6 address 2800:130:1:114::2/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 no ip address
 ipv6 address FE80::108:2 link-local
 ipv6 address 2800:130:1:108::2/64
 ipv6 enable
 ipv6 eigrp 10
 clock rate 2000000
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 1.1.1.1
 no shutdown
control-plane
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
end
```

ARCHIVO DE CONFIGURACION DE R2 QUITO

```
version 12.4

service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
class-map match-any APLICACIONES
 match access-group name quito
 match  precedence 4
 match  precedence 3
class-map match-any VIDEO
 match access-group name quito
 match  precedence 4
class-map match-any VOICE
 match access-group name quito
 match  precedence 5
policy-map QoS_nested
 class VOICE
  priority 384
 class VIDEO
  bandwidth 1500
 class APLICACIONES
  bandwidth 512
policy-map QoS_parent
 class class-default
  shape average 2400000
```

```
 service-policy QoS_nested
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::101:1 link-local
 ipv6 address 2800:130:1:101::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.1
 description datos vlan0.1
 encapsulation dot1Q 1 native
interface FastEthernet0/0.15
 description datos_quito
 bandwidth 512
 encapsulation dot1Q 15
 ipv6 address 2800:130:1:115::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.16
 description voip_quito
 bandwidth 384
 encapsulation dot1Q 16
 ipv6 address 2800:130:1:116::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.17
 description video_quito
 bandwidth 1500
 encapsulation dot1Q 17
 ipv6 address 2800:130:1:117::1/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 description enalce wan
 bandwidth 3300
 no ip address
 ipv6 address FE80::108:1 link-local
 ipv6 address 2800:130:1:108::1/64
 ipv6 enable
 ipv6 traffic-filter quito out
 ipv6 eigrp 10
 clock rate 2000000
 service-policy output QoS_paren
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 2.2.2.2
 no shutdown
ipv6 access-list quito
 permit ipv6 host 2800:130:1:115::2 host
2800:130:1:125::2
 permit ipv6 host 2800:130:1:116::2 host
2800:130:1:126::2
 permit ipv6 host 2800:130:1:117::2 host
2800:130:1:127::2
 permit ipv6 host 2800:130:1:115::2 host
2800:130:1:135::2
 permit ipv6 host 2800:130:1:116::2 host
2800:130:1:136::2
 permit ipv6 host 2800:130:1:117::2 host
2800:130:1:137::2
 permit ipv6 host 2800:130:1:115::2 host
2800:130:1:145::2
 permit ipv6 host 2800:130:1:116::2 host
2800:130:1:146::2
 permit ipv6 host 2800:130:1:117::2 host
2800:130:1:147::2
 permit ipv6 host 2800:130:1:115::2 host
2800:130:1:155::2
 permit ipv6 host 2800:130:1:116::2 host
2800:130:1:156::2
 permit ipv6 host 2800:130:1:117::2 host
2800:130:1:157::2
 permit ipv6 host 2800:130:1:115::2 host
2800:130:1:165::2
 permit ipv6 host 2800:130:1:116::2 host
2800:130:1:166::2
 permit ipv6 host 2800:130:1:117::2 host
2800:130:1:167::2
 permit ipv6 host 2800:130:1:115::2 host
2800:130:1:175::2
 permit ipv6 host 2800:130:1:116::2 host
2800:130:1:176::2
 permit ipv6 host 2800:130:1:117::2 host
2800:130:1:177::2
 deny ipv6 any any
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
```

ANEXO 28 ARCHIVOS DE CONFIGURACIÓN DE LA RED DE GUAYAQUIL IPV6 (SIMULADO)

ARCHIVO DE CONFIGURACIÓN DE R5 GUAYAQUIL

```
12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::114:3 link-local
 ipv6 address 2800:130:1:114::3/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 no ip address
 ipv6 address FE80::109:2 link-local
 ipv6 address 2800:130:1:109::2/64
 ipv6 enable
 ipv6 eigrp 10
 clock rate 2000000
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 5.5.5.5
 no shutdown
control-plane
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
end
```

ARCHIVO DE CONFIGURACIÓN DE R6 GUAYAQUIL

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
class-map match-any APLICACIONES
 match access-group name guayaquil
 match  precedence 3
class-map match-any VIDEO
 match access-group name guayaquil
 match  precedence 4
class-map match-any VOICE
 match access-group name guayaquil
 match  precedence 5
policy-map QoS_nested
 class VOICE
  priority 128
 class VIDEO
  bandwidth 640
 class APLICACIONES
  bandwidth 256
policy-map QoS_parent
```

```
 class class-default
  shape average 1024000
  service-policy QoS_nested
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::102:1 link-local
 ipv6 address 2800:130:1:102::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.25
 description datos_guayaquil
 bandwidth 256
 encapsulation dot1Q 25
 ipv6 address 2800:130:1:125::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.26
 description voip_guayaquil
 bandwidth 128
 encapsulation dot1Q 26
 ipv6 address 2800:130:1:126::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.27
 description video_guayaquil
 bandwidth 640
 encapsulation dot1Q 27
 ipv6 address 2800:130:1:127::1/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 description enlace_wan
 bandwidth 1000
 no ip address
 ipv6 address FE80::109:1 link-local
 ipv6 address 2800:130:1:109::1/64
 ipv6 enable
 ipv6 traffic-filter guayaquil out
 ipv6 eigrp 10
 clock rate 2000000
 service-policy output QoS_parent
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 6.6.6.6
 no shutdown
ipv6 access-list guayaquil
 permit ipv6 host 2800:130:1:125::2 host
2800:130:1:115::2
 permit ipv6 host 2800:130:1:126::2 host
2800:130:1:116::2
 permit ipv6 host 2800:130:1:127::2 host
2800:130:1:117::2
 deny ipv6 any any
 permit ipv6 host 2800:130:1:125::2 host
2800:130:1:135::2
 permit ipv6 host 2800:130:1:126::2 host
2800:130:1:136::2
 permit ipv6 host 2800:130:1:127::2 host
2800:130:1:137::2
 permit ipv6 host 2800:130:1:125::2 host
2800:130:1:145::2
 permit ipv6 host 2800:130:1:126::2 host
2800:130:1:146::2
 permit ipv6 host 2800:130:1:127::2 host
2800:130:1:147::2
 permit ipv6 host 2800:130:1:125::2 host
2800:130:1:155::2
 permit ipv6 host 2800:130:1:126::2 host
2800:130:1:156::2
 permit ipv6 host 2800:130:1:127::2 host
2800:130:1:157::2
 permit ipv6 host 2800:130:1:125::2 host
2800:130:1:165::2
 permit ipv6 host 2800:130:1:126::2 host
2800:130:1:166::2
 permit ipv6 host 2800:130:1:127::2 host
2800:130:1:167::2
 permit ipv6 host 2800:130:1:125::2 host
2800:130:1:175::2
 permit ipv6 host 2800:130:1:126::2 host
2800:130:1:176::2
 permit ipv6 host 2800:130:1:127::2 host
2800:130:1:177::2
control-plane
line con 0
 exec-timeout 0 0
 logging synchronous
line aux 0
line vty 0 4
 login
end
```

ANEXO 29 ARCHIVOS DE CONFIGURACIÓN DE LA RED DE CUENCA IPV6 (SIMULADO)

ARCHIVO DE CONFIGURACIÓN DE R7 CUENCA

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::114:4 link-local
 ipv6 address 2800:130:1:114::4/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 no ip address
 ipv6 address FE80::110:2 link-local
 ipv6 address 2800:130:1:110::2/64
 ipv6 enable
 ipv6 eigrp 10
 clock rate 2000000
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 7.7.7.7
 no shutdown
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
```

ARCHIVO DE CONFIGURACIÓN DE R8 CUENCA

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
class-map match-any APLICACIONES
 match access-group name cuenca
 match  precedence 3
class-map match-any VIDEO
 match access-group name cuenca
 match  precedence 4
class-map match-any VOICE
 match access-group name cuenca
 match  precedence 5
policy-map QoS_nested
 class VOICE
  priority 128
 class VIDEO
  bandwidth 640
 class APLICACIONES
  bandwidth 256
policy-map QoS_parent
 class class-default
  shape average 1024000
  service-policy QoS_nested
!
interface FastEthernet0/0
 no ip address
```

```
 duplex auto
 speed auto
 ipv6 address FE80::103:1 link-local
 ipv6 address 2800:130:1:103::1/64
 ipv6 address 2800:130:1:104::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.35
 description datos_cuenca
 bandwidth 256
 encapsulation dot1Q 35
 ipv6 address 2800:130:1:135::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.36
 description voip_cuenca
 bandwidth 128
 encapsulation dot1Q 36
 ipv6 address 2800:130:1:136::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.37
 description video_cuenca
 bandwidth 640
 encapsulation dot1Q 37
 ipv6 address 2800:130:1:137::1/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 description enlace_wan
 bandwidth 1400
 no ip address
 ipv6 address FE80::110:1 link-local
 ipv6 address 2800:130:1:110::1/64
 ipv6 address 2800:130:1:111::1/64
 ipv6 enable
 ipv6 traffic-filter cuenca out
 ipv6 eigrp 10
 clock rate 2000000
 service-policy output QoS_parent
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 8.8.8.8
 no shutdown
ipv6 access-list cuenca
 permit ipv6 host 2800:130:1:135::2 host
2800:130:1:115::2
 permit ipv6 host 2800:130:1:136::2 host
2800:130:1:116::2
 permit ipv6 host 2800:130:1:137::2 host
2800:130:1:117::2
 permit ipv6 host 2800:130:1:135::2 host
2800:130:1:125::2
 permit ipv6 host 2800:130:1:136::2 host
2800:130:1:126::2
 permit ipv6 host 2800:130:1:137::2 host
2800:130:1:127::2
 permit ipv6 host 2800:130:1:135::2 host
2800:130:1:145::2
 permit ipv6 host 2800:130:1:136::2 host
2800:130:1:146::2
 permit ipv6 host 2800:130:1:137::2 host
2800:130:1:147::2
 permit ipv6 host 2800:130:1:135::2 host
2800:130:1:155::2
 permit ipv6 host 2800:130:1:136::2 host
2800:130:1:156::2
 permit ipv6 host 2800:130:1:137::2 host
2800:130:1:157::2
 permit ipv6 host 2800:130:1:135::2 host
2800:130:1:165::2
 permit ipv6 host 2800:130:1:136::2 host
2800:130:1:166::2
 permit ipv6 host 2800:130:1:137::2 host
2800:130:1:167::2
 permit ipv6 host 2800:130:1:135::2 host
2800:130:1:175::2
 permit ipv6 host 2800:130:1:136::2 host
2800:130:1:176::2
 permit ipv6 host 2800:130:1:137::2 host
2800:130:1:177::2
 deny ipv6 any any
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
```

ANEXO 30 ARCHIVOS DE CONFIGURACIÓN DE LA RED DE LOJA IPV6 (SIMULADO)

ARCHIVO DE CONFIGURACIÓN R3 LOJA

```
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::114:1 link-local
 ipv6 address 2800:130:1:114::1/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 no ip address
 ipv6 address FE80::107:2 link-local
 ipv6 address 2800:130:1:107::2/64
 ipv6 enable
 ipv6 eigrp 10
 clock rate 2000000
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 3.3.3.3
 no shutdown
control-plane
line con 0
line aux 0
line vty 0 4
end
```

ARCHIVOS DE CONFIGURACION R4 LOJA

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
class-map match-any APLICACIONES
 match access-group name loja
 match  precedence 3
class-map match-any VIDEO
 match access-group name loja
 match  precedence 4
class-map match-any VOICE
 match access-group name loja
 match  precedence 5
policy-map QoS_nested
 class VOICE
  priority 128
 class VIDEO
  bandwidth 640
 class APLICACIONES
  bandwidth 256
policy-map QoS_parent
 class class-default
  shape average 1024000
  service-policy QoS_nested
interface FastEthernet0/0
 description enlace_wan
 no ip address
 duplex auto
 speed auto
```

```
 ipv6 address FE80::100:1 link-local
 ipv6 address 2800:130:1:100::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.45
 description datos_loja
 bandwidth 256
 encapsulation dot1Q 45
 ipv6 address 2800:130:1:145::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.46
 description voip_loja
 bandwidth 128
 encapsulation dot1Q 46
 ipv6 address 2800:130:1:146::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.47
 description video_loja
 bandwidth 640
 encapsulation dot1Q 47
 ipv6 address 2800:130:1:147::1/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 description enlace_wan
 bandwidth 1400
 no ip address
 ipv6 address FE80::107:1 link-local
 ipv6 address 2800:130:1:107::1/64
 ipv6 enable
 ipv6 traffic-filter loja out
 ipv6 eigrp 10
 clock rate 2000000
 service-policy output QoS_parent
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 4.4.4.4
 no shutdown
ipv6 access-list loja
 permit ipv6 host 2800:130:1:145::2 host
2800:130:1:115::2
 permit ipv6 host 2800:130:1:146::2 host
2800:130:1:116::2
 permit ipv6 host 2800:130:1:147::2 host
2800:130:1:117::2
 permit ipv6 host 2800:130:1:145::2 host
2800:130:1:125::2
 permit ipv6 host 2800:130:1:146::2 host
2800:130:1:126::2
 permit ipv6 host 2800:130:1:147::2 host
2800:130:1:127::2
 permit ipv6 host 2800:130:1:145::2 host
2800:130:1:135::2
 permit ipv6 host 2800:130:1:146::2 host
2800:130:1:136::2
 permit ipv6 host 2800:130:1:147::2 host
2800:130:1:137::2
 permit ipv6 host 2800:130:1:145::2 host
2800:130:1:155::2
 permit ipv6 host 2800:130:1:146::2 host
2800:130:1:156::2
 permit ipv6 host 2800:130:1:147::2 host
2800:130:1:157::2
 permit ipv6 host 2800:130:1:145::2 host
2800:130:1:165::2
 permit ipv6 host 2800:130:1:146::2 host
2800:130:1:166::2
 permit ipv6 host 2800:130:1:147::2 host
2800:130:1:167::2
 permit ipv6 host 2800:130:1:145::2 host
2800:130:1:175::2
 permit ipv6 host 2800:130:1:146::2 host
2800:130:1:176::2
 permit ipv6 host 2800:130:1:147::2 host
2800:130:1:177::2
 deny ipv6 any any
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
```

ANEXO 31 ARCHIVOS DE CONFIGURACIÓN DE LA RED DE MANTA IPV6 (SIMULADO)

ARCHIVO DE CONFIGURACIÓN R16 MANTA

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
class-map match-any APLICACIONES
 match access-group name manta
 match  precedence 3
class-map match-any VIDEO
 match access-group name manta
 match  precedence 4
class-map match-any VOICE
 match access-group name manta
 match  precedence 5
policy-map QoS_nested
 class VOICE
  priority 128
 class VIDEO
  bandwidth 320
 class APLICACIONES
  bandwidth 256
policy-map QoS_parent
 class class-default
  shape average 704000
  service-policy QoS_neste
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::105:1 link-local
 ipv6 address 2800:130:1:105::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.65
 description datos_manta
 bandwidth 256
 encapsulation dot1Q 65
 ipv6 address 2800:130:1:165::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.66
 description voip_manta
 bandwidth 128
 encapsulation dot1Q 66
 ipv6 address 2800:130:1:166::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.67
 description video_manta
 bandwidth 320
 ipv6 address 2800:130:1:167::1/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 description enalce_wan
 bandwidth 704
 no ip address
 ipv6 address FE80::112:1 link-local
 ipv6 address 2800:130:1:112::1/64
 ipv6 enable
 ipv6 traffic-filter manta out
 ipv6 eigrp 10
 clock rate 2000000
 service-policy output QoS_parent
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 16.16.16.16
 no shutdown
ipv6 access-list manta
 permit ipv6 host 2800:130:1:165::2 host
2800:130:1:115::2
 permit ipv6 host 2800:130:1:166::2 host
2800:130:1:116::2
```

```
 permit ipv6 host 2800:130:1:167::2 host
2800:130:1:117::2
 permit ipv6 host 2800:130:1:165::2 host
2800:130:1:125::2
 permit ipv6 host 2800:130:1:166::2 host
2800:130:1:126::2
 permit ipv6 host 2800:130:1:167::2 host
2800:130:1:127::2
 permit ipv6 host 2800:130:1:165::2 host
2800:130:1:135::2
 permit ipv6 host 2800:130:1:166::2 host
2800:130:1:136::2
 permit ipv6 host 2800:130:1:167::2 host
2800:130:1:137::2
 permit ipv6 host 2800:130:1:165::2 host
2800:130:1:145::2
 permit ipv6 host 2800:130:1:166::2 host
2800:130:1:146::2
 permit ipv6 host 2800:130:1:167::2 host
2800:130:1:147::2
 permit ipv6 host 2800:130:1:165::2 host
2800:130:1:155::2
 permit ipv6 host 2800:130:1:166::2 host
2800:130:1:156::2
 permit ipv6 host 2800:130:1:167::2 host
2800:130:1:157::2
 permit ipv6 host 2800:130:1:165::2 host
2800:130:1:175::2
 permit ipv6 host 2800:130:1:166::2 host
2800:130:1:176::2
 permit ipv6 host 2800:130:1:167::2 host
2800:130:1:177::2
 deny ipv6 any any
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
```

ARCHIVO DE CONFIGURACION R17 MANTA

```
12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::114:6 link-local
 ipv6 address 2800:130:1:114::6/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 no ip address
 ipv6 address FE80::112:2 link-local
 ipv6 address 2800:130:1:112::2/64
 ipv6 enable
 ipv6 eigrp 10
 clock rate 2000000
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 17.17.17.17
 no shutdown
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
```

ANEXO 32 ARCHIVOS DE CONFIGURACIÓN DE LA RED DE SANTO DOMINGO IPV6 (SIMULADO)

ARCHIVO DE CONFIGURACION R10 SANTO DOMINGO

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
class-map match-any APLICACIONES
 match access-group name santo_domingo
 match  precedence 3
class-map match-any VIDEO
 match access-group name santo_domingo
 match  precedence 4
class-map match-any VOICE
 match access-group name santo_domingo
 match  precedence 5
policy-map QoS_nested
 class VOICE
  priority 128
 class VIDEO
  bandwidth 320
 class APLICACIONES
  bandwidth 256
policy-map QoS_parent
 class class-default
  shape average 704000
  service-policy QoS_nested
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::104:1 link-local
 ipv6 address 2800:130:1:103::1/64
 ipv6 address 2800:130:1:104::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.55
 description datos_santo_domingo
 bandwidth 256
 encapsulation dot1Q 55
 ipv6 address 2800:130:1:155::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.56
 description voip_santo_domingo
 bandwidth 128
 encapsulation dot1Q 56
 ipv6 address 2800:130:1:156::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.57
 description video_santo_domingo
 bandwidth 320
 encapsulation dot1Q 57
 ipv6 address 2800:130:1:157::1/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 description enlace_wan
 bandwidth 704
 no ip address
 ipv6 address FE80::111:1 link-local
 ipv6 address 2800:130:1:110::1/64
 ipv6 address 2800:130:1:111::1/64
 ipv6 enable
 ipv6 traffic-filter santo_domingo out
 ipv6 eigrp 10
 clock rate 2000000
 service-policy output QoS_parent
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 10.10.10.10
 no shutdown
ipv6 access-list santo_domingo
```

```
 permit ipv6 host 2800:130:1:155::2 host
2800:130:1:115::2
 permit ipv6 host 2800:130:1:156::2 host
2800:130:1:116::2
 permit ipv6 host 2800:130:1:157::2 host
2800:130:1:117::2
 permit ipv6 host 2800:130:1:155::2 host
2800:130:1:125::2
 permit ipv6 host 2800:130:1:156::2 host
2800:130:1:126::2
 permit ipv6 host 2800:130:1:157::2 host
2800:130:1:127::2
 permit ipv6 host 2800:130:1:155::2 host
2800:130:1:135::2
 permit ipv6 host 2800:130:1:156::2 host
2800:130:1:136::2
 permit ipv6 host 2800:130:1:157::2 host
2800:130:1:137::2
 permit ipv6 host 2800:130:1:155::2 host
2800:130:1:145::2
 permit ipv6 host 2800:130:1:156::2 host
2800:130:1:146::2
 permit ipv6 host 2800:130:1:157::2 host
2800:130:1:147::2
 permit ipv6 host 2800:130:1:155::2 host
2800:130:1:165::2
 permit ipv6 host 2800:130:1:156::2 host
2800:130:1:166::2
 permit ipv6 host 2800:130:1:157::2 host
2800:130:1:167::2
 permit ipv6 host 2800:130:1:155::2 host
2800:130:1:175::2
 permit ipv6 host 2800:130:1:156::2 host
2800:130:1:176::2
 permit ipv6 host 2800:130:1:157::2 host
2800:130:1:177::2
 deny ipv6 any any
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
```

ARCHIVO DE CONFIGURACION R11 SANTO DOMINGO

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::114:5 link-local
 ipv6 address 2800:130:1:114::5/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 no ip address
 ipv6 address FE80::111:2 link-local
 ipv6 address 2800:130:1:111::2/64
 ipv6 enable
 ipv6 eigrp 10
 clock rate 2000000
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 11.11.11.11
 no shutdown
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
```

ANEXO 33 ARCHIVOS DE CONFIGURACIÓN DE LA RED DE SAN RAFAEL IPV6 (SIMULADO)

ARCHIVO DE CONFIGURACIÓN R14 SAN RAFAEL

```
12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
interface FastEthernet0/0
 no ip address
 duplex auto
 speed auto
 ipv6 address FE80::114:7 link-local
 ipv6 address 2800:130:1:114::7/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 no ip address
 ipv6 address FE80::113:2 link-local
 ipv6 address 2800:130:1:113::2/64
 ipv6 enable
 ipv6 eigrp 10
 clock rate 2000000
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 14.14.14.14
 no shutdown
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
```

ARCHIVO DE CONFIGURACIÓN R15 SAN RAFAEL

```
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
hostname Router
boot-start-marker
boot-end-marker
no aaa new-model
memory-size iomem 5
ip cef
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
ipv6 unicast-routing
multilink bundle-name authenticated
archive
 log config
  hidekeys
class-map match-any APLICACIONES
 match access-group name san_rafael
 match  precedence 3
class-map match-any VIDEO
 match access-group name san_rafael
 match  precedence 4
class-map match-any VOICE
 match access-group name san_rafael
 match  precedence 5
policy-map QoS_nested
 class VOICE
  priority 128
 class VIDEO
  bandwidth 320
 class APLICACIONES
  bandwidth 256
policy-map QoS_parent
 class class-default
  shape average 704000
  service-policy QoS_nested
interface FastEthernet0/0
 no ip address
 duplex auto
```

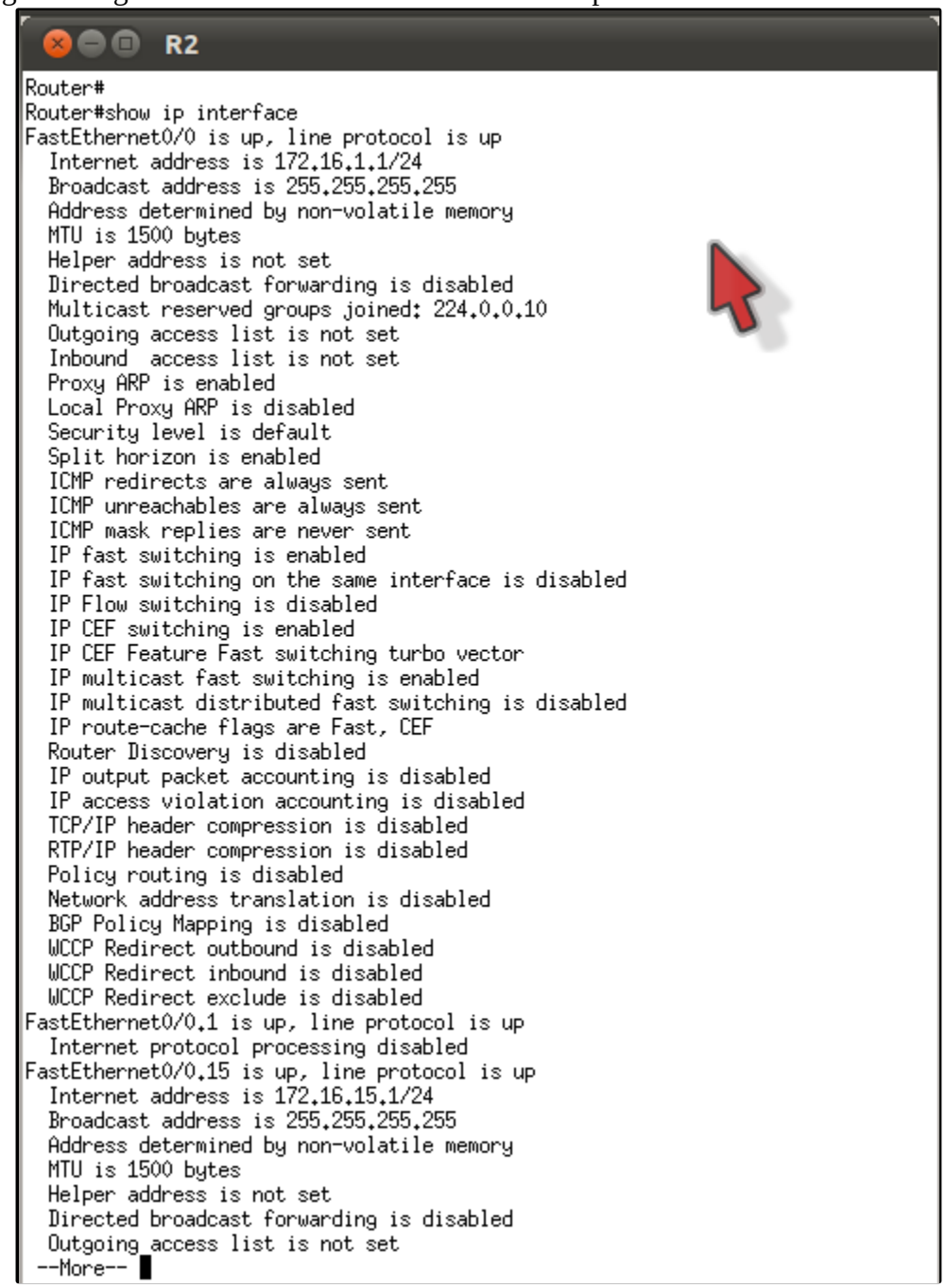
```
 speed auto
 ipv6 address FE80::106:1 link-local
 ipv6 address 2800:130:1:106::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.75
 description datos_san_rafael
 bandwidth 256
 encapsulation dot1Q 75
 ipv6 address 2800:130:1:175::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.76
 description voip_san_rafael
 bandwidth 128
 encapsulation dot1Q 76
 ipv6 address 2800:130:1:176::1/64
 ipv6 enable
 ipv6 eigrp 10
interface FastEthernet0/0.77
 description video_san_rafael
 bandwidth 320
 encapsulation dot1Q 77
 ipv6 address 2800:130:1:177::1/64
 ipv6 enable
 ipv6 eigrp 10
interface Serial0/0
 description enlac_wan
 bandwidth 704
 no ip address
 ipv6 address FE80::113:1 link-local
 ipv6 address 2800:130:1:113::1/64
 ipv6 enable
 ipv6 traffic-filter san_rafael out
 ipv6 eigrp 10
 clock rate 2000000
 service-policy output QoS_parent
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
interface Serial0/1
 no ip address
 shutdown
 clock rate 2000000
ip forward-protocol nd
ip http server
no ip http secure-server
ipv6 router eigrp 10
 router-id 15.15.15.15
 no shutdown
ipv6 access-list san_rafael
 permit ipv6 host 2800:130:1:175::2 host
2800:130:1:115::2
 permit ipv6 host 2800:130:1:176::2 host
2800:130:1:116::2
 permit ipv6 host 2800:130:1:177::2 host
2800:130:1:117::2
 permit ipv6 host 2800:130:1:175::2 host
2800:130:1:125::2
 permit ipv6 host 2800:130:1:176::2 host
2800:130:1:126::2
 permit ipv6 host 2800:130:1:177::2 host
2800:130:1:127::2
 permit ipv6 host 2800:130:1:175::2 host
2800:130:1:135::2
 permit ipv6 host 2800:130:1:176::2 host
2800:130:1:136::2
 permit ipv6 host 2800:130:1:177::2 host
2800:130:1:137::2
 permit ipv6 host 2800:130:1:175::2 host
2800:130:1:145::2
 permit ipv6 host 2800:130:1:176::2 host
2800:130:1:146::2
 permit ipv6 host 2800:130:1:177::2 host
2800:130:1:147::2
 permit ipv6 host 2800:130:1:175::2 host
2800:130:1:155::2
 permit ipv6 host 2800:130:1:176::2 host
2800:130:1:156::2
 permit ipv6 host 2800:130:1:177::2 host
2800:130:1:157::2
 permit ipv6 host 2800:130:1:175::2 host
2800:130:1:165::2
 permit ipv6 host 2800:130:1:176::2 host
2800:130:1:166::2
 permit ipv6 host 2800:130:1:177::2 host
2800:130:1:167::2
 deny ipv6 any any
control-plane
line con 0
line aux 0
line vty 0 4
 login
end
```

ANEXO 34 PRUEBAS REALIZADAS SOBRE LA SIMULACION EIGRP CON IPv4

- **PRUEBA 1**

  Configuración de las interfaces.- En esta parte se está revisando las interfaces, las rutas que tienen y cuál es la unidad máxima de transmisión.

  En la gráfica siguiente se muestra el resultado de esta prueba.



Se evidencia que se encuentran las interfaces configuradas con las rutas en IPv4 y que dentro de la interface fa0/0 están configuradas algunas sub-interfaces que se las utiliza

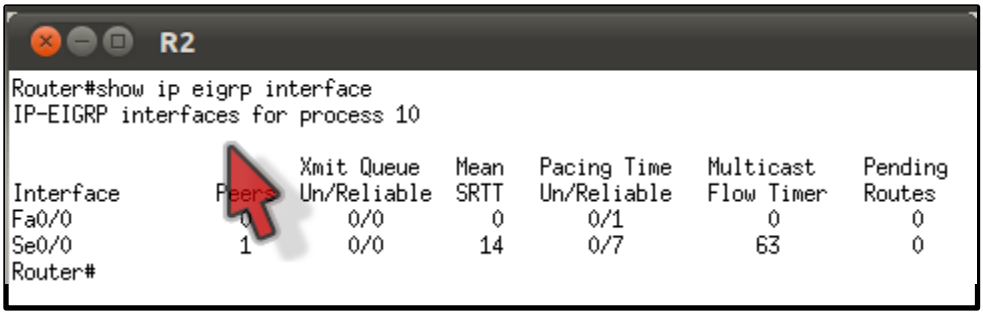
para los servicios de datos, VoIP, y video conferencia, también se puede evidenciar que la unidad de transferencia máxima por defecto es de 1500 bytes, pero esto se puede configurar manualmente

- **PRUEBA 2**

  Interfaces configuradas con EIGRP.- En esta prueba se está utilizando el comando ***show ip EIGRP interface,*** aquí se está revisando que las interfaces estén configuradas adecuadamente de acuerdo a las rutas pre-establecidas. Algunos campos que se evalúan son:

CAMPO	DESCRIPCIÓN
Interface	Interface sobre el cual se ha configurado EIGRP
Peers	Número de vecinos directamente conectados
Xmit Queue un/reliable (cola no confiable / confiable)	Paquetes poco confiables / transmisión de colas confiables
Mean SRTT	Intervalo de tiempo de ida y vuelta en milisegundos.
Pacing Time un/reliable (sincronización no confiable / confiable)	Regulación del tiempo utilizado para determinar cuando los paquetes EIGRP deben ser enviados a la interfaz.
Multicast Flow Time (temporizador de flujo multicast)	Número máximo en segundos en los que el router envíe los paquetes de multidifusión EIGRP
Pending Routes (rutas pendientes)	Número de rutas en los paquetes en la en la transmisión de espera de cola para ser enviados

En el siguiente gráfico tenemos el resultado de esa consulta en el router R2 de Quito.



El resultado nos muestra que la interface se0/0:

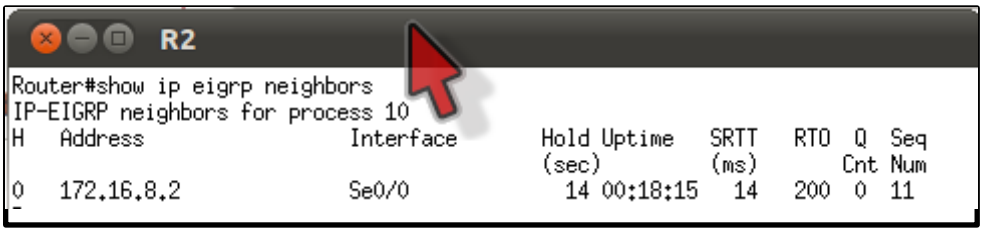
- Está configurada con EIGRP.
- Su intervalo de tiempo de ida y vuelta es de 14 milisegundos.
- Se ha determinado que los paquetes de EIGRP deben ser enviados cada 7 milisegundos.
- Los paquetes de difusión serán enviados cada 63 segundos
- No existen paquetes en espera.

- **PRUEBA 3**

  Vecinos de los routers configurado con EIGRP.- lo que vamos a evaluar en esta prueba se ve en el siguiente cuadro:

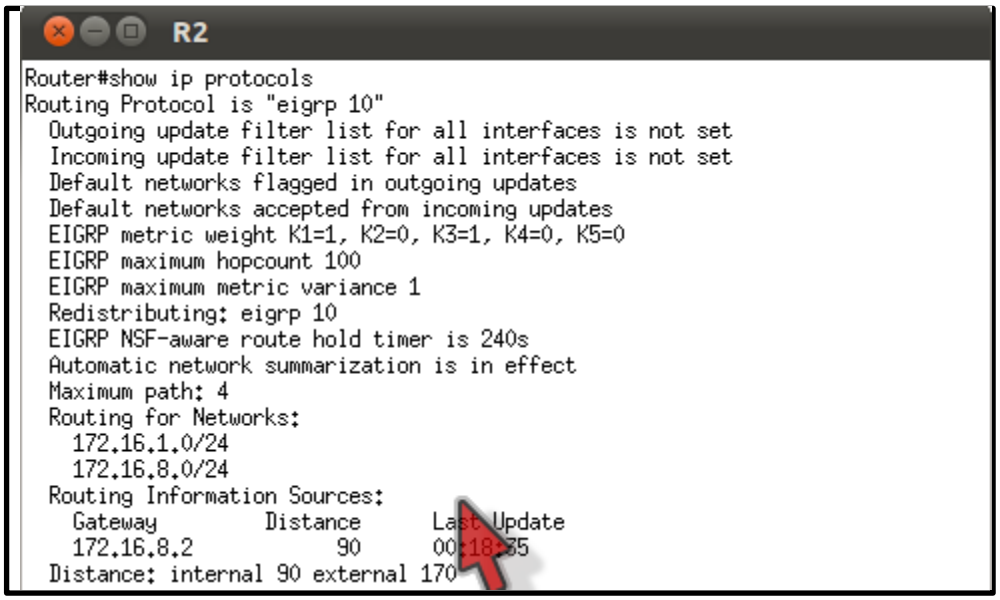
CAMPOS	DESCRIPCIÓN
ADDRESS	Dirección ip del punto EIGRP
INTERFACE	Interface en la cual recibe los paquetes de saludo.
HOLD UPTIME	Tiempo transcurrido en horas, minutos y segundos desde que el router escucha por primera vez a su vecino
SRTT	Intervalo de tiempo de ida y vuelta en milisegundos. Tiempo necesario para que un paquete viaje hasta un vecino
RTO	Tiempo de espera de retransmisión (milisegundos) tiempo que espera para enviar nuevamente otro paquete al vecino
Q count	Numero de paquetes EIGRP (actualización, consulta y respuesta) que el software está esperando para enviar.
SEQ num	Numero de orden de la última actualización, consulta o paquete de respuesta que se recibió de este vecino.

Se utiliza el comando *show ip eigrp neighbors* para obtener la descripción. En la siguiente gráfica se tiene el resultado del Router R2 de Quito.



El resultado de esta prueba es:
En el router R2 de Quito la dirección configurada con EIGRP en la interface se0/0 es 172.16.8.2, el tiempo que ha transcurrido desde que el router R2 escucho a su vecino es 00 horas, 18 minutos, 15 segundos, el tiempo que le toma a un paquete en llegar a su vecino es 14 milisegundos y para volver a enviar otro paquete tendrá que esperar 200 milisegundos.

- **PRUEBA 4**
  Protocolo en uso para el enrutamiento dinámico.- para esta prueba se utilizara el comando *show ip protocols* el cual nos muestra el siguiente resultado:



El resultado de esta prueba es:

- Se evidencio que en el router R2 de Quito si tiene configurado EIGRP con sistema autónomo 10.
- Se utiliza por defecto dos métricas que son; ancho de banda (k1) y retraso (k3).
- El máximo tiempo de mantenimiento (hopcount) es 100 milisegundos.
- El tiempo de espera para escuchar a un vecino será de 240 segundos.
- El Gateway es 172.16.8.2.
- La distancia administrativa es de 90 lo cual quiere decir que es confiable.
- La última actualización se realizó hace 18 minutos y 35 segundos.

- **PRUEBA 5**

  Traza de la ruta con EIGRP.- El objetivo es verificar el funcionamiento de los algoritmos de enrutamiento y enrutado IPv4.

  En la siguiente gráfica tenemos el resultado de *traceroute ip 172.16.2.1*. Lo que se está realizando es resolver los saltos que hace desde el router R2 Quito hasta el router R6 de Guayaquil.

  Como resultado obtenemos que el router de Quito sale por el router R1 con la dirección 172.16.8.2, luego pasa por el ISP y entra al router de Guayaquil R5 por la dirección 172.16.14.3, y luego entra al router R6 de Guayaquil por la dirección 172.16.9.1. De esta forma llega a su destino.

- **Discusión de resultados**

  En las pruebas realizadas se puede evidenciar que el algoritmo de enrutamiento EIGRP con el algoritmo enrutado IPv4 funciona exitosamente en la simulación de la red WAN de la UTPL.

La tabla de vecinos nos muestra que los paquetes que se envían a los routers vecinos tardan apenas 7 milisegundos, lo que evidencia su rapidez en envío de paquetes (PRUEBA 2).

Para el re-envío de paquetes el tiempo también es relativamente bajo, 200 milisegundos (PRUEBA 3).

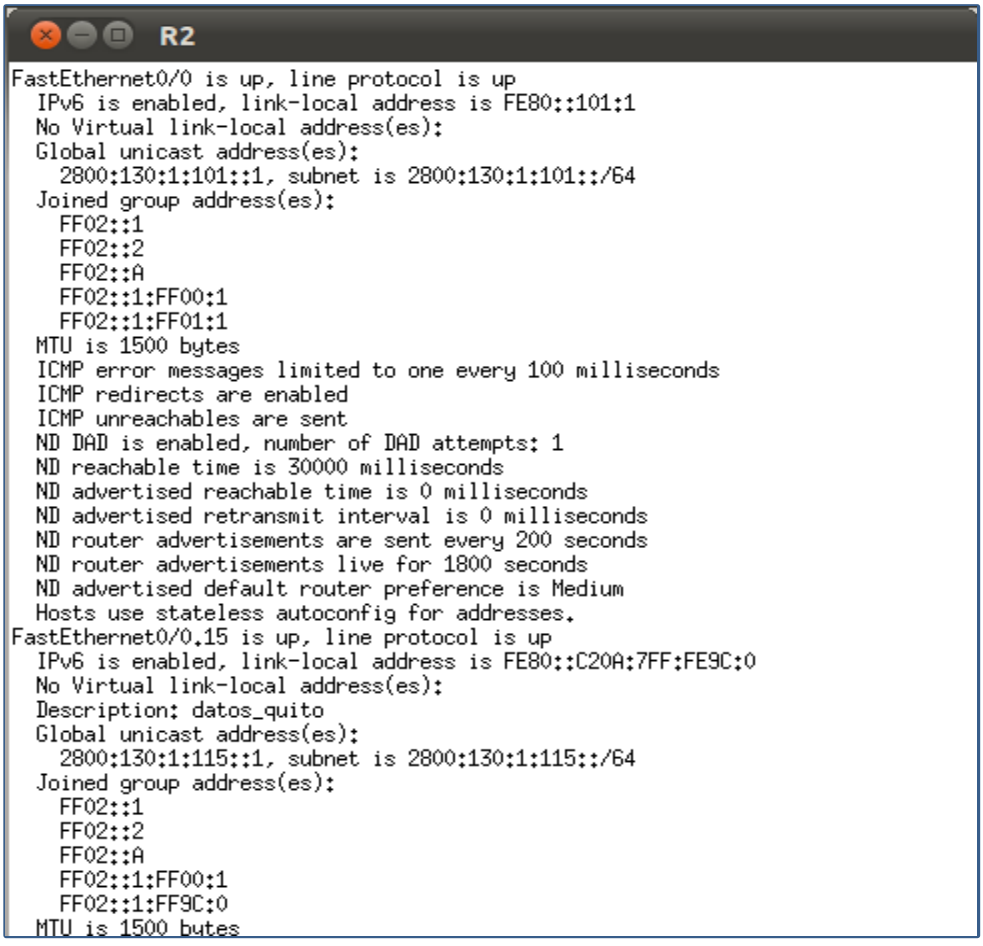
El tiempo de espera para escuchar a un vecino es de 240 segundos, pero se lo puede configurar para esperar menos tiempo. La métrica que utiliza es una combinación entre el ancho de banda y el retardo, esto evidencia que utiliza múltiples métricas para un mejor rendimiento. (PRUEBA 4)

El resultado de la PRUEBA 5 evidencia el funcionamiento del algoritmo de enrutamiento EIGRP y el algoritmo enrutado IPv4.

ANEXO 35 PRUEBAS REALIZADAS SOBRE LA SIMULACION EIGRP CON IPv6

- **PRUEBA 1**

  Configuración de las interfaces.- Para ver las interfaces que están configuradas utilizamos el comando *show ipv6 interfaces* en el cual se puede observar las configuraciones que se ha realizado a las interfaces y si existen sub-interfaces también muestra con la respectiva configuración, en nuestro caso se puede visualizar las direcciones globales únicas y las direcciones link-local configuradas en las interfaces y las interfaces globales únicas configuradas en la sub-interface, como nos podemos dar cuenta en la sub-interface fa0/0.15 no se puso una dirección link-local, sin embargo esta se puso aleatoriamente, también se puede observar que se crea un grupo de direcciones locales al sitio en cada interface. También se puede ver la unidad de transferencia máxima que es de 1500 bytes.



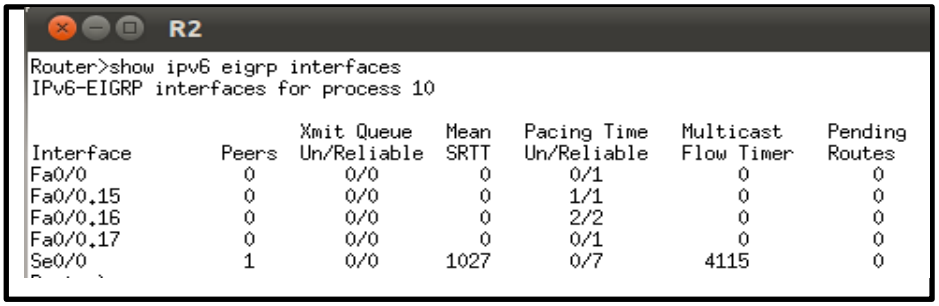
Ejecución del comando show ipv6 interfaces.

En esta prueba se evidencia que se ha configurado correctamente el direccionamiento en cada router en la simulación.

- **PRUEBA 2**

  Interfaces configuradas con EIGRP

En esta prueba se está utilizando el comando ***show ip EIGRP interface***. En la siguiente Figura se puede ver cuáles son las interfaces que están configuradas con IPv6 y EIGRP en el router R2 de Quito.



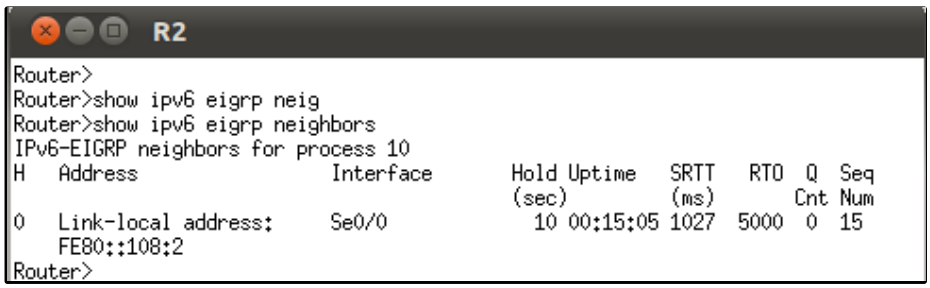
Ejecución del comando Show ipv6 eigrp interfaces

En la interface se0/0 se puede evidenciar que:

- Existe un router vecino directamente conectado.
- El intervalo de tiempo de ida y vuelta es de 1027 milisegundos
- El tiempo regulado para determinar cuando los paquetes EIGRP deben ser enviados a la interface es de 7 segundos (sincronización)
- Los paquetes multidifusión son enviados por el router cada 4115 segundos.
- En la vlan 15 y 17 se detecta que el tiempo regulado para determinar cuando los paquetes EIGRP deben ser enviados a la interface es de 1 segundo y la vlan 16 es de 2 segundos (sincronización).

- **PRUEBA 3**
  Vecinos de los routers configurados con EIGRP

Los routers que pertenecen a una misma red física se comunican por medio de un protocolo *Hello* que se lo utiliza para intercambiar paquetes de saludo, luego de esto EIGRP utiliza un protocolo de transporte fiable para garantizar la entrega correcta.



Ejecución del comando show ipv6 neighbors

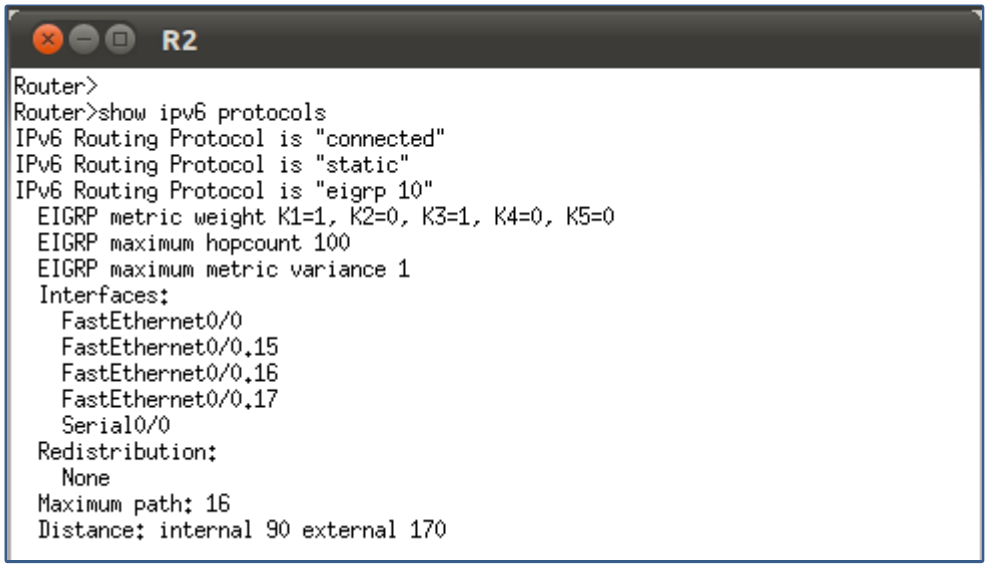
Se puede ver que la dirección link-local del router R1 de la red de Quito es la única dirección que se conecta con el router R2 de la red de Quito para transmitir paquetes a través del protocolo *Hello*. Si existiera más routers conectados en esa misma red de seguro se detectarían otros vecinos del router R2 de la red de Quito. El intervalo de

tiempo de ida y vuelta de un paquete es de 1027 milisegundos y el tiempo de espera para enviar otro paquete es de 5000 milisegundos.

- **PRUEBA 4**

Protocolo en uso para el enrutamiento dinámico.

Para ver en nuestra simulación de la red WAN MPLS si se está aplicando un algoritmo de enrutamiento Dinámico como es EIGRP se puede aplicar el siguiente comando ***show ipv6 protocols,*** aquí también se pueden ver los parámetros del protocolo de enrutamiento.



Comando show ipv6 protocols

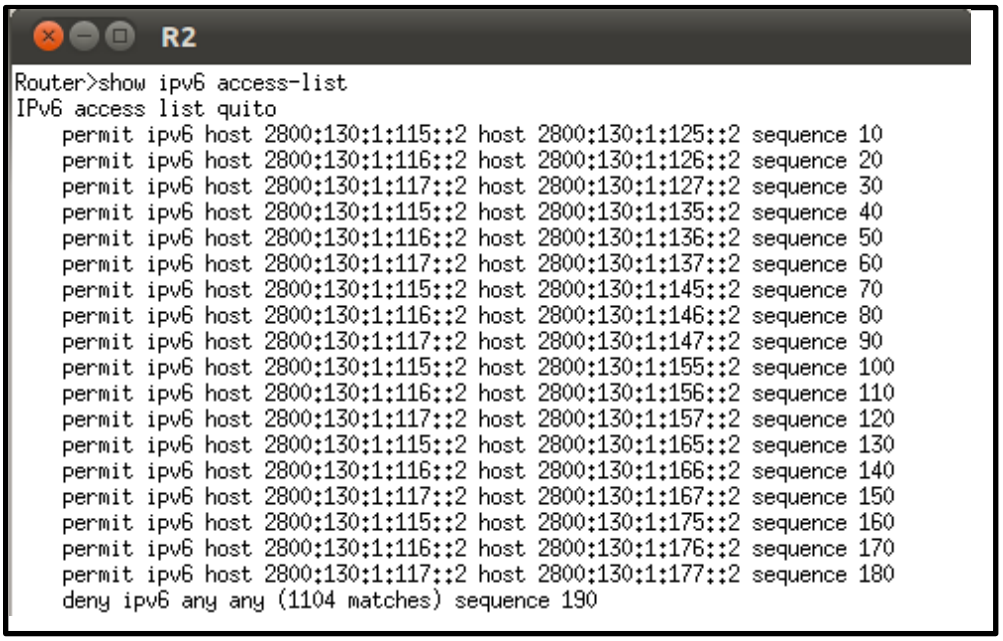
Como se ve en la gráfica se está detallando que el protocolo está conectado de forma estática y utilizando un sistema autónomo de 10, además se puede ver las métricas de eigrp (K1= ancho de banda, K2= fiabilidad, K3 retraso, K4= carga, K5= MTU) de las cuales por defecto se tiene activado k1 y k3. Otro punto importante es que muestra todas las interfaces en las cuales se ha configurado EIGRP, y se evidencia la distancia administrativa interna de 90, y externa de 170, estos valores de distancia administrativa lo que representa es la confiabilidad del protocolo de enrutamiento.

- **PRUEBA 5**

Métricas Configuradas en IPv6

Las métricas se configuraron de acuerdo a los servicios que presta la red, se tomó en cuenta que cada servicio de cada red se conecte con el mismo tipo de servicio en otra red pero no con un servicio diferente. Es por esta razón se configuró las listas de control de acceso por el momento de host a host aunque se puede incluir toda una red, esto depende del criterio del administrador de la red. Las listas de control de acceso se las utiliza

principalmente para controlar el tráfico de la red, para crear un grupo de host que se les permita la conexión con un host o una red.



Comando show ipv6 access-list

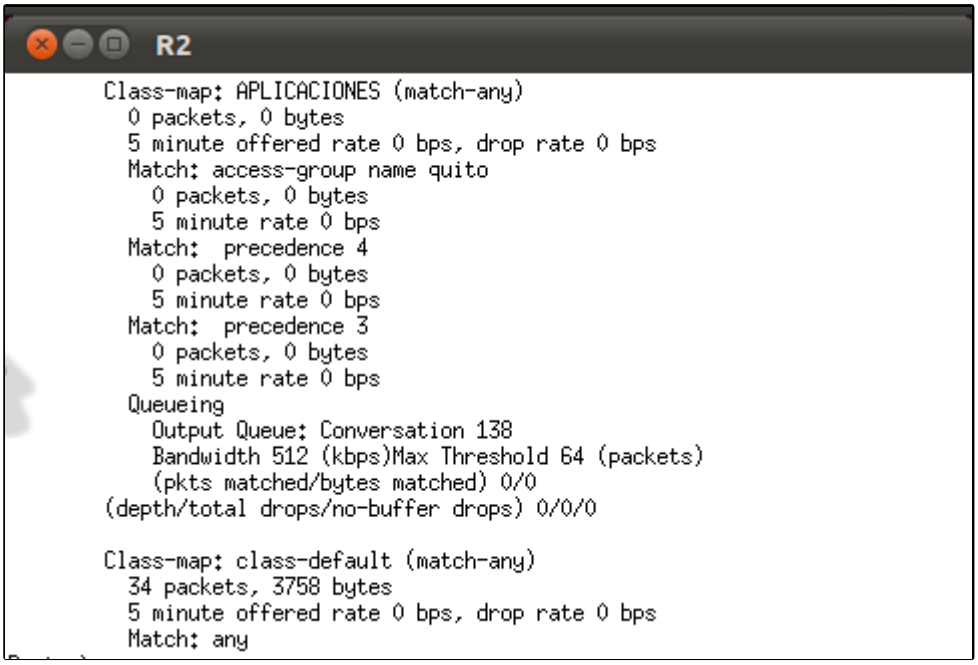
Como se ve en la imagen anterior, se estableció una configuración de las ACLs en todas las VLANs de las redes. Y esta configuración de las ACLs se encuentra en cada uno de los routers que contienen VLANs.

Para realizar esta prueba se utilizó el comando ***Show ip Access-list.***

- **PRUEBA 6**
  Políticas de mapeo de la calidad de servicio

  Las políticas de calidad de servicio se configuraron poniendo al servicio de VoIP como prioritario, esto quiere decir que si se tiene los tres servicio activos funcionando y utilizando todo el ancho de banda, el que tendrá prioridad será VoIP, también que si un servicio no está activo los otros dos servicios tienen que dividirse el ancho de banda que no se está utilizando. Esta parte no se pudo demostrar debido a que se necesita máquinas reales para hacer estas pruebas, esto se debe a que la máquina que se está utilizando solamente tiene 4 GB de memoria y utiliza un procesador Core dos Dúo y como se tiene esa limitante no se puede cargar imágenes de los sistemas operativos reales en esta simulación porque todos los veinte routers que se están simulando utilizan el 100% del procesador y aproximadamente 3,5GB de la memoria. Esto se trató de realizar pero la máquina no soporta por las limitantes antes mencionadas. De todas maneras las configuraciones se las realizaron en cada router que tiene las VLANs configuradas y encapsulados los servicios que se presta como son Datos, VoIP y Video Conferencia.

A continuación se presenta el resultado de la configuración de la calidad de servicio en donde se muestra también la precedencia que tiene cada servicio.



Resultado de las Políticas de mapeo.

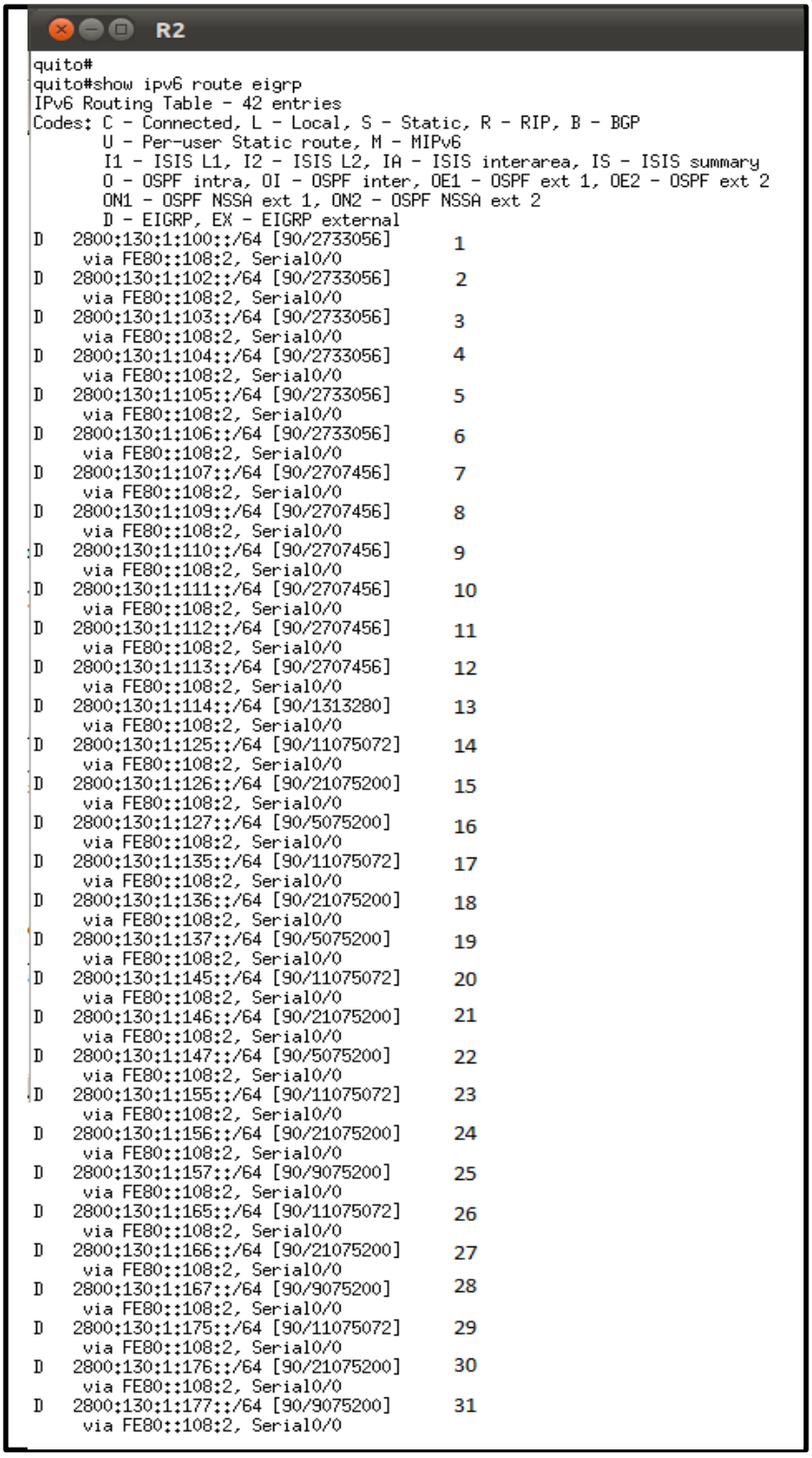
Como se ve en la Figura solo en la clase por defecto se está transmitiendo los paquetes enviados al momento de realizar los Ping.

- **PRUEBA 7**
  Reconocimiento de rutas con EIGRP.

  Para poder realizar esta prueba sobre la simulación nosotros debemos tener configurado todo el direccionamiento en IPv6 en todos los routers, las máquinas deben estar configuradas con sus respectivas direcciones IPv6, además las VLANs también deben estar configuradas para poder realizar las conexiones con otros servicios, todas las políticas deben estar correctamente configuradas para no tener problemas de conexiones futuras, también las políticas de mapeo deben estar configuradas para aprovechar el ancho de banda de los servicio prestados. Una vez configurado todo esto estaremos listos para realizar las siguientes pruebas que demuestran que el algoritmo de enrutamiento está configurado en su totalidad. Para demostrar esto aplicaremos el comando ***show ipv6 route eigrp*** sobre el router R2 de la red de Quito. Se deben detectar 34 rutas debido a que existen 7 redes, las cuales cuentan con dos routers cada una, lo que suma 14 rutas, y en cada red tenemos 3 sub-interfaces a las cuales hay que llegar también, lo cual suma 21 sub-interfaces. Esto da un total de 35 Rutas, pero se debe restar los tres servicios que están encapsulados en el router sobre el cual se realizará las pruebas y la dirección de la interfaz en donde se encuentran configuradas. Esto nos da un total de 33 redes que debe descubrir

el Router R2 de la red de Quito que es la que se está tomando como ejemplo a lo largo de todo el capítulo 6.

A continuación se muestra el resultado de las rutas aprendidas por el router R2 quito.



Comando show ipv6 route

Como se puede ver en la Figura anterior todas las rutas descubiertas tienen antepuesto una letra D, la cual significa que está utilizando el algoritmo de enrutamiento EIGRP.

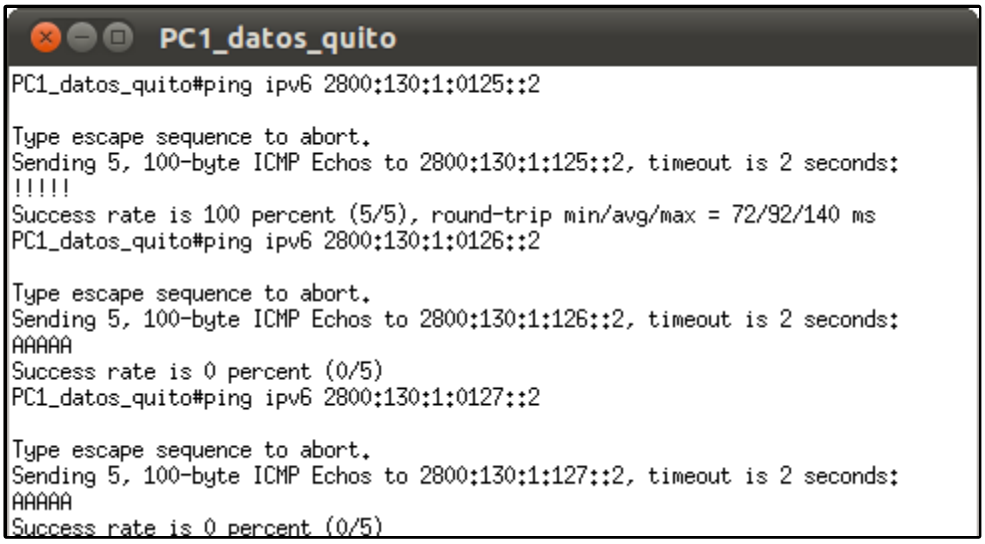
En el router R2 de Quito también se puede ver todos los saltos que se puede hacer para llegar a otro router, esto se puede realizar con el comando ***tracerouter ipv6 eigrp dirección_global.*** En nuestra simulación se ha recopilado toda la información de los saltos a todos los routers que se realiza desde el router R2 de la red de Quito a excepción de los routers PCs y de su misma red. Como resultado se obtuvo 24 rutas que se describen en la siguiente tabla. (Ver Figura 21 para una mejor comprensión de las rutas).

Rutas del router 2 de la red de Quito

#	RUTA	ROUTER	SALTO 1	ROUTER	SALTO 2	ROUTER	SALTO 3
1	R2 Quito > R6 Guayaquil	R1	2800:130:1:0108::2	R5	2800:130:1:0114::3	R6	2800:130:1:0109::1
2	R2 Quito > R6 Guayaquil	R1	2800:130:1:0108::2	R5	2800:130:1:0114::3	R6	2800:130:1:0102::1
3	R2 Quito > R10 Santo Domingo	R1	2800:130:1:0108::2	R11	2800:130:1:0114::5	R10	2800:130:1:0111::1
4	R2 Quito > R10 Santo Domingo	R1	2800:130:1:0108::2	R11	2800:130:1:0114::5	R10	2800:130:1:0104::1
5	R2 Quito > R15 San Rafael	R1	2800:130:1:0108::2	R14	2800:130:1:0114::7	R15	2800:130:1:0106::1
6	R2 Quito > R15 San Rafael	R1	2800:130:1:0108::2	R14	2800:130:1:0114::7	R15	2800:130:1:0113::1
7	R2 Quito > R4 Loja	R1	2800:130:1:0108::2	R3	2800:130:1:0114::1	R4	2800:130:1:0100::1
8	R2 Quito > R4 Loja	R1	2800:130:1:0108::2	R3	2800:130:1:0114::1	R4	2800:130:1:0107::1
9	R2 Quito > R8 Cuenca	R1	2800:130:1:0108::2	R7	2800:130:1:0114::4	R8	2800:130:1:0103::1
10	R2 Quito > R8 Cuenca	R1	2800:130:1:0108::2	R7	2800:130:1:0114::4	R8	2800:130:1:0110::1
11	R2 Quito > R16 Manta	R1	2800:130:1:0108::2	R17	2800:130:1:0114::6	R16	2800:130:1:0105:1
12	R2 Quito > R16 Manta	R1	2800:130:1:0108::2	R17	2800:130:1:0114::6	R16	2800:130:1:0112::1
13	R2 Quito >R5 Guayaquil	R1	2800:130:1:0108::2	R5	2800:130:1:0109::2		
14	R2 Quito > R5 Guayaquil	R1	2800:130:1:0108::2	R5	2800:130:1:0114::3		
15	R2 Quito > R11 Santo Domingo	R1	2800:130:1:0108::2	R11	2800:130:1:0111::2		
16	R2 Quito > R11 Santo Domingo	R1	2800:130:1:0108::2	R11	2800:130:1:0114::5		
17	R2 Quito > R14 San Rafael	R1	2800:130:1:0108::2	R14	2800:130:1:0113::2		
18	R2 Quito > R14 San Rafael	R1	2800:130:1:0108::2	R14	2800:130:1:0114::7		
19	R2 Quito > R3 Loja	R1	2800:130:1:0108::2	R3	2800:130:1:0107::2		
20	R2 Quito > R3 Loja	R1	2800:130:1:0108::2	R3	2800:130:1:0114::1		
21	R2 Quito > R7 Cuenca	R1	2800:130:1:0108::2	R7	2800:130:1:0110::2		
22	R2 Quito > R7 Cuenca	R1	2800:130:1:0108::2	R7	2800:130:1:0114::4		
23	R2 Quito > R17 Manta	R1	2800:130:1:0108::2	R17	2800:130:1:0112::2		
24	R2 Quito > R17 manta	R1	2800:130:1:0108::2	R17	2800:130:1:0114::6		

- **PRUEBA 8**
  Prueba de conexión del servicio de datos de la red de Quito.

  En esta prueba lo que se está realizando es la comprobación de la conexión de la PC1 que pertenece al servicio de datos con las máquinas de servicios de Guayaquil.

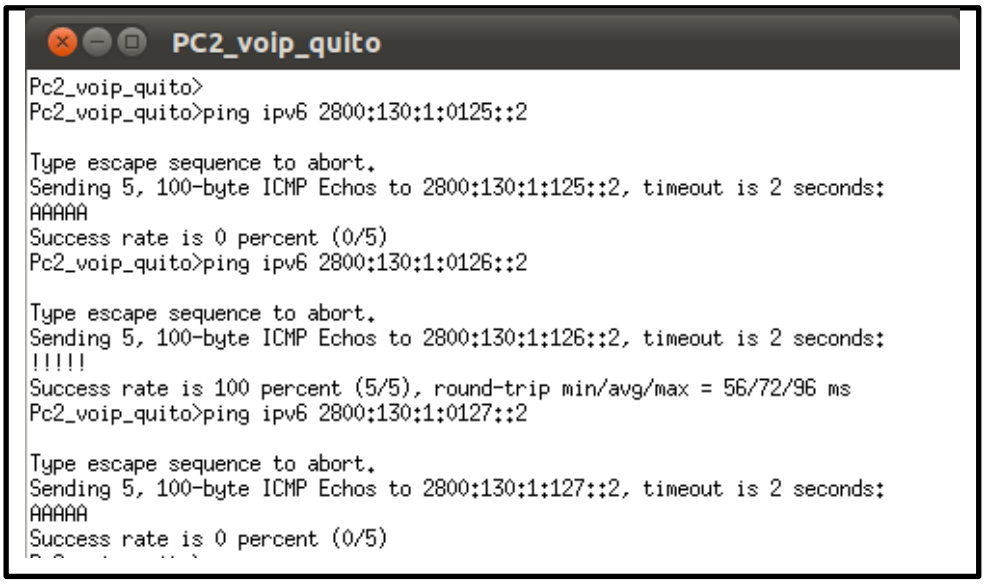


Comprobación de la conexión del servicio de datos Quito

Como resultado en la Figura anterior se puede observar que el servicio de datos de la red de Quito solamente se está conectando con el servicio de datos de la red Guayaquil, esto es gracias a las listas de control de acceso que están controlando las conexiones que se realizan con todos los servicios de las redes que representan a los centros asociados.

- **PRUEBA 9**
  Prueba de conexión del servicio de VoIP de la red de Quito

  En este servicio se está realizando la prueba de conexión del servicio de VoIP de la red de Quito con los servicios de la red de Guayaquil con el fin de observar si los permisos que se estableció en la ACLs de la red de Guayaquil y Quito están funcionando correctamente. Las configuraciones de las ACLs configuradas en estos dos routers reflejan la configuración en todas las redes, ya que si se conecta la red de los servicios de VoIP con otro centro asociado se obtendrá los mismos resultados debido a la configuración de las ACLs que están presentes en todos los Routers a excepción de los routers PCs y los que están conectados al ISP.

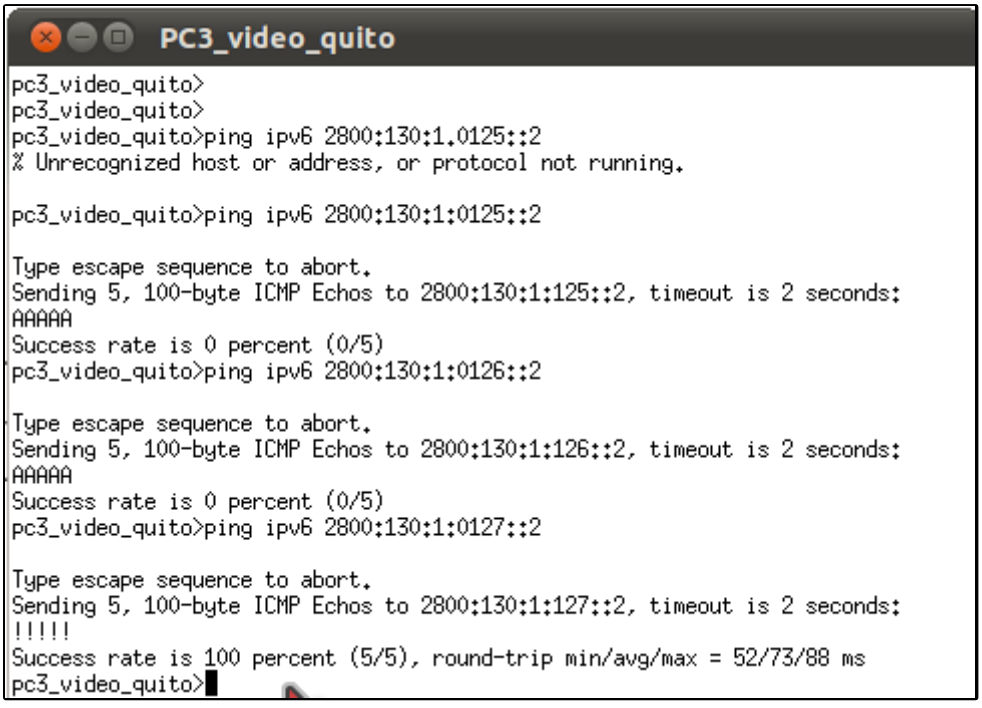


Comprobación de la conexión del servicio de VoIP Quito

Cono resultado se obtiene que el servicio de VoIP de la red de Quito solamente se conecte con el servicio de VoIP de la ciudad de Guayaquil. Si esta red de quito se quiere conectar con cualquier otra red de los centros asociados se obtendrá el mismo resultado.

- **PRUEBA 10**
  Prueba de conexión del servicio de Video de la red de Quito

  En la siguiente figura detalla las conexiones del servicio de Video.



Comprobación de la conexión del servicio de Video Quito

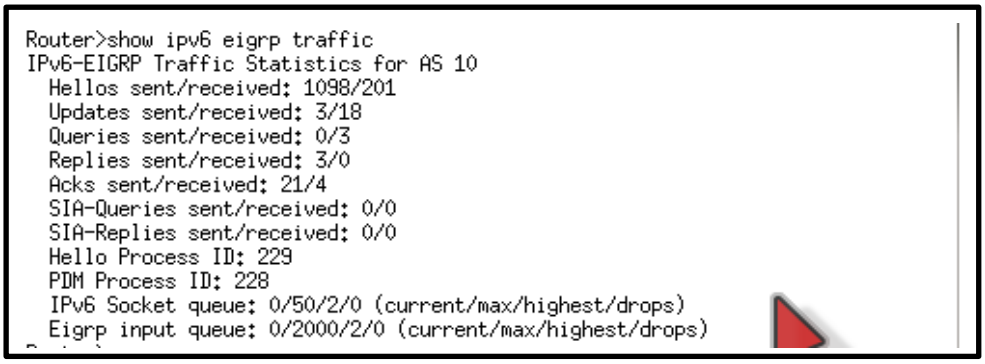
Se puede evidenciar que existe la misma tendencia que los dos otros casos anteriores, solamente los servicios que son iguales se pueden conectar, el resto está bloqueado por la lista de control de acceso.

- **PRUEBA 11**
  Tabla de topología de EIGRP

  Nos muestra cual es la dirección destino, luego cual es el salto intermedio que en este caso está identificado como sucesor, y luego cual es el salto por donde sale para realizar la conexión, también nos muestra cual es la interface por donde sale. Esta tabla nos sirve como mapa para ver cuáles son las conexiones que se puede realizar desde este router R2 de la red de Quito. Para poder visualizar en el simulador esta topología se puede utilizar el siguiente comando ***show ipv6 eigrp topology*** y los resultados se pueden ver en el anexo 26.

- **PRUEBA 12**
  Tráfico de la red

  Todo el tráfico que se realiza de un punto de la red, en este caso la red de quito que se tomó como ejemplo, se lo puede visualizar con el comando ***show ipv6 eigrp traffic,*** en el cual se pude ver la cantidad de paquetes enviado y recibidos, esto se registra gracias al protocolo Hello.



Comando show ipv6 eigrp traffic

También se puede visualizar las actualizaciones, consultas y replicas entre otros datos que son de gran importancia.

Para poder ver todos los archivos de configuración IPV6 de los routers se puede revisar DESDE EL ANEXO 27 hasta ANEXO 33.

Discusión de resultados

- En la simulación del algoritmo de enrutamiento EIGRP y enrutado ipv6 se pudo apreciar que cuando se configura las direcciones IPv6 hay que configurar dos tipos de direcciones los globales únicos y los link local para poder reconocer los vecinos. Las direcciones site-local se crean automáticamente. (Prueba 1).
- Los tiempos de intervalos son más altos que la simulación de ipv4 (Prueba 2)
- Los routers que están conectados entre sí comparten una tabla de vecinos para reconocer al dispositivo que está más próximo (Prueba 3)
- Las métricas por defecto que se está utilizando son la de ancho de banda y retardo (Prueba 4)
- Las métricas colocadas en cada dispositivo controlan que cada servicio se conecte con sus similares de host a host. (Prueba 5).
- Desde un dispositivo se puede ver todas las rutas aprendidas, esta es una característica principal del algoritmo de enrutamiento EIGRP. (Prueba 7).
- Las pruebas realizadas en el servicio de datos nos revelan que solo se puede conectar con sus similares, esto debido a las ACLs. De igual forma se puede apreciar esta distinción en las pruebas de VoIP y video conferencia.

ANEXO 36 CONFIGURACIÓN BASICA DE EIGRP

DISPOSITIVO	INTERFACE	DIRECCIÓN IP	MASCARA DE SUBRED	GATEWAY POR DEFECTO
R1	Fa 0/0	172.16.1.1	255.255.255.0	N/A
	S2/0	172.16.3.1	255.255.255.252	N/A
	S3/0	192.168.10.5	255.255.255.252	N/A
R2	Fa 0/0	172.16.2.1	255.255.255.0	N/A
	S2/0	172.16.3.2	255.255.255.252	N/A
	S3/0	192.168.10.9	255.255.255.252	N/A
R3	Fa 0/0	192.168.1.1	255.255.255.0	N/A
	S2/0	192.168.10.6	255.255.255.252	N/A
	S3/0	192.168.10.10	255.255.255.252	N/A
PC1		172.16.1.10	255.255.255.0	172.16.1.1
PC2		172.16.2.10	255.255.255.0	172.16.2.1
PC3		192.168.1.10	255.255.255.0	192.168.1.1

ANEXO 37 CONFIGURACIÓN INTERFACES SERIALES R1 (EJEMPLO)

interface Serial2/0
description serial2/0R1
bandwidth 64
ip address 172.16.3.1 255.255.255.252
interface Serial3/0
description serial3/0R1
ip address 192.168.10.5 255.255.255.252

CONFIGURACIÓN INTERFACES SERIALES R2
interface Serial2/0
description serial2/0R2
ip address 172.16.3.2 255.255.255.252
clock rate 56000
interface Serial3/0
description serial3/0R2
ip address 192.168.10.9 255.255.255.252

CONFIGURACIÓN INTERFACES SERIALES R3
interface Serial2/0
description serial2/0R3
ip address 192.168.10.6 255.255.255.252
clock rate 56000
interface Serial3/0
description serial3/0R3
ip address 192.168.10.10 255.255.255.252

ANEXO 38 CONFIGURACIÓN DE LAS INTERFACES ETHERNET EN LOS ROUTERS R1, R2, R3. (EJEMPLO)

R1
interface FastEthernet0/0
ip address 172.16.1.1 255.255.255.0
R2
interface FastEthernet0/0
ip address 172.16.2.1 255.255.255.0
R3
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0

ANEXO 39 PERMITIR EIGRP EN LOS ROUTERS (EJEMPLO)

R1
R1(config)# **router eigrp 1**
R1(config-router)#

CONFIGURACIÓN CLASSFUL NETWORK EN R1
R1 (config-router)# **network 172.16.0.0**
R1 (config-router)#

WILCARDMASK

255.255.255.255
-255.255.255.252
_____

0. 0. 0. 3

R1(config-router)# **network 192.168.10.4 0.0.0.3**
R1(config-router)#

ANEXO 40 CONFIGURACIÓN EIGRP DEL ROUTER R2 (EJEMPLO)

R2(config)# **router eigrp 1**
R2(config-router)#
Configuración classful network en R2
R2 (config-router)# **network 172.16.0.0**
R2 (config-router)#
Wildcard-mask
R2(config-router)# **network 192.168.10.8 0.0.0.3**
R2(config-router)#

CONFIGURACIÓN EIGRP DEL ROUTER R3
R3(config)# **router eigrp 1**
R3(config-router)#
Configuración classful network en R3
R3 (config-router)# **network 192.168.1.0**
R3 (config-router)#
Wildcard-mask
R3(config-router)# **network 192.168.10.4 0.0.0.3**
R3(config-router)#
R3(config-router)# **network 192.168.10.8 0.0.0.3**
R3(config-router)#end

ANEXO 41 VECINOS DE R1 (EJEMPLO)

R1#show ip eigrp neighbors

IP-EIGRP neighbors for process 1

H	Address	Interface	Hold Uptime (sec)	SRTT (ms)	RTO	Q Cnt	Seq Num
0	172.16.3.2	Se2/0	10 02:19:38	40	1000	0	9
1	192.168.10.6	Se3/0	11 02:19:38	40	1000	0	4

INFORMACIÓN DEL PROTOCOLO DE ENRUTAMIENTO EIGRP

Routing Protocol is "eigrp 1 "

Outgoing update filter list for all interfaces is not set

Incoming update filter list for all interfaces is not set

Default networks flagged in outgoing updates

Default networks accepted from incoming updates

EIGRP metric weight K1=1, K2=0, K3=1, K4=0, K5=0

EIGRP maximum hopcount 100

EIGRP maximum metric variance 1

Redistributing: eigrp 1

Automatic network summarization is in effect

Automatic address summarization:

192.168.10.0/24 for FastEthernet0/0

Summarizing with metric 20512000

Maximum path: 4

Routing for Networks:

192.168.1.0

192.168.10.4/30

192.168.10.8/30

Routing Information Sources:

Gateway Distance Last Update

192.168.10.5 90 5893

INFORMACIÓN DE LAS MÉTRICAS DE EIGRP

R3#show interface serial2/0

Serial2/0 is up, line protocol is up (connected)

Hardware is HD64570

Description: serial2/0R3

Internet address is 192.168.10.6/30

MTU 1500 bytes, BW 128 Kbit, DLY 20000 usec,

reliability 255/255, txload 1/255, rxload 1/255

Encapsulation HDLC, loopback not set, keepalive set (10 sec)

ANEXO 42 CARACTERÍSITICAS Y MEJORAS DE LOS PROTOCOLOS DE ENRUTAMIENTO [35] [36]

PROTOCOLOS DE ENRUTAMIENTO	*CARACTERISTICAS*	*MEJORAS*	*DISTANCIA ADMINISTRATIVA*
RIP	• *Calcula el camino más corto al destino con el algoritmo vector distancia* • *Se conecta por el Puerto 520 por el protocolo UDP de la capa de transporte del modelo OSI.* • *Numero de saltos 15.* • *Se actualiza cada 30seg.* • *Se desactiva cada 180seg.* • *Se elimina cada 300seg.* • *Desarrollado por CISCO*		*120*
IGRP	• *Se utiliza para redes grandes.* • *No utiliza número de saltos.* • *En la capa de transporte utiliza su propio protocolo IGRP.* • *Calcula su métrica basándose en diferentes atributos de red (retraso de red, de velocidad y capacidad, ancho de banda)* • *Funciona similar a UDP.* • *Desarrollado por CISCO.* • *Puede mantener hasta seis rutas de coste diferentes entre redes de origen y destino* • *Mejor escalabilidad* • *Métrica sofisticada* • *Soporte de múltiples rutas*	• *La métrica admite una red con un número máximo de 255 saltos de router.* • *La métrica diferencia entre diferentes tipos de medios de conexión y los costes asociados a cada uno de ellos.* • *Ofrece convergencia de funcionalidad, a medida que existen cambios en la red, informa inmediatamente* • *Métrica de 24 bit*	*100*
EIGRP	*A parte de las características de su antecesor(IGRP) tiene las siguientes:* • *Limites de saltos 224* • *Publica la información de la tabla de enrutamiento solo a routers vecinos* • *Descubre los vecinos mediante mensajes Hello* • *Utiliza su propio protocolo de enrutamiento EIGRP*	• *Soporte Para VLSM* • *Actualizaciones incrementales y parciales* • *Métrica de 32 bits.*	*90*
OSPF	• *Respuesta rápida y sin bucles ante cambios* • *Seguridad ante los cambios* • *Soporte de múltiples métricas* • *Balanceo de carga en múltiples caminos* • *Escalabilidad en el crecimiento de rutas externas*		*110*

IS-IS	• *Enrutamiento jerárquico* • *Comportamiento sin clases* • *Inundación rápida de nueva información* • *Convergencia rápida* • *Muy escalable* • *Sintonizador de tiempo flexible*		*115*
BGP(EXTERNO)			*20*

ANEXO 43 PROPUESTA PARA LA SIMULACION DE LAS VLANS EN IPV6

CIUDAD	SERVICIOS	INTERFACE	VLAN	DIRECION DE VLAN
QUITO	DATOS	Fa0/0.15	15	2800:130:1:0115::2/64
	VoIP	Fa0/0.16	16	2800:130:1:0116::2/64
	VIDEO	Fa0/0.17	17	2800:130:1:0117::2/64
GUAYAQUIL	DATOS	Fa0/0.25	25	2800:130:1:0125::2/64
	VoIP	Fa0/0.26	26	2800:130:1:0126::2/64
	VIDEO	Fa0/0.27	27	2800:130:1:0127::2/64
CUENCA	DATOS	Fa0/0.1	35	2800:130:1:0135::2/64
	VoIP	Fa0/0.2	36	2800:130:1:0136::2/64
	VIDEO	Fa0/0.3	37	2800:130:1:0137::2/64
LOJA	DATOS	Fa0/0.1	45	2800:130:1:0145::2/64
	VoIP	Fa0/0.2	46	2800:130:1:0146::2/64
	VIDEO	Fa0/0.3	47	2800:130:1:0147::2/64
MANTA	DATOS	Fa0/0.1	65	2800:130:1:0165::2/64
	VoIP	Fa0/0.2	66	2800:130:1:0166::2/64
	VIDEO	Fa0/0.3	67	2800:130:1:0167::2/64
SANTO DOMINGO	DATOS	Fa0/0.1	55	2800:130:1:0155::2/64
	VoIP	Fa0/0.2	56	2800:130:1:0156::2/64
	VIDEO	Fa0/0.3	57	2800:130:1:0157::2/64
SAN RAFAEL	DATOS	Fa0/0.1	75	2800:130:1:0175::2/64
	VoIP	Fa0/0.2	76	2800:130:1:0176::2/64
	VIDEO	Fa0/0.3	77	2800:130:1:0177::2/64

ANEXO 44 CONFIGURACIÓN DEL DIRECCIONAMIENTO (SIMULADOR)

Configuración router R1 Quito

Router# (config) interface fa0/0
Router#(config-if)ipv6 address fe80::0114:2 link-local
Router#(config-if)ipv6 address 2800:130:1:0114::2
Router#(config)interface se0/0
Router#(config-if)ipv6 address fe80::0108:2 link-local
Router#(config-if)ipv6 address 2800:130:1:0108::2

Configuración router R2 Quito

router#(config)interface fa0/0
router#(config-if)ipv6 address fe80::0101:1 link-local
router#(config-if)ipv6 address 2800:130:1:0101::1
router#(config)interface se0/0
router#(config-if)ipv6 address fe80::0108:1 link-local
Router#(config-if)ipv6 address 2800:130:1:0108::1

Configuración router R5 Guayaquil

Router #(config)interface fa0/0
Router #(config-if)ipv6 address fe80::0114:3 link-local
Router #(config-if)ipv6 address 2800:130:1:0114::3
Router #(config)interface se0/0
Router #(config-if)ipv6 address fe80::0109:2 link-local
Router #(config-if)ipv6 address 2800:130:1:0102::2

Configuración router R6 Guayaquil

Router #(config)interface fa0/0
Router #(config-if)ipv6 address fe80::0102:1 link-local
Quito#(config-if)ipv6 address 2800:130:1:0102::1
Router #(config)interface se0/0
Quito#(config-if)ipv6 address fe80::0109:1 link-local
Router #(config-if)ipv6 address 2800:130:1:0109::1

Configuración router R7 Cuenca

Router #(config)interface fa0/0
Router #(config-if)ipv6 address fe80::0114:4 link-local
Router #(config-if)ipv6 address 2800:130:1:0114::4
Router #(config)interface se0/0
Router #(config-if)ipv6 address fe80::0110:2 link-local
Router #(config-if)ipv6 address 2800:130:1:0110::2

Configuración router R8 Cuenca

Router #(config)interface fa0/0
Router #(config-if)ipv6 address fe80::0103:1 link-local
Quito#(config-if)ipv6 address 2800:130:1:0103::1
Router #(config)interface se0/0
Quito#(config-if)ipv6 address fe80::0110:1 link-local
Router #(config-if)ipv6 address 2800:130:1:0110::1

Configuración router R3 Loja

Router #(config)interface fa0/0
Router #(config-if)ipv6 address fe80::0114:1 link-local
Router #(config-if)ipv6 address 2800:130:1:0114::1
Router #(config)interface se0/0
Router #(config-if)ipv6 address fe80::0107:2 link-local
Router #(config-if)ipv6 address 2800:130:1:0107::2

Configuración router R4 Loja

Router #(config)interface fa0/0
Router #(config-if)ipv6 address fe80::0100:1 link-local
Quito#(config-if)ipv6 address 2800:130:1:0100::1
Router #(config)interface se0/0
Quito#(config-if)ipv6 address fe80::0107:1 link-local
Router #(config-if)ipv6 address 2800:130:1:0107::1

Configuración router R16 Manta

Router #(config)interface fa0/0
Router #(config-if)ipv6 address fe80::0105:1 link-local
Router #(config-if)ipv6 address 2800:130:1:0105::1
Router #(config)interface se0/0
Router #(config-if)ipv6 address fe80::0112:1 link-local
Router #(config-if)ipv6 address 2800:130:1:0112::1

Configuración router R17 Manta

Router #(config)interface fa0/0
Router #(config-if)ipv6 address fe80::0114:6 link-local

Quito#(config-if)ipv6 address 2800:130:1:0114::6
Router #(config)interface se0/0
Quito#(config-if)ipv6 address fe80::0112:2 link-local
Router #(config-if)ipv6 address 2800:130:1:0112::2

Configuración router R10 Santo Domingo

Router #(config)interface fa0/0
Router #(config-if)ipv6 address fe80::0104:1 link-local
Router #(config-if)ipv6 address 2800:130:1:0104::1
Router #(config)interface se0/0
Router #(config-if)ipv6 address fe80::0111:1 link-local
Router #(config-if)ipv6 address 2800:130:1:0111::1

Configuración router R11 Santo Domingo

Router #(config)interface fa0/0
Router #(config-if)ipv6 address fe80::0114:5 link-local
Quito#(config-if)ipv6 address 2800:130:1:0114::5
Router #(config)interface se0/0
Quito#(config-if)ipv6 address fe80::0111:2 link-local
Router #(config-if)ipv6 address 2800:130:1:0111::2

Configuración router R14 San Rafael

Router #(config)interface fa0/0
Router #(config-if)ipv6 address fe80::0114:7 link-local
Router #(config-if)ipv6 address 2800:130:1:0114::7
Router #(config)interface se0/0
Router #(config-if)ipv6 address fe80::0113:2 link-local
Router #(config-if)ipv6 address 2800:130:1:0113::2

Configuración router R15 San Rafael

Router #(config)interface fa0/0
Router #(config-if)ipv6 address fe80::0106:1 link-local
Quito#(config-if)ipv6 address 2800:130:1:0106::1
Router #(config)interface se0/0
Quito#(config-if)ipv6 address fe80::0113:1 link-local
Router #(config-if)ipv6 address 2800:130:1:0113::1

ANEXO 45 ACTIVACIÓN DE EIGRP EN RED WAN MPLS

(SIMULADOR)

CONFIGURACIÓN QUITO ROUTER R1

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 1.1.1.1
        no shutdown
        end
```

CONFIGURACIÓN QUITO ROUTER R2

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 2.2.2.2
        no shutdown
        end
```

CONFIGURACIÓN GUAYAQUIL ROUTER R5

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 5.5.5.5
        no shutdown
        end
```

CONFIGURACIÓN GUAYAQUIL ROUTER R6

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 6.6.6.6
        no shutdown
        end
```

CONFIGURACIÓN CUENCA ROUTER R7

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 7.7.7.7
        no shutdown
        end
```

CONFIGURACIÓN CUENCA ROUTER R8

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 8.8.8.8
        no shutdown
        end
```

CONFIGURACIÓN LOJA ROUTER R3

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 3.3.3.3
        no shutdown
        end
```

CONFIGURACIÓN LOJA ROUTER R4

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 4.4.4.4
        no shutdown
        end
```

CONFIGURACIÓN MANTA ROUTER R16

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 16.16.16.16
        no shutdown
        end
```

CONFIGURACIÓN MANTA ROUTER R17

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 17.17.17.17
        no shutdown
        end
```

CONFIGURACIÓN SANTO DOMINGO ROUTER R10

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 10.10.10.10
        no shutdown
        end
```

CONFIGURACIÓN SANTO DOMINGO ROUTER R11

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 11.11.11.11
        no shutdown
        end
```

CONFIGURACIÓN SAN RAFAEL ROUTER R14

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 14.14.14.14
        no shutdown
        end
```

CONFIGURACIÓN CUENCA ROUTER R15

```
enable
        conf ter
        ipv6 unicast-routing
        interface se0/0
        ipv6 enable
        ipv6 eigrp 10
        ipv6 router eigrp 10
        router-id 15.15.15.15
        no shutdown
        end
```

ANEXO 46 CONFIGURACIÓN DE VLANS (SIMULADOR)

ROUTER DE QUITO R2
interface fa0/0
interface fa0/0.15
description datos_quito
encapsulation dot1Q 15
ipv6 address 2800:130:1:0115::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 2.2.2.2
no shutdown
interface fa0/0.16
description voip_quito
encapsulation dot1Q 16
ipv6 address 2800:130:1:116::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 2.2.2.2
no shutdown
interface fa0/0.17
description video_quito
encapsulation dot1Q 17
ipv6 address 2800:130:1:117::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 2.2.2.2
no shutdown

ROUTER DE GUAYAQUIL R6
interface fa0/0
interface fa0/0.25
description datos_guayaquil
encapsulation dot1Q 25
ipv6 address 2800:130:1:0125::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 6.6.6.6
no shutdown
interface fa0/0.26
description voip_guayaquil
encapsulation dot1Q 26
ipv6 address 2800:130:1:126::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 6.6.6.6
no shutdown
interface fa0/0.27
description video_guayaquil
encapsulation dot1Q 27
ipv6 address 2800:130:1:127::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 6.6.6.6
no shutdown

ROUTER DE CUENCA R8
interface fa0/0
interface fa0/0.35
description datos_cuenca
encapsulation dot1Q 35
ipv6 address 2800:130:1:0135::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 8.8.8.8
no shutdown
interface fa0/0.36
description voip_cuenca
encapsulation dot1Q 36
ipv6 address 2800:130:1:136::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 8.8.8.8
no shutdown
interface fa0/0.37
description video_cuenca
encapsulation dot1Q 37
ipv6 address 2800:130:1:137::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 8.8.8.8
no shutdown

ROUTER DE LOJA R4
interface fa0/0
interface fa0/0.45
description datos_loja
encapsulation dot1Q 45
ipv6 address 2800:130:1:0145::1/64
ipv6 enable
IPV6 eigrp 10

ipv6 router eigrp 10
route-id 4.4.4.4
no shutdown
interface fa0/0.46
description voip_loja
encapsulation dot1Q 46
ipv6 address 2800:130:1:146::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 4.4.4.4
no shutdown
interface fa0/0.47
description video_loja
encapsulation dot1Q 47
ipv6 address 2800:130:1:147::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 4.4.4.4
no shutdown

ROUTER DE SANTO DOMINGO R10

interface fa0/0
interface fa0/0.55
description datos_santo_domingo
encapsulation dot1Q 55
ipv6 address 2800:130:1:0155::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 10.10.10.10
no shutdown
interface fa0/0.56
description voip_santo domingo
encapsulation dot1Q 56
ipv6 address 2800:130:1:156::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 10.10.10.10
no shutdown
interface fa0/0.57
description video_santo_domingo
encapsulation dot1Q 57
ipv6 address 2800:130:1:157::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 10.10.10.10
no shutdown

ROUTER DE MANTA R16

interface fa0/0
interface fa0/0.65
description datos_manta
encapsulation dot1Q 65
ipv6 address 2800:130:1:0165::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 16.16.16.16
no shutdown
interface fa0/0.66
description voip_manta
encapsulation dot1Q 66
ipv6 address 2800:130:1:166::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 16.16.16.16
no shutdown
interface fa0/0.67
description video_manta
encapsulation dot1Q 67
ipv6 address 2800:130:1:167::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 16.16.16.16
no shutdown

ROUTER DE SAN RAFAEL R15

interface fa0/0
interface fa0/0.75
description datos_san_rafael
encapsulation dot1Q 75
ipv6 address 2800:130:1:0175::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 15.15.15.15
no shutdown
interface fa0/0.76
description voip_san_rafael
encapsulation dot1Q 76
ipv6 address 2800:130:1:176::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 15.15.15.15
no shutdown
interface fa0/0.77
description video_san_rafael
encapsulation dot1Q 77
ipv6 address 2800:130:1:177::1/64
ipv6 enable
IPV6 eigrp 10
ipv6 router eigrp 10
route-id 15.15.15.15
no shutdown

ANEXO 47 CONFIGURACIÓN DE ACLs (SIMULADOR)

LISTA DE CONTROL DE ACESO DE GUAYAQUIL
ROUTER R6

```
enable
conf ter
ipv6 access-list guayaquil
//conexión a Quito
permit host 2800:130:1:0125::2 host
2800:130:1:0115::2
permit host 2800:130:1:0126::2 host
2800:130:1:0116::2
permit host 2800:130:1:0127::2 host
2800:130:1:0117::2
//conexión a Cuenca
permit host 2800:130:1:0125::2 host
2800:130:1:0135::2
permit host 2800:130:1:0126::2 host
2800:130:1:0136::2
permit host 2800:130:1:0127::2 host
2800:130:1:0137::2
//conexión a Loja
permit host 2800:130:1:0125::2 host
2800:130:1:0145::2
permit host 2800:130:1:0126::2 host
2800:130:1:0146::2
permit host 2800:130:1:0127::2 host
2800:130:1:0147::2
//conexión a Santo Domingo
permit host 2800:130:1:0125::2 host
2800:130:1:0155::2
permit host 2800:130:1:0126::2 host
2800:130:1:0156::2
permit host 2800:130:1:0127::2 host
2800:130:1:0157::2
//conexión a Manta
permit host 2800:130:1:0125::2 host
2800:130:1:0165::2
permit host 2800:130:1:0126::2 host
2800:130:1:0166::2
permit host 2800:130:1:0127::2 host
2800:130:1:0167::2
//conexión a San Rafael
permit host 2800:130:1:0125::2 host
2800:130:1:0175::2
permit host 2800:130:1:0126::2 host
2800:130:1:0176::2
permit host 2800:130:1:0127::2 host
2800:130:1:0177::2
deny any any
interface se0/0
ipv6 traffic filter guayaquil out
```

LISTA DE CONTROL DE ACESO DE QUITO
ROUTER R2

```
ipv6 access-list quito
//conexión a Guayaquil
permit host 2800:130:1:0115::2 host
2800:130:1:0125::2
permit host 2800:130:1:0116::2 host
2800:130:1:0126::2
permit host 2800:130:1:0117::2 host
2800:130:1:0127::2
//conexión a Cuenca
permit host 2800:130:1:0115::2 host
2800:130:1:0135::2
permit host 2800:130:1:0116::2 host
2800:130:1:0136::2
permit host 2800:130:1:0117::2 host
2800:130:1:0137::2
//conexión a Loja
permit host 2800:130:1:0115::2 host
2800:130:1:0145::2
permit host 2800:130:1:0116::2 host
2800:130:1:0146::2
permit host 2800:130:1:0117::2 host
2800:130:1:0147::2
//conexión a Santo Domingo
permit host 2800:130:1:0115::2 host
2800:130:1:0155::2
permit host 2800:130:1:0116::2 host
2800:130:1:0156::2
permit host 2800:130:1:0117::2 host
2800:130:1:0157::2
//conexión a Manta
permit host 2800:130:1:0115::2 host
2800:130:1:0165::2
permit host 2800:130:1:0116::2 host
2800:130:1:0166::2
permit host 2800:130:1:0117::2 host
2800:130:1:0167::2
//conexión a San Rafael
permit host 2800:130:1:0115::2 host
2800:130:1:0175::2
permit host 2800:130:1:0116::2 host
2800:130:1:0176::2
permit host 2800:130:1:0117::2 host
2800:130:1:0177::2
deny any any
interface se0/0
ipv6 traffic filter quito out
```

LISTA DE CONTROL DE ACESO DE CUENCA
ROUTER R8

```
ipv6 access-list cuenca
```

//conexión a Quito
permit host 2800:130:1:0135::2 host 2800:130:1:0115::2
permit host 2800:130:1:0136::2 host 2800:130:1:0116::2
permit host 2800:130:1:0137::2 host 2800:130:1:0117::2
//conexión a Guayaquil
permit host 2800:130:1:0135::2 host 2800:130:1:0125::2
permit host 2800:130:1:0136::2 host 2800:130:1:0126::2
permit host 2800:130:1:0137::2 host 2800:130:1:0127::2
//conexión a Loja
permit host 2800:130:1:0135::2 host 2800:130:1:0145::2
permit host 2800:130:1:0136::2 host 2800:130:1:0146::2
permit host 2800:130:1:0137::2 host 2800:130:1:0147::2
//conexión a Santo Domingo
permit host 2800:130:1:0135::2 host 2800:130:1:0155::2
permit host 2800:130:1:0136::2 host 2800:130:1:0156::2
permit host 2800:130:1:0137::2 host 2800:130:1:0157::2
//conexión a Manta
permit host 2800:130:1:0135::2 host 2800:130:1:0165::2
permit host 2800:130:1:0136::2 host 2800:130:1:0166::2
permit host 2800:130:1:0137::2 host 2800:130:1:0167::2
//conexión a San Rafael
permit host 2800:130:1:0135::2 host 2800:130:1:0175::2
permit host 2800:130:1:0136::2 host 2800:130:1:0176::2
permit host 2800:130:1:0137::2 host 2800:130:1:0177::2
deny any any
interface se0/0
ipv6 traffic filter cuenca out

LISTA DE CONTROL DE ACESO DE LOJA
ROUTER R4

ipv6 access-list loja
//conexión a Quito
permit host 2800:130:1:0145::2 host 2800:130:1:0115::2
permit host 2800:130:1:0146::2 host 2800:130:1:0116::2
permit host 2800:130:1:0147::2 host 2800:130:1:0117::2
//conexión a Guayaquil
permit host 2800:130:1:0145::2 host 2800:130:1:0125::2
permit host 2800:130:1:0146::2 host 2800:130:1:0126::2
permit host 2800:130:1:0147::2 host 2800:130:1:0127::2
//conexión a Cuenca
permit host 2800:130:1:0145::2 host 2800:130:1:0135::2
permit host 2800:130:1:0146::2 host 2800:130:1:0136::2
permit host 2800:130:1:0147::2 host 2800:130:1:0137::2
//conexión a Santo Domingo
permit host 2800:130:1:0145::2 host 2800:130:1:0155::2
permit host 2800:130:1:0146::2 host 2800:130:1:0156::2
permit host 2800:130:1:0147::2 host 2800:130:1:0157::2
//conexión a Manta
permit host 2800:130:1:0145::2 host 2800:130:1:0165::2
permit host 2800:130:1:0146::2 host 2800:130:1:0166::2
permit host 2800:130:1:0147::2 host 2800:130:1:0167::2
//conexión a San Rafael
permit host 2800:130:1:0145::2 host 2800:130:1:0175::2
permit host 2800:130:1:0146::2 host 2800:130:1:0176::2
permit host 2800:130:1:0147::2 host 2800:130:1:0177::2
deny any any
interface se0/0
ipv6 traffic filter loja out

LISTA DE CONTROL DE ACCESO DE SANTO DOMINGO
ROUTER R10

ipv6 access-list santo_domingo
//conexión a Quito
permit host 2800:130:1:0155::2 host 2800:130:1:0115::2
permit host 2800:130:1:0156::2 host 2800:130:1:0116::2
permit host 2800:130:1:0157::2 host 2800:130:1:0117::2
//conexión a Guayaquil
permit host 2800:130:1:0155::2 host 2800:130:1:0125::2

permit host 2800:130:1:0156::2 host 2800:130:1:0126::2
permit host 2800:130:1:0157::2 host 2800:130:1:0127::2
//conexión a Cuenca
permit host 2800:130:1:0155::2 host 2800:130:1:0135::2
permit host 2800:130:1:0156::2 host 2800:130:1:0136::2
permit host 2800:130:1:0157::2 host 2800:130:1:0137::2
//conexión a Loja
permit host 2800:130:1:0155::2 host 2800:130:1:0145::2
permit host 2800:130:1:0156::2 host 2800:130:1:0146::2
permit host 2800:130:1:0157::2 host 2800:130:1:0147::2
//conexión a Manta
permit host 2800:130:1:0155::2 host 2800:130:1:0165::2
permit host 2800:130:1:0156::2 host 2800:130:1:0166::2
permit host 2800:130:1:0157::2 host 2800:130:1:0167::2
//conexión a San Rafael
permit host 2800:130:1:0155::2 host 2800:130:1:0175::2
permit host 2800:130:1:0156::2 host 2800:130:1:0176::2
permit host 2800:130:1:0157::2 host 2800:130:1:0177::2
deny any any
interface se0/0
ipv6 traffic filter santo_domingo out

LISTA DE CONTROL DE ACCESO DE MANTA ROUTER R8

ipv6 access-list manta
//conexión a Quito
permit host 2800:130:1:0165::2 host 2800:130:1:0115::2
permit host 2800:130:1:0166::2 host 2800:130:1:0116::2
permit host 2800:130:1:0167::2 host 2800:130:1:0117::2
//conexión a Guayaquil
permit host 2800:130:1:0165::2 host 2800:130:1:0125::2
permit host 2800:130:1:0166::2 host 2800:130:1:0126::2
permit host 2800:130:1:0167::2 host 2800:130:1:0127::2
//conexión a Cuenca
permit host 2800:130:1:0165::2 host 2800:130:1:0135::2
permit host 2800:130:1:0166::2 host 2800:130:1:0136::2
permit host 2800:130:1:0167::2 host 2800:130:1:0137::2
//conexión a Loja
permit host 2800:130:1:0165::2 host 2800:130:1:0145::2
permit host 2800:130:1:0166::2 host 2800:130:1:0146::2
permit host 2800:130:1:0167::2 host 2800:130:1:0147::2
//conexión a Santo Domingo
permit host 2800:130:1:0165::2 host 2800:130:1:0155::2
permit host 2800:130:1:0166::2 host 2800:130:1:0156::2
permit host 2800:130:1:0167::2 host 2800:130:1:0157::2
//conexión a San Rafael
permit host 2800:130:1:0165::2 host 2800:130:1:0175::2
permit host 2800:130:1:0166::2 host 2800:130:1:0176::2
permit host 2800:130:1:0167::2 host 2800:130:1:0177::2
deny any any
interface se0/0
ipv6 traffic filter manta out

LISTA DE CONTROL DE ACCESO DE SAN RAFAEL ROUTER R15

ipv6 access-list san_rafael
//conexión a Quito
permit host 2800:130:1:0175::2 host 2800:130:1:0115::2
permit host 2800:130:1:0176::2 host 2800:130:1:0116::2
permit host 2800:130:1:0177::2 host 2800:130:1:0117::2
//conexión a Guayaquil
permit host 2800:130:1:0175::2 host 2800:130:1:0125::2
permit host 2800:130:1:0176::2 host 2800:130:1:0126::2
permit host 2800:130:1:0177::2 host 2800:130:1:0127::2
//conexión a Cuenca
permit host 2800:130:1:0175::2 host 2800:130:1:0135::2
permit host 2800:130:1:0176::2 host 2800:130:1:0136::2
permit host 2800:130:1:0177::2 host 2800:130:1:0137::2

```
//conexión a Loja
permit host 2800:130:1:0175::2 host
2800:130:1:0145::2
permit host 2800:130:1:0176::2 host
2800:130:1:0146::2
permit host 2800:130:1:0177::2 host
2800:130:1:0147::2
//conexión a Santo Domingo
permit host 2800:130:1:0175::2 host
2800:130:1:0155::2
permit host 2800:130:1:0176::2 host
2800:130:1:0156::2
permit host 2800:130:1:0177::2 host
2800:130:1:0157::2
//conexión a Manta
permit host 2800:130:1:0175::2 host
2800:130:1:0165::2
permit host 2800:130:1:0176::2 host
2800:130:1:0166::2
permit host 2800:130:1:0177::2 host
2800:130:1:0167::2
deny any any
interface se0/0
ipv6 traffic filter san_rafael out
```

ANEXO 48 CONFIGURACIÓN DE CALIDAD DE SERVICO (QoS)(SIMULADOR)

ROUTER R2 QUITO

```
conf ter
class-map match-any APLICACIONES
match access-group name quito
match precedence 3
EXIT
class-map match-any VIDEO
match access-group name quito
match precedence 4
EXIT
class-map match-any VOICE
match access-group name quito
match precedence 5
exit
conf ter
policy-map QoS_nested
class VOICE
priority 384
class VIDEO
bandwidth 1500
class APLICACIONES
bandwidth 512
exit
exit
policy-map QoS_parent
class class-default
shape average 2400000
service-policy QoS_nested
interface se0/0
description enlace_wan
service-policy output QoS_parent
bandwidth 3300
end
```

ROUTER R6 GUAYAQUIL

```
conf ter
class-map match-any APLICACIONES
match access-group name guayaquil
match precedence 3
EXIT
class-map match-any VIDEO
match access-group name guayaquil
match precedence 4
EXIT
class-map match-any VOICE
match access-group name guayaquil
match precedence 5
exit
conf ter
policy-map QoS_nested
class VOICE
priority 128
class VIDEO
bandwidth 640
class APLICACIONES
bandwidth 256
exit
exit
policy-map QoS_parent
class class-default
shape average 1024000
service-policy QoS_nested
exit
exit
interface se0/0
description enlace_wan
service-policy output QoS_parent
bandwidth 1000
end
```

ROUTER R8 CUENCA

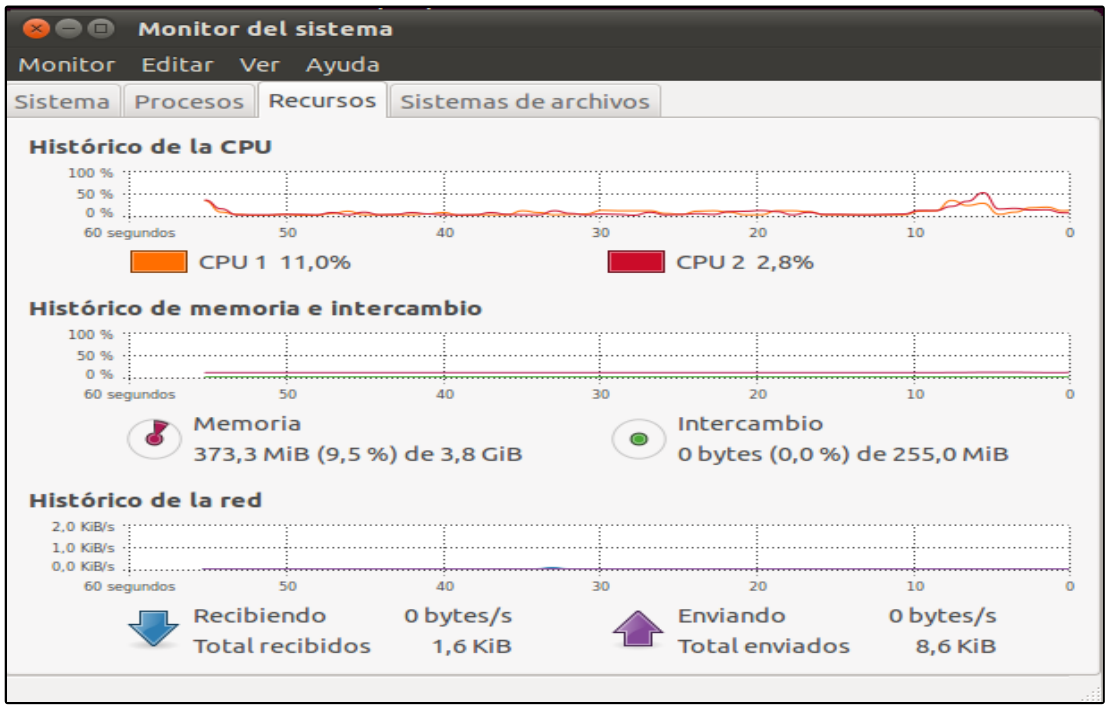
```
conf ter
class-map match-any APLICACIONES
match access-group name cuenca
match precedence 3
EXIT
class-map match-any VIDEO
match access-group name cuenca
match precedence 4
EXIT
class-map match-any VOICE
match access-group name cuenca
match precedence 5
exit
conf ter
policy-map QoS_nested
class VOICE
priority 128
class VIDEO
bandwidth 640
class APLICACIONES
bandwidth 256
exit
exit
policy-map QoS_parent
class class-default
shape average 1024000
service-policy QoS_nested
exit
exit
interface se0/0
description enlace_wan
service-policy output QoS_parent
bandwidth 1400
```

end
ROUTER R4 LOJA
conf ter
class-map match-any APLICACIONES
match access-group name loja
match precedence 3
EXIT
class-map match-any VIDEO
match access-group name loja
match precedence 4
EXIT
class-map match-any VOICE
match access-group name loja
match precedence 5
exit
conf ter
policy-map QoS_nested
class VOICE
priority 128
class VIDEO
bandwidth 640
class APLICACIONES
bandwidth 256
exit
exit
policy-map QoS_parent
class class-default
shape average 1024000
service-policy QoS_nested
exit
exit
interface se0/0
description enlace_wan
service-policy output QoS_parent
bandwidth 1400
end
ROUTER R16 MANTA
conf ter
class-map match-any APLICACIONES
match access-group name manta
match precedence 3
EXIT
class-map match-any VIDEO
match access-group name manta
match precedence 4
EXIT
class-map match-any VOICE
match access-group name manta
match precedence 5
exit
conf ter
policy-map QoS_nested
class VOICE
priority 128
class VIDEO
bandwidth 320
class APLICACIONES
bandwidth 256
exit
exit
policy-map QoS_parent
class class-default
shape average 704000
service-policy QoS_nested
exit
exit
interface se0/0
description enlace_wan
service-policy output QoS_parent
bandwidth 704
end
ROUTER R10 SANTO DOMINGO
conf ter
class-map match-any APLICACIONES
match access-group name santo_domingo
match precedence 3
EXIT
class-map match-any VIDEO
match access-group name santo_domingo
match precedence 4
EXIT
class-map match-any VOICE
match access-group name santo_domingo
match precedence 5
exit
conf ter
policy-map QoS_nested
class VOICE
priority 128
class VIDEO
bandwidth 320
class APLICACIONES
bandwidth 256
exit
exit
policy-map QoS_parent
class class-default
shape average 704000
service-policy QoS_nested
exit
exit
interface se0/0
description enlace_wan
service-policy output QoS_parent
bandwidth 704
end
ROUTER R15 SAN RAFAEL
conf ter

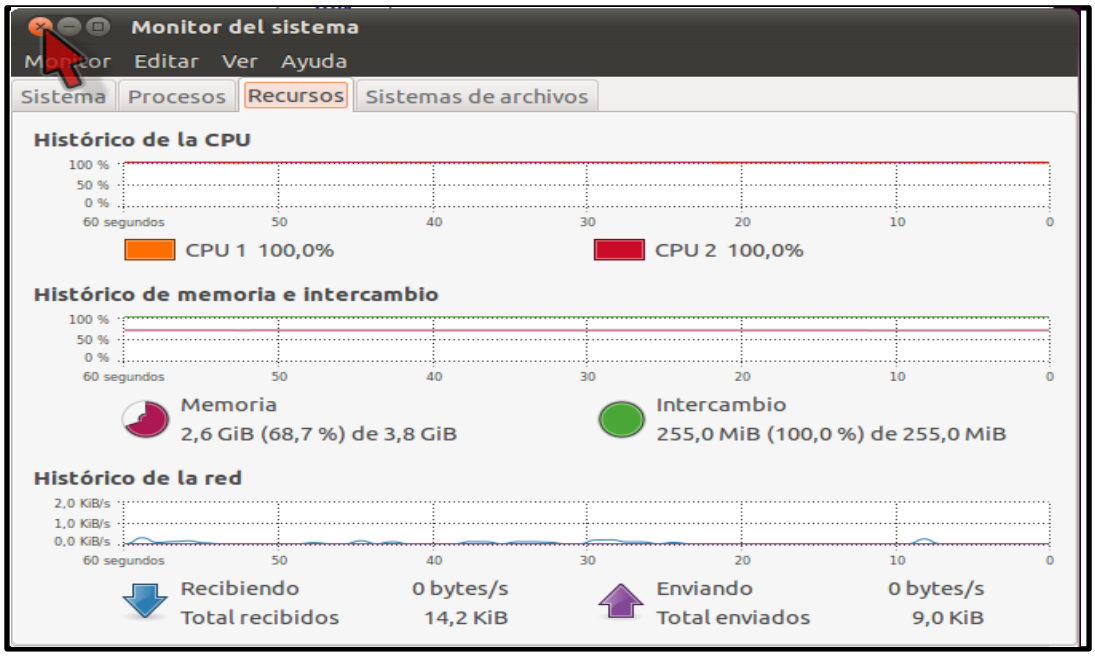
```
class-map match-any APLICACIONES
match access-group name san_rafael
match precedence 3
EXIT
class-map match-any VIDEO
match access-group name san_rafael
match precedence 4
EXIT
class-map match-any VOICE
match access-group name san_rafael
match precedence 5
exit
conf ter
policy-map QoS_nested
class VOICE
priority 128
class VIDEO
bandwidth 320
class APLICACIONES
bandwidth 256
exit
exit
policy-map QoS_parent
class class-default
shape average 704000
service-policy QoS_nested
exit
exit
interface se0/0
description enlace_wan
service-policy output QoS_parent
bandwidth 704
        end
```

ANEXO 49 CÁLCULO DE VALORES APROXIMADOS EN MILISEGUNDOS

Como se está trabajando con un simulador, se debe tomar en cuenta que el equipo anfitrión simula 18 dispositivos de los 35 debido a que utiliza el 100% de su capacidad, esto se puede ver en la gráfica siguiente.

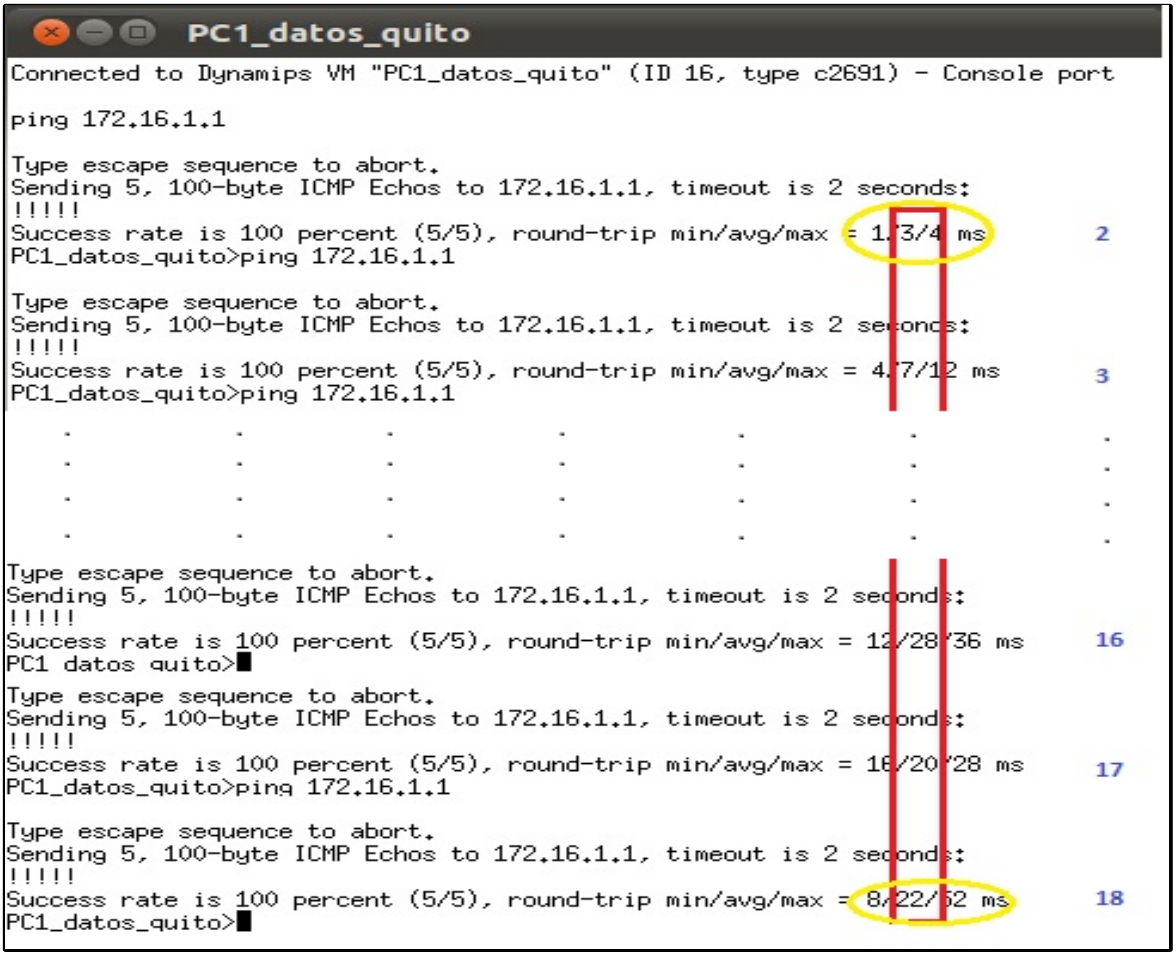


Gráfica. Antes de utilizar el simulador



Gráfica. Después de utilizar el simulador con 18 dispositivos activos

Cuando se activan dos routers en el simulador y se realiza un ping entre estos, el resultado es de 3 milisegundos, como se ve en la siguiente gráfica en el círculo amarillo, pero cuando se va activando en el simulador más routers el valor va aumentando, esto representa una alteración en los datos, este valor se lo puede tomar como un margen de error en cada salto en milisegundos. Para realizar este cálculo del tiempo en milisegundos que se tarda en cada salto, se activaran 18 dispositivos y el resultado final se tomara como un margen de error en cada salto.



Gráfica. Margen de error en milisegundos

Como se puede ver en la gráfica después de activar los 18 dispositivos se tiene un margen de error de 22 milisegundos por cada salto.

Desde la máquina del centro asociado Quito, hasta llegar a cualquier otro centro asociado, realiza cinco saltos tomando en cuenta el computador al que llega. Esto quiere decir que existe un margen de error de 100 a 110 milisegundos que se deben restar cuando se realice un ping desde el computador del centro asociado Quito a cualquier otro centro asociado en la simulación. El valor que se restará será de 105 milisegundos como margen de error.

ANEXO 50 VALORES SIMULADOS Y APROXIMADOS

Datos del simulador del servicio de Datos IPv4

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.25.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/123/140 ms
PC1_datos_quito>ping 172.16.35.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.35.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/123/144 ms
PC1_datos_quito>ping 172.16.55.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.55.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/130/180 ms
PC1_datos_quito>ping 172.16.65.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.65.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/128/148 ms
PC1_datos_quito>ping 172.16.75.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.75.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/146/196 ms
PC1_datos_quito>
```

Datos del simulador del servicio de Datos IPv6

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:125::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/128/152 ms
PC1_datos_quito>ping 2800:130:1:0135::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:135::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/128/176 ms
PC1_datos_quito>ping 2800:130:1:0155::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:155::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 144/197/348 ms
PC1_datos_quito>ping 2800:130:1:0165::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:165::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 124/148/192 ms
PC1_datos_quito>ping 2800:130:1:0175::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:175::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/120/200 ms
PC1_datos_quito>
```

Datos aproximados del servicio de datos IPv6

Simulado ipv6 (ms)	Aproximado ipv6 (ms)
96/128/152	23
84/128/176	23
144/197/348	92
124/148/192	43
84/120/200	15

Datos aproximados del servicio de datos IPv4

Simulado ipv4 (ms)	Aproximado ipv4 (ms)
96/123/140	18
100/123/144	18
100/130/180	25
116/128/148	23
100/146/196	41

Datos del simulador del servicio de Voip IPv4

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.26.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/116/128 ms
Pc2_voip_quito>ping 172.16.36.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.36.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/124/144 ms
Pc2_voip_quito>ping 172.16.56.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.56.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 88/112/128 ms
Pc2_voip_quito>ping 172.16.66.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.66.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/120/136 ms
Pc2_voip_quito>ping 172.16.76.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.76.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 76/108/148 ms
Pc2_voip_quito>
```

Datos del simulador del servicio de Voip IPv6

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:126::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/115/144 ms
Pc2_voip_quito>ping 2800:130:1:0136::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:136::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 108/133/192 ms
Pc2_voip_quito>ping 2800:130:1:0156::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:156::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/139/172 ms
Pc2_voip_quito>ping 2800:130:1:0166::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:166::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/140/156 ms
Pc2_voip_quito>ping 2800:130:1:0176::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:176::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/121/160 ms
```

Datos aproximados del servicio de VOIP IPv6

Simulado ipv6 (ms)	Aproximado ipv6 (ms)
96/115/144	10
108/133/192	28
96/139/172	34
120/140/156	35
84/121/160	16

Datos aproximados del servicio de VOIP IPv4

Simulado ipv6 (ms)	Aproximado ipv6 (ms)
80/116/128	116 - 105 = 11
72/124/144	124 - 105 = 19
88/112/128	112 - 105 = 7
104/120/136	120 - 105 = 15
76/108/148	108 - 105 = 3

Datos del simulador del servicio de Video IPv4

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.27.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 72/138/184 ms
pc3_video_quito>ping 172.16.37.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.37.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/126/152 ms
pc3_video_quito>ping 172.16.57.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.57.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/113/132 ms
pc3_video_quito>ping 172.16.67.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.67.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/119/148 ms
pc3_video_quito>ping 172.16.77.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.77.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 104/152/176 ms
pc3_video_quito>
```

Datos del simulador del servicio de Video IPv6

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:127::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/121/152 ms
pc3_video_quito>ping 2800:130:1:0137::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:137::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/142/172 ms
pc3_video_quito>ping 2800:130:1:0157::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:157::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/112/144 ms
pc3_video_quito>ping 2800:130:1:0167::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:167::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 100/131/188 ms
pc3_video_quito>ping 2800:130:1:0177::2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 2800:130:1:177::2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/132/160 ms
```

Datos aproximados del servicio de video IPv6

Simulado ipv6 (ms)	Aproximado ipv6 (ms)
80/121/152	16
100/142/172	37
100/112/144	7
100/131/188	26
84/132/160	27

Datos aproximados del servicio de video IPv4

Simulado ipv6 (ms)	Aproximado ipv6 (ms)
72/138/184	33
116/126/152	21
96/113/132	27
96/119/148	14
104/152/176	47

PAPER

SIMULACIÓN DE ALGORITMOS DE ENRUTAMIENTO DINÁMICO SOBRE LA RED WAN MPLS DE LA UTPL

Ing. Carlos Córdova
cgcordova@utpl.edu.ec

Ing. Byron Jaramillo
bgjaramillo@utpl.edu.ec

Gonzalo Piedra

gppiedrax@utpl.edu.ec

Resumen: El proyecto contempla el estudio de los protocolos de enrutamiento y enrutados y su simulación en el modelo de la red WAN de la UTPL, evaluar sus características y beneficios principales para la red WAN de la UTPL y evaluar los resultados de la simulación.

Palabras claves: Algoritmos de enrutamiento, enrutados, GNS3, MPLS, EIGRP.

1. **Introducción:** La red WAN de la UTPL cuenta con tecnología MPLS[25] la cual no se está aprovechando al máximo, esta tecnología permite implementar algoritmos de enrutamiento dinámico y enrutados con el fin de mejorar la escalabilidad, confiabilidad y rapidez de la comunicación entre las redes de los centros asociados que cuentan con esta tecnología.

2. **Algoritmo de Enrutamiento**
   En la actualidad existen varios algoritmos de enrutamiento dinámico con diferentes versiones, entre los más importantes tenemos RIP, IGRP, EIGRP [1], OSPF [2], IS-IS entre otros, los cuales se diferencian por sus características, como son confiabilidad, compatibilidad y uso adecuado en la red. Estos algoritmos representan una gran ayuda porque permiten descubrir las redes de forma dinámica, ahorrándonos el trabajo de cambiar la configuración de toda la red cada vez que se realiza la integración de un nuevo dispositivo.
   Estos algoritmos se los utiliza de acuerdo a los requerimientos que se tiene en la red que se está manejando. Los administradores deben realizar un estudio de cómo está compuesta la red y cuáles son los requerimientos necesarios.
   Los protocolos de enrutamiento sirven para intercambiar las tablas de enrutamiento y compartir la información. Permiten enrutar los protocolos enrutados como pueden ser protocolos IP, IPX[26], Apple Talk.
   Los protocolos de enrutamiento se clasifican en IGP[27] y EGP[28]. Los protocolos IGP se clasifican a su vez en protocolos de Vector Distancia y protocolos de Estado de Enlace. Los protocolos de Vector Distancia, son los que determinan la dirección y la distancia hacia cualquier enlace en la internetwork, se clasifican en RIP, IGRP y EIGRP. Los protocolos de estado de enlace fueron diseñados para superar las limitaciones de los protocolos Vector Distancia, se clasifican en: OSPF e IS-IS. Por otra parte el EGP se clasifica en BGP[29].

3. **Características de algoritmos de enrutamiento**
   Todos los algoritmos de enrutamiento que se ha mencionado tienen características específicas que los hacen aptos para las redes, ya sean LAN o WAN. Aquellas redes

[25] Multiprotocol Label Switching

[26] Internet Packet Exchange
[27] Interior Gateway Protocol
[28] Exterior Gateway Protocol
[29] Border Gateway Protocol

que se consideran pequeñas no tiene más de 15 saltos para llegar a su destino, su distancia administrativa entre más baja sea significa que más confiable es.

Estas características sirven para identificar cual es el algoritmo de enrutamiento óptimo a utilizar en una red dependiendo de sus requerimientos y los dispositivos que se estén utilizando. Cabe destacar que existen más características que se pueden identificar como son: la actualización, desactivación y tiempo de borrado de un paquete. En la siguiente tabla se muestra algunas características que se deben tomar en cuenta para escoger un algoritmo de enrutamiento apto para la red WAN de la UTPL.

Tabla1. Características principales de protocolos de enrutamiento

PROTOCOLOS DE ENRUTAMIENTO			
Protocolos	**# Saltos**	**Distancia Administrativa**	**Propietario**
RIP	15	120	Universal
IGRP	255	100	Cisco
EIGRP	224	90	Cisco
OSPF	Sin limite	110	Universal
IS-IS	Sin limite	115	Universal

4. Algoritmos Enrutados

Son un conjunto de protocolos que ofrecen información para que un router envíe los paquetes al dispositivo correspondiente hasta llegar a su destino. Estos protocolos asignan a cada dispositivo un número de red y de host y en algunos casos sólo en número de red.

Los protocolos de enrutamiento más conocidos son: Protocolos IP, IPX, DEC net, Apple Talk, Banyan VINES y XNS[30]. De estos los que pueden ejecutar en MPLS son IP, IPX y Apple Talk. [3][4][5]. En la UTPL el algoritmo enrutado que se está utilizando es el IP en su versión 4 y 6, pero hasta el momento aplicados de forma estática.

[30] Xerox Network Systems

5. Características de algoritmos enrutados

El algoritmo enrutado que es aconsejable utilizar en la red WAN de la UTPL es el algoritmo IP, porque es el más extendido y actualmente utiliza la Universidad.

Tabla2. Características principales de protocolos enrutados IP

CARACTERÍSTICAS DE PROTOCOLO ENRUTADO IP		
Características	**IPv4**	**IPv6**
Tamaño de dirección	2^{32}	2^{128}
Formatos de direcciones	decimal	Hexadecimal
Simplifica encabezado	X	✓
Seguridad	X	Ipsec.
Autoconfiguración	X	✓
Creado para	conexión	Conexión y movilidad

El algoritmo enrutado que tiene mayores beneficios es IPv6, por sus características principales: Seguridad y tamaño de direcciones.

6. Criterios de selección del protocolo de enrutamiento

Para escoger el algoritmo de enrutamiento adecuado para la red WAN de la UTPL, analizaremos algunos criterios de selección.

Tabla 3. Resumen de criterios de selección del algoritmo de enrutamiento

CRITERIOS	**PROTOCOLOS DE ENRUTAMIENTO**	
	OSPF	**EIGRP**
Topología de red		✓
Resumen de rutas y dirección	✓	✓
Velocidad de convergencia	✓	✓
Selección de rutas	✓	✓
Capacidad de ampliación		✓
Sencillez de simulación		✓
Seguridad	✓	✓
Compatibilidad	✓	✓

De acuerdo a los criterios de selección el algoritmo de enrutamiento más apto para la red WAN de la UTPL es el algoritmo EIGRP, porque se adapta a cualquier topología de red, y tiene capacidad de ampliación, mientras el algoritmo de enrutamiento OSPF necesita una red jerárquica para poder utilizarlo, no tiene

capacidad de ampliación y es más tediosa su configuración.

7. Factibilidad y simulación de algoritmo de enrutamiento EIGRP

Factibilidad de EIGRP

Este protocolo de enrutamiento cumple con los requerimientos de la red WAN de la UTPL, por ser el más confiable de todos los algoritmos que se ha estudiado, no consume ancho de banda ni recursos exagerados, utiliza VLSM para no desperdiciar las direcciones IP, es compatible con los dispositivos CISCO que se utiliza en la red WAN de la UTPL y soporta redes grandes con más de 15 saltos.

Simulación de EIGRP

Este algoritmo de enrutamiento se puede simular porque es compatible con los dispositivos CISCO que utiliza en la red WAN de la UTPL, es compatible con algunos IOS[31] que se utiliza en los dispositivos ya que soportan EIGRP e IP, y se adapta a los cambios de topología de la red, las actualizaciones las realiza solamente cuando ocurre un cambio en la topología o en los routers vecinos con lo que ahorra tiempo y esfuerzo.

Problemas de EIGRP

- No todos los IOS de los dispositivos CISCO son compatibles con este algoritmo de enrutamiento, por lo que hay que actualizar los dispositivos si es necesario.
- Si un dispositivo de la red WAN de la UTPL no es CISCO el protocolo de enrutamiento no es apto para la simulación e implementación.

Antes de entrar a la simulación es necesario ver unos conceptos básicos de direccionamiento IPv6.

[31] Internetwork Operating System

Tabla de direccionamiento en IPv6.

En la UTPL se tiene siete centros asociados con la tecnología MPLS. En la actualidad, la red IPv6 asignada por LACNIC para la UTPL es la 2800: 130::/32 y de acuerdo a este rango de redes se debe simular el resto de la red en los centros asociados.

Se ha tomado la red 2800:130:1::/32 que está asignada a la UTPL, esta red hay que transformarla a un /56 para poder obtener 256 subredes que servirán en el direccionamiento de la red. Es importante recordar que los primeros 64 bits están asignados a la red, y estos se subdividen en 48 bits de red y 16 bits de subred, los siguientes 64 bits están asignados a hosts.

Aclarado este punto se procede a obtener la nueva red: 2800:139:1:0000::/56, existen 8 bits que se puede utilizar para subredes, estos 8 bits se transforman en 256 subredes que salen de las combinaciones que existen entre los números del 1-9 y las letras de la A-F. Estas subredes se las puede subnetear para sacar nuestras redes para integrarlas a los routers. Podemos utilizar el /64, /112, /126, y /128, el /127 no se lo utiliza por cuestiones de seguridad. En caso de que se obtenga algún enlace punto a punto o punto host, se utilizará las dos últimas subredes para poder identificar de que se trata de un tunelado. En este caso se tendrá que utilizar las subredes 2800:139:1:00FF::/64 y 2800:139:1:00FE::/64 respectivamente, y luego subnetear para obtener direcciones reservadas para esos routers o hosts. De modo que tendríamos direcciones reservadas a /128 para este tipo de tunelado. [6], [7], [8], [9].

8. Pasos para la simulación de algoritmo de enrutamiento y enrutado.

Una vez que se ha realizado la tabla de direccionamiento de acuerdo a la red que se tiene, se procede a configurar los dispositivos para que se configure los algoritmos de enrutamiento y enrutados. Para esto primero se debe observar que los

dispositivos tengan soporte en sus IOS para IPv6 y EIGRP. Después de esto se puede proceder a realizar la configuración de los algoritmos de enrutamiento y enrutados. Como pasos a seguir para realizar la configuración tenemos:

Activación de EIGRP para IPv6

Se escoge un número de sistema autónomo que sirve para gestionar tráfico con políticas de rutas propias, en este caso el Sistema Autónomo (AS) que se escogió es diez.

Tabla 4. Activación de EIGRP para IPv6

Comando o acción
Quito> enable
Quito# configure terminal
Quito#(config) ipv6 unicast-routing
Quito #(config) interface fa0/0
Quito #(config-if) ipv6 enable
Quito #(config-if) ipv6 eigrp 10
Quito #(config-if) ipv6 router eigrp 10
Quito #(config-router)router-id 2.2.2.2
Quito#(config-router)no shutdown

En esta parte de la activación se pone un identificador de ruta que está dado en IPv4, como se puede ver en la tabla 4. Una vez que se activa EIGRP para IPv6 y ya teniendo configurado el enrutamiento IPv6, se puede descubrir las rutas dinámicamente.

Creación de VLANs y encapsulamiento Dot1Q

La creación de las VLANs se lo realiza en los dispositivos que dan la cara a las máquinas que prestan el servicio de video conferencia, para poder encapsular diferentes servicios en una sola interface.

Tabla 5. Comandos para VLANs

Comando o acción
Quito> enable
Quito# configure terminal
Quito #(config) interface fa0/0
Creación de VLAN de datos
Quito #(config-if) interface fa0/0.15
Quito #(config-subif) description datos_quito
Quito #(config-subif) encapsulation dot1Q
Quito #(config-subif) ipv6 address 2800:130:1:0115::1/64
Quito #(config-subif) ipv6 enable
Quito #(config-subif) ipv6 eigrp 10
Quito #(config-subif) ipv6 router eigrp 10
Quito #(config-router)router-id 2.2.2.2
Quito#(config-router)no shutdown
Creación de VLAN de VOIP
Quito #(config-if) interface fa0/0.16
Quito #(config-subif) description voip_quito
Quito #(config-subif) encapsulation dot1Q
Quito #(config-subif) ipv6 address 2800:130:1:0116::1/64
Quito #(config-subif) ipv6 enable
Quito ##(config-subif) ipv6 eigrp 10
Quito #(config-subif) ipv6 router eigrp 10
Quito #(config-router)router-id 2.2.2.2
Quito#(config-router)no shutdown

En cada VLAN, también se debe configurar el ID en IPv4 de la interface a la que pertenece, la dirección IPv6 que lo identifica y el tipo de encapsulamiento que se aplica (Dot1Q).

Listas de control de acceso

Las ACLs sirven para controlar tráfico, en el caso particular se debe configurar las ACLs necesarias de acuerdo a las necesidades de la institución.

Configuración de calidad de servicio (QoS)

Para la calidad de servicio tenemos que aplicar anchos de banda con prioridad, cuando se aplica QoS en la red se está aprovechando la tecnología MPLS.

Para realizar la configuración de calidad de servicio se debe tomar algunos puntos en consideración, como son: ¿Cuál será el servicio que tenga prioridad sobre el resto?, ¿cuál será la precedencia de cada servicio, los anchos de banda que se asignaran a cada servicio, y las políticas que se asignaran para la salida y lo que sé queda adentro?.

A continuación se presenta una tabla en la cual está la configuración de la calidad de servicio que se realizó en la red WAN de la UTPL.

Tabla 6. Configuración de calidad de servicio

```
QUITO
conf ter
class-map match-any APLICACIONES
match access-group name quito
match precedence 3
EXIT

class-map match-any VIDEO
match access-group name quito
match precedence 4
EXIT

class-map match-any VOICE
match access-group name quito
match precedence 5
exit

conf ter
policy-map QoS_nested

class VOICE
priority 384

class VIDEO
bandwidth 1500

class APLICACIONES
bandwidth 512
exit
exit

policy-map QoS_parent
class class-default
shape average 2400000
service-policy QoS_nested

interface se0/0
description enlace_wan
service-policy output QoS_parent
bandwidth 3300
end
```

Hasta aquí, se ha realizado toda la configuración necesaria para realizar el enrutamiento dinámico con algoritmo de enrutamiento EIGRP y algoritmo enrutado IPv4 e IPv6 que es tomado de la configuración actual de la red WAN. En todos los dispositivos de la red se configuró de forma similar pero tomando en cuenta el direccionamiento IPv6.

9. Pruebas realizadas sobre el enrutamiento Dinámico EIGRP simulado.

Para comprobar la realización del enrutamiento dinámico se realizó algunas pruebas que muestran resultados obtenidos.
Estas son algunas de las pruebas más importantes realizadas en el laboratorio de la simulación de la red WAN de la UTPL.

Interfaces configuradas con EIGRP

En esta prueba se está utilizando el comando ***show ip EIGRP interface***. En la siguiente Figura se puede ver cuáles son las interfaces que están configuradas con IPv6 y EIGRP.

```
R2
Router>show ipv6 eigrp interfaces
IPv6-EIGRP interfaces for process 10

                     Xmit Queue   Mean   Pacing Time   Multicast
Interface      Peers Un/Reliable  SRTT   Un/Reliable   Flow Timer
Fa0/0              0     0/0        0       0/1           0
Fa0/0.15           0     0/0        0       1/1           0
Fa0/0.16           0     0/0        0       2/2           0
Fa0/0.17           0     0/0        0       0/1           0
Se0/0              1     0/0     1027       0/7        4115
```

Figura 1. Ejecución del comando show IPv6 EIGRP interfaces

En la interface se0/0 se puede evidenciar que:

- Existe un router vecino directamente conectado.
- El intervalo de tiempo de ida y vuelta es de 1027 milisegundos
- El tiempo regulado para determinar cuando los paquetes EIGRP deben ser enviados a la interface es de 7 segundos (sincronización)
- Los paquetes multidifusión son enviados por el router cada 4115 segundos.
- En la VLAN 15 y 17 se detecta que el tiempo regulado para determinar cuando los paquetes EIGRP deben ser enviados a la interface es de 1 segundo y la VLAN 16 es de 2 segundos (sincronización).

Métricas Configuradas en IPv6

Las métricas se configuraron de acuerdo a los servicios que presta la red. Se tomó en cuenta que cada servicio de cada red se conecte con el mismo tipo de servicio en otra red, pero no con un servicio diferente.
Es por esta razón que se configuró las listas de control de acceso, por el momento de host a host, aunque se puede incluir toda una red, esto depende del criterio del administrador de la red.

```
R2
Router>show ipv6 access-list
IPv6 access list quito
    permit ipv6 host 2800:130:1:115::2 host 2800:130:1:125::2 sequence 10
    permit ipv6 host 2800:130:1:116::2 host 2800:130:1:126::2 sequence 20
    permit ipv6 host 2800:130:1:117::2 host 2800:130:1:127::2 sequence 30
                                  .
                                  .
                                  .
    permit ipv6 host 2800:130:1:115::2 host 2800:130:1:175::2 sequence 160
    permit ipv6 host 2800:130:1:116::2 host 2800:130:1:176::2 sequence 170
    permit ipv6 host 2800:130:1:117::2 host 2800:130:1:177::2 sequence 180
    deny ipv6 any any (1104 matches) sequence 190
```

Figura2. Commando show ipv6 access-list

Reconocimiento de rutas con EIGRP

Para el correcto funcionamiento de la simulación de debe configurar:

- Direccionamiento IPv6
- Direccionamiento IPv4
- VLANs
- ACLs
- QoS

Para revisar la correcta configuración aplicaremos el comando ***show ipv6 route eigrp*** .Se deben detectar 34 rutas debido a que existen 7 redes, las cuales cuentan con dos routers cada una, lo que suma 14 rutas, y en cada red tenemos 3 sub-interfaces a las cuales hay que llegar también, lo cual suma 21 sub-interfaces. Esto da un total de 35 Rutas, pero se debe restar los tres servicios que están encapsulados en el router sobre el cual se realizara las pruebas y la dirección de la interfaz en donde se encuentran configuradas. Esto da un total de 33 redes que debe descubrir.

A continuación se muestra el resultado de las rutas aprendidas por el router R2 Quito sobre el cual se ha realizado todas las pruebas correspondientes para sacar estos resultados.

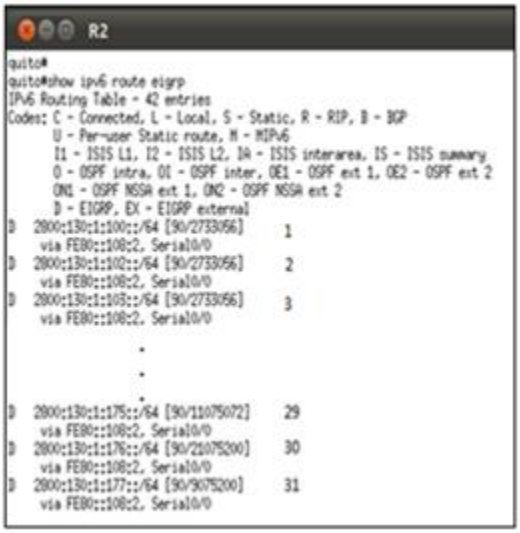


Figura 3. Comando Show IP Route

Prueba de conexión del servicio de datos de la red de Quito.

En esta prueba lo que se está realizando es la comprobación de la conexión de la PC1 que pertenece al servicio de datos con las máquinas de servicios de Guayaquil.

Figura 4. Comprobación de la conexión del servicio de datos Quito

Como resultado en la Figura anterior se puede observar que el servicio de datos de la red de Quito solamente se está conectando con el servicio de datos de la red Guayaquil, esto es gracias a las listas de control de acceso que están controlando las conexiones que se realizan con todos los servicios de las redes que representan a los centros asociados. En el resto de pruebas de los otros servicios se ve un comportamiento similar.

10. Comparaciones con el estado actual de la red WAN MPLS

Para poder realizar la comparación del estado actual con la simulación que tenemos, debemos tomar en cuenta que los dispositivos que están actualmente funcionando en la red WAN de la UTPL cumplen una función específica, mientras que en la simulación se utiliza una sola máquina, y esto puede afectar el rendimiento y la apreciación de los datos. Aclarado esto procedemos a realizar las comparaciones de la simulación con el estado actual.

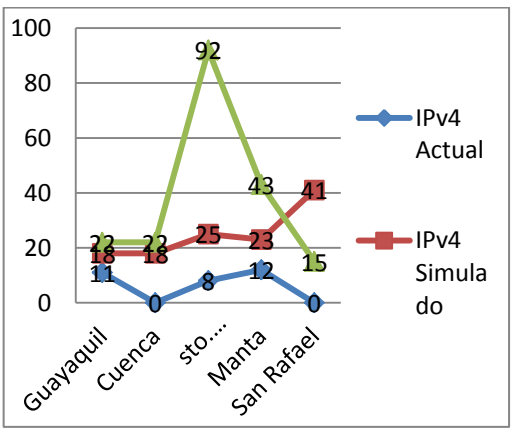


Figura 5. Comparación del retardo del canal de datos

En la Figura 5, se puede observar que la simulación IPv4 tiene un poco más de retardo en cuanto a lo que actualmente está implementado, pero este retardo no es muy significativo, mientras que la simulación IPv6, dobla el tiempo de retardo en comparación con lo que esta implementado actualmente.

Comparación del retardo del canal de VoIP

Las pruebas de retardo del canal de VoIP se realizan en cinco centros asociados.

En la prueba del canal de VoIP se puede apreciar que el IPv4 simulado con el IPv4 que se encuentra actualmente configurado en la red WAN MPLS de la UTPL, son análogos en cuanto al resultado al menos en los tres primeros centros asociados.

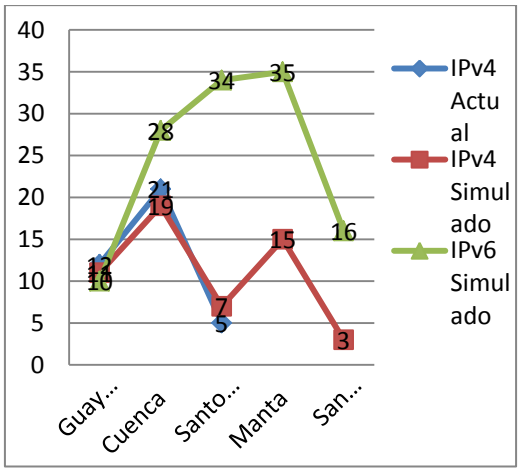


Figura 6. Comparación del retardo del canal de VoIP

En cambio la simulación de IPv6 tiene un aumento considerable en relación a IPv4 implementado.

Comparación del retardo del canal de Video

En la Figura 7, se puede apreciar que la simulación de algoritmo dinámico mantiene un retraso en comparación con lo que está actualmente.

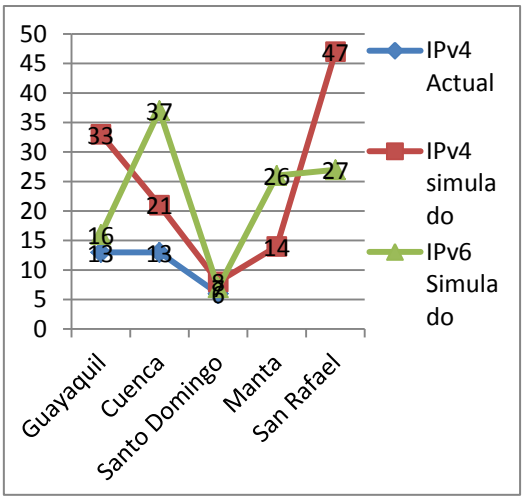


Figura 7. Comparación del retardo del canal de VIDEO

Aunque la simulación presenta una leve elevación del retardo, se puede concluir que este retraso no es de consideración, y que existe una secuencia en los datos.

Comparación de número de saltos

El número de saltos que se puede observar en la parte de la simulación es igual para todos los centros asociados, lo que hace que se tenga un rango de retardo similar en cada uno de los canales de los centros asociados.

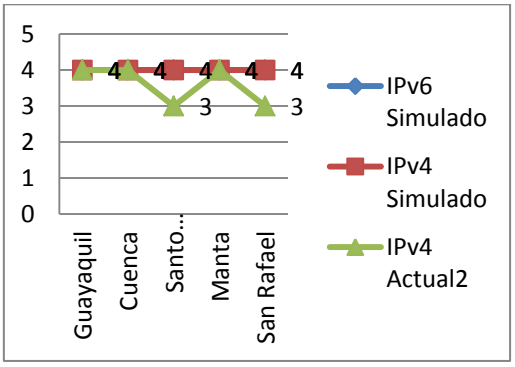


Figura 8. Número de saltos

En cambio el número de saltos de la parte que esta implementada de forma estática varía, lo cual también hace que varíe el retardo en los diferentes servicios de: Datos, Video conferencia y VoIP.

Comparación General

De acuerdo a los conceptos, pruebas y observaciones se puede definir las ventajas

que tiene la configuración simulada de la red WAN de la UTPL con respecto a la configuración actual, y viceversa. Esta comparación se la efectúa en base a toda la investigación que se ha realizado hasta el momento.

Tabla 7. Diferencias ente la simulación y lo actual

CONSIDERACIÓN	ACTUAL	SIMULADO
Rutas a difundir	Proceso manual	Proceso automático.
Soporte de VLSM	Soportado	Soportado
Escalabilidad	No factible para redes grandes y cambiantes	Se adapta rápidamente a los cambios realizados en la red.
Rapidez	Depende de las rutas estáticas.	Depende de la rapidez de convergencia del algoritmo
Direccionamiento	Estático, depende en todo momento del administrador	Dinámico, se difunde en toda la red.

Como se puede observar en el Tabla 7, la única desventaja que tiene la simulación con respecto a la configuración actual de la red WAN de la UTPL, es que su tiempo de respuesta es un poco lento, esto se puede justificar, porque cuando se está manejando una configuración Dinámica, esta deberá revisar sus tablas (tablas de vecinos, topología y encaminamiento) y escoger cual es la dirección que se necesita para realizar la conexión de la red. En cuanto a la administración de las redes, la simulación es mucho más rápida con relación a la configuración que se encuentra actualmente en la red WAN de la UTPL.

Conclusiones

- En el entorno simulado con IPv4 se puede apreciar que los canales de datos, voz y video son análogos con un error de (2 - 20 ms) lo que permite validar el modelo de simulación.
- En el entorno simulado con IPv6, es análogo con la implementación actual de la red WAN MPLS de la UTPL, con un error de 2 – 40 ms.
- En base a la verificación del modelo simulado se pude concluir que el modelo IPv6 trabajará eficientemente en el entorno real. Aunque los tiempos de transferencia sean un poco elevados en cuanto al enrutamiento estático que esta implementado actualmente.
- Al implementar el algoritmo de enrutamiento dinámico la convergencia o anuncio de nuevas rutas en la red WAN MPLS de la UTPL es mucho más rápida que un modelo estático.
- Al momento de tener los servicios ya configurados se estableció que se necesitaba implementar ACLs debido a que todo se conectaba con todo y no existía un control en los servicios prestados, por lo que se debe configurar ACLs para permitir a determinados host ingresar a los servicios.
- Se pudo evidenciar en las pruebas que el algoritmo enrutado IPV4 e IPv6 son aptos para configurarlos con el algoritmo de enrutamiento EIGRP y que pueden convivir ambos protocolos porque al momento de realizar la configuración se realizó ambas configuraciones en el mismo esquema de red.

Recomendaciones

- Se debe implementar el proyecto propuesto por parte del administrador de la red WAN debido a que mejorará el servicio, rendimiento, disponibilidad y administración de la red WAN de la UTPL.
- Antes de probar una nueva configuración de la red WAN se debe tener un laboratorio de experimentación con GNS-3 que tenga replicada la configuración de la red WAN de la UTPL lo cual ayudará a los administradores a su gestión y cambios.
- Se debe implementar IPv6 ya que estamos en una etapa de transición y los proveedores ya están trabajando sobre este protocolo, de tal forma que la UTPL ya tiene acceso a ipv6 de forma nativa.
- Es recomendable tener el enrutamiento de IPv6 en base a lo que ya se tiene

implementado con IPv4 para que el administrador pueda reconocer inmediatamente las redes que están configuradas sobre la red WAN de la UTPL y realizar una correcta administración**.**

- Para evitar inconvenientes al momento de realizar cambios sobre la red WAN de la UTPL, se debe respaldar los datos de los dispositivos en caso de que se requiera volver a la configuración anterior o en caso de que alguna configuración no se realice correctamente.
- Para implementar las configuraciones del algoritmo de enrutamiento EIGRP y algoritmos enrutados IPv4 o IPv6 se debe actualizar los IOS de los equipos para que soporten las configuraciones.
- La máquina en la cual se va a simular la red debe tener más de 4Gb de memoria para realizar una simulación completa y por mínimo un procesador Core i5 o i7 para no tener problemas en la simulación.
- En el equipo anfitrión de la simulación se recomienda tener 6144 Mb a 8192 Mb de memoria RAM, debido a que los dispositivos utilizan IOS reales y la memoria que utiliza cada dispositivo simulado es de 128 a 180 Mb y se debe tomar en cuenta que son 35 dispositivos simulados.

Bibliografía

[1] Ing. Jorge Álvarez, Resumen módulo 10, CCNA 1 v 3.1. , *[On-line] Disponible en:* http://members.fortunecity.es/unitec/resumen10.htm

[2] ICE (2008) Protocolos de Enrutamiento y Tráfico Soportado por la RAI, *[On-line] Disponible en:* https://www.grupoice.com/PEL/docsAdq/CD20081742CAR-078.doc

[3] UNITEC. Ing. Jorge Álvarez. (2005). Capa de red, protocolos, *[On-line] Disponible en:* http://members.fortunecity.es/unitec/resumen10.htm

[4] Mitecnologico, *[On-line] Disponible en:* http://www.mitecnologico.com/Main/ProtocolosEnrutadosYDeEnrutamiento

[5] ESPOL. Diseño de una red troncal en anillo de fibra óptica para el transporte de tráfico IP sobre MPLS entre las ciudades de Guayaquil, Quito y Cuenca. , *[On-line] Disponible en:* http://www.dspace.espol.edu.ec/bitstream/123456789/2547/1/5023.pdf

[6] LAC-TF IPv6 Subnetting, *[On-line] Disponible en:* http://mail.lacnic.net/pipermail/lactf/2006-January/001204.html

[7] RFC3177 - IAB/IESG Recommendations on IPv6 Address Allocations, *[On-line] Disponible en:* http://www.faqs.org/rfcs/rfc3177.html

[8] RFC3627 - Use of /127 Prefix Length Between Routers Considered, *[On-line] Disponible en:* http://www.faqs.org/rfcs/rfc3627.html

[9] The ISP Column, Just how big is IPv6? - or Where did all those addresses go?, Geoff Huston, *[On-line] Disponible en:* http://www.potaroo.net/ispcol/2005-07/ipv6size.html