UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TEMA:

Implementación del modelo Inter-AS VPN opción C para continuidad de servicios VPN entre dos redes MPLS en el Ecuador utilizando el simulador GNS3

AUTOR:

Ing. Carlos Luis Alvarez Cuesta

Trabajo de titulación previo a la obtención del grado de Magister en Telecomunicaciones

TUTOR:

Ing. Romero Paz Manuel de Jesús, MSc.

Guayaquil, 29 de octubre 2018

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

CERTIFICACIÓN

Certificamos que el presente trabajo fue realizado en su totalidad por Carlos Luis Alvarez Cuesta como requerimiento parcial para la obtención del Título de Magíster en Telecomunicaciones.

TUTOR

_____

MSc. Manuel Romero Paz

DIRECTOR DEL PROGRAMA

_____

MSc. Manuel Romero Paz

Guayaquil, 29 de octubre 2018

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

DECLARACIÓN DE RESPONSABILIDAD

YO, CARLOS LUIS ALVAREZ CUESTA

DECLARO QUE:

El trabajo de Titulación "**Implementación del modelo Inter-AS VPN opción C para continuidad de servicios VPN entre dos redes MPLS en el Ecuador utilizando el simulador GNS3**" previo a la obtención del Título de **Magíster en Telecomunicaciones**, ha sido desarrollado respetando derechos intelectuales de terceros conforme las citas que constan en el documento, cuyas fuentes se incorporan en las referencias o bibliografías. Consecuentemente este trabajo es de mi total autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance del Trabajo de Titulación referido.

Guayaquil, 29 de octubre del 2018

EL AUTOR

_____

Ing. Carlos Luis Alvarez Cuesta

UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO
MAESTRÍA EN TELECOMUNICACIONES

AUTORIZACIÓN

YO, CARLOS LUIS ALVAREZ CUESTA

Autorizo a la Universidad Católica de Santiago de Guayaquil a la **publicación**, en la biblioteca de la institución del Trabajo de Titulación de Titulación, "**Implementación del modelo Inter-AS VPN opción C para continuidad de servicios VPN entre dos redes MPLS en el Ecuador utilizando el simulador GNS3**" cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y total autoría.

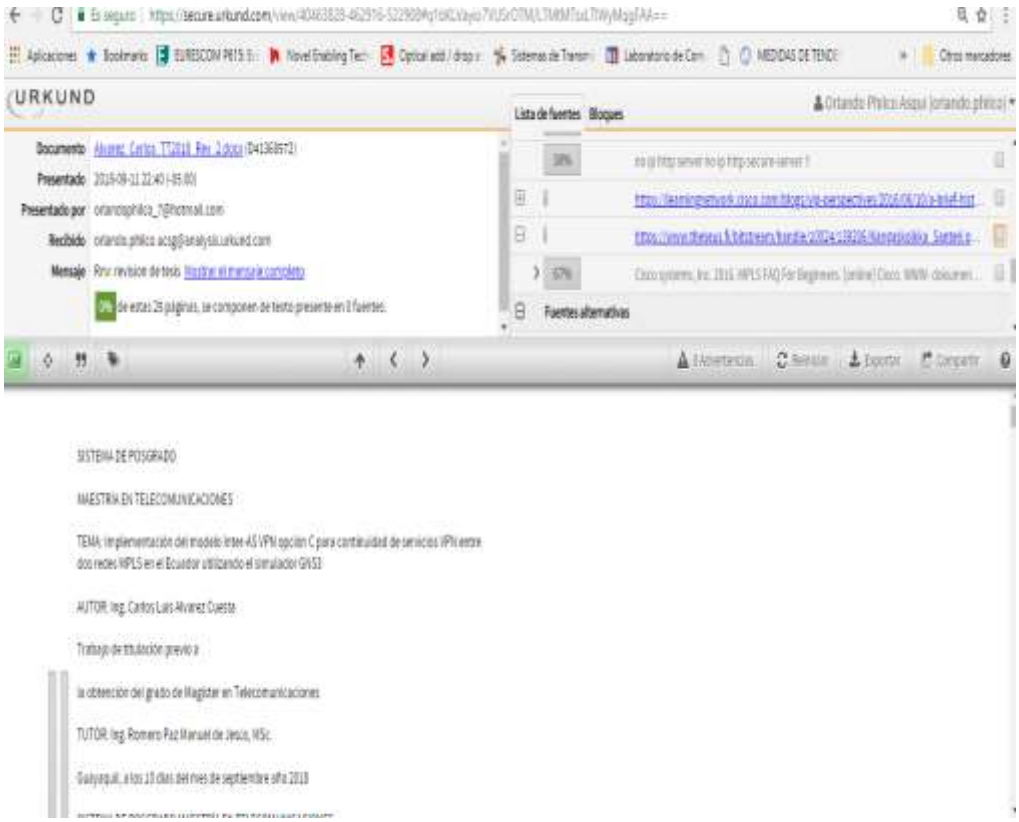
Guayaquil, 29 de octubre del 2018

EL AUTOR

_____

Ing. Carlos Luis Alvarez Cuesta

REPORTE DE URKUND



Reporte Urkund del Trabajo de Titulación de Maestría en Telecomunicaciones denominado: **Implementación del modelo Inter-AS VPN opción C para continuidad de servicios VPN entre dos redes MPLS en el Ecuador utilizando el simulador GNS3** a cargo del ingeniero **Carlos Luis Alvarez Cuesta.** Se encuentra al 0% de coincidencias.

Agradecimientos

Ante todo agradecer a Dios por darme la oportunidad de cumplir una meta más en mi carrera profesional.

A mis amados padres Luis y Mirian, sin el esfuerzo de ellos no estaría donde estoy. A ellos siempre mi gratitud por su constancia y coraje para salir adelante en momentos difíciles y sobre todo motivar a sus hijos a superarse.

A mi hermano Luis y a todos mis familiares Nina, Enedina, John, Valerie, Socorro, Enrique, Christian por nombrar algunos, quienes siempre estuvieron junto a mí para darme aliento.

Al Ing. Manuel Romero por su apoyo incondicional en todo momento, por su dedicación y guía en este trabajo de titulación.

A mi esposa Dulce María por su constante apoyo en todos los emprendimientos que realizamos juntos.

Carlos Luis Alvarez Cuesta.

Dedicatoria

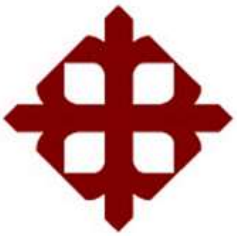
Dedico este trabajo de titulación mis padres Luis y Mirian, su gran esfuerzo hizo que llegue hasta aquí y su aliento hará que llegue más lejos.

A mi abuela Mariana, quien siempre estará presente en mi corazón y que estoy seguro que guía mis pasos desde el cielo.

A mi hermano y familiares un apoyo incondicional.

A Dulce y Bruno, mi amada familia.

Carlos Luis Alvarez Cuesta.



UNIVERSIDAD CATÓLICA
DE SANTIAGO DE GUAYAQUIL

SISTEMA DE POSGRADO

MAESTRÍA EN TELECOMUNICACIONES

TRIBUNAL DE SUSTENTACIÓN

f. _____

ROMERO PAZ MANUEL DE JESÚS

TUTOR

f. _____

MSc. Orlando Philco Asqui

REVISOR

f. _____

MSc. Luis Córdova Rivadeneira

REVISOR

f. _____

MSc. Romero Paz Manuel de Jesús

DIRECTOR DEL PROGRAMA

INDICE

INDICE FIGURAS

INDICE DE TABLAS

Resumen

El presente trabajo de titulación comparte la experiencia de simulación del Inter AS opción C como solución escalable para la continuidad de servicios VPN (Virtual Private Network) capa 3 a través de sistemas autónomos.

Para brindar esta experiencia al lector, es necesario detallar fundamentos teóricos del Inter AS opción C tales como: BGP (Border Gateway Protocol), MPLS (Muliprotocol Label Switching), MP-BGP (Multiprotocol Border Gateway Protocol). De igual manera, se dará a conocer el software de simulación GNS3 que servirá para simular dos dominios MPLS en los cuales se levantará un servicio Inter AS.

Los clientes constantemente buscan mejoras en sus redes de datos y más aún optimizar costos de infraestructura. La simulación del Inter AS le permitirá al lector constatar los beneficios y usos del Inter AS, los cuales servirán para aplicarlos a casos reales que permitan monetizar la solución.

Palabras Claves:

VPN, Inter AS, BGP, MPLS, MP-BGP, GNS3.

Abstract

The present degree work shares the simulation experience of the Inter AS option C as a scalable solution for the continuity of VPN (Private Virtual Network) services layer 3 through autonomous systems.

In order to provide this experience to the reader, it is necessary to detail the theoretical foundations of the Inter AS option C such as: BGP (Border Gateway Protocol), MPLS (Muliprotocol Label Switching), MP-BGP (multiprotocol protocol Border Gateway). In the same way, the GNS3 simulation software will be announced that will serve to simulate two MPLS domains in which an Inter AS service will be built.

Customers always seek improvements in their data networks and more without optimizing infrastructure costs. The simulation of Inter AS will allow the reader to verify the benefits and uses of Inter AS, which will be used to apply them to real cases that allow the solution to be monetized.

Key words:

VPN, Inter AS, BGP, MPLS, MP-BGP, GNS3.

Capítulo 1: Descripción del Proyecto de Intervención.

El proyecto de intervención describe el uso de la funcionalidad INTERAS Opción C (Inter Autonomous System) como alternativa para extensión de servicios VPN (Virtual Private Network) entre dominios MPLS (Multiprotocol Label Switching).

1.1. Introducción.

Hoy en día con el vertiginoso incremento de tráfico de aplicaciones de voz y datos, las empresas de servicio deben imperiosamente invertir en su infraestructura de redes IP (Internet Protocol) para sostener la continuidad de su negocio.

Dada la situación económica actual del Ecuador, los altos ejecutivos de las empresas siempre estudian nuevas formas de minimizar los costos de operación y maximizar sus ganancias. Como resultado de estos estudios, muchas veces, la unión o alianza entre empresas representa un camino próspero para mejorar sus finanzas.

El presente trabajo investigativo, se enfoca en diseñar y simular la unificación de redes MPLS (Multiprotocol Label Switching) para la continuidad de servicios de VPN extremo a extremo utilizando Inter-AS VPN opción C, lo cual permite optimizar el uso de infraestructura de las empresas que forman la alianza estratégica.

El Inter-AS permite la sinergia entre redes MPLS de distintas empresas con el fin de brindar un servicio de transmisión de voz y datos con la infraestructura más cercana al cliente. Cabe resaltar, de que esta infraestructura puede ser de cualquiera de las dos empresas que interviene en el Inter-AS.

Para simular el Inter-AS, se utilizará el simulador GNS3 (Graphical Network Simulator), el cual es un software de código abierto bajo GPL (General Public License) v3. Dicha plataforma permite bosquejar y simular la unificación de dos redes MPLS para brindar servicios VPN extremo a extremo.

1.2. Antecedentes.

El desarrollo de las comunicaciones ha sido siempre un motor que impulsa a grandes empresas a innovar y crear soluciones efectivas para minimizar los impactos que conlleva el crecimiento de tráfico de aplicaciones de voz y datos.

Conforme incrementa la demanda de los servicios de los usuarios, las redes crecen y se hacen más y más complejas. Como consecuencia, el gasto operativo de estas redes también se ve afectado y por ende la rentabilidad del negocio.

La solución INTER AS VPN opción C, fue publicada por primera vez el 2 de mayo del año 2005 (Cisco Systems, 2014), publicación que sirvió para que muchos ingenieros de networking diseñen soluciones propias para su medio, en base a sus necesidades y las de los usuarios.

1.3. Definición del problema

En muchos casos las empresas de servicio de comunicaciones en el Ecuador, no cuentan con puntos de presencia de infraestructura MPLS en todas las localidades en las que el usuario quisiera acceder a servicios de VPN de datos. Sin embargo, existen empresas que son filiales y que tienen puntos de presencia MPLS situados según su nicho de mercado, lo cual podría brindar el servicio VPN en la localidad que necesita el cliente, pero que por la falta de la unificación de redes MPLS entre empresas, no se puede llegar a brindar el servicio de VPN extremo a extremo.

Justificación del Problema a Investigar.

Lo más importante para una empresa de servicio es lucrarse de sus ventas y satisfacer la necesidad de los clientes. La problemática en base a la falta de unificación de redes para brindar servicios de VPN extremo a extremo, lleva a investigar el INTER AS VPN opción C para diseñar y simular la continuidad de servicios de VPN entre 2 redes MPLS.

1.4. Objetivos

Los objetivos planteados para el presente trabajo de investigación son los siguientes:

1.4.1. Objetivo General:

Implementar en GNS3 un servicio VPN extremo a extremo a través de 2 dominios MPLS utilizando INTER AS VPN opción C.

1.4.2. Objetivos específicos:

- ✓ Conocer los elementos que componen un dominio MPLS y entender su funcionamiento.
- ✓ Describir el uso del INTER-AS opción C en la extensión de servicios de VPN entre dominios MPLS.
- ✓ Simular 2 dominios MPLS como base para el estudio del INTER AS VPN opción C.
- ✓ Simular servicios VPN extremo a extremo a través de 2 dominios MPLS de distinto AS usando INTER AS VPN opción C.
- ✓ Analizar las ventajas que brinda el INTER AS VPN opción C en la continuidad de servicios VPN a través de distintos dominios MPLS.

- ✓ Análisis extremo a extremo del plano de control y de forwarding de los paquetes de datos a través de los 2 dominios MPLS que intervienen en el INTER AS VPN.

1.5. Hipótesis

Dadas las necesidades de comunicación de los clientes de hoy en día en lo que respecta a servicios VPN y la necesidad de proveer la continuidad de estos servicios a través de 2 dominios distintos MPLS, impulsan a este trabajo investigativo a respaldar en base a resultados obtenidos de las simulaciones, el criterio de que el INTER AS VPN opción C es el método de conectividad más escalable y funcional en lo que respecta a servicios VPN extremo a extremo.

1.6. Metodología de investigación.

Este trabajo es de carácter documental, investigativo y experimental, en el cual se utiliza el conocimiento empírico, el conocimiento teórico y una simulación para expresar al lector las bondades del Inter AS VPN opción C (Cruz, 2014).

Vale mencionar que el presente trabajo utiliza el método inductivo, el cual es un procedimiento de sistematización que va de lo individual a lo general, es decir que a partir de los resultados obtenidos en forma particular busca un sustento para una replicación general (Gomez, 2012).

Capítulo 2: Fundamentación Teórica.

Para fundamentar el estudio, se deben conocer los conceptos que intervienen en el INTER-AS, razón por la cual este capítulo resumirá los fundamentos teóricos de MPLS y el INTER-AS como método para interconexión de dominios MPLS.

2.1. Fundamentos de MPLS.

MPLS, definido como estándar por la IETF (Internet Engineering Task Force) con la RFC 3031 (Viswanathan, Callon, & Rosen, 2001), es una tecnología que se caracteriza por asignar etiquetas o labels a los paquetes que ingresan a la red MPLS y que luego son enviados a sus distintos destinos.

MPLS es una tecnología multiprotocolo, en razón de que para el plano de forwarding de los paquetes, utiliza intercambio de etiquetas entre los equipos que componen el dominio MPLS, y para el plano de control se pueden utilizar como IGP (Interior Gateway Protocol) los protocolos dinámicos OSPF (Open Short Path First), ISIS (Intermediate System to Intermediate System), BGP (Border Gateway Protocol), etc.). Como alternativa a utilizar protocolos dinámicos, se puede considerar el uso de enrutamiento estático, sin embargo, no es lo más aconsejable dada la poca escalabilidad y el incremento en la carga operativa para habilitar manualmente nuevos enrutamientos.

2.2. Arquitectura MPLS

Para comprender el funcionamiento de una red MPLS y los servicios que se pueden implementar, es necesario conocer los principales componentes que integran un dominio MPLS.

En la figura 2.1 se observa de manera general los componentes de un dominio MPLS.

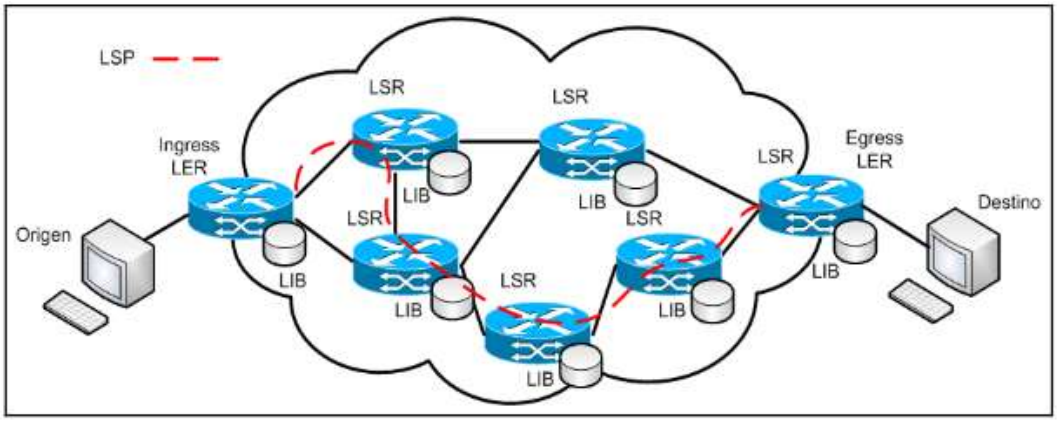


Figura 2. 1: Estructura del paquete IP con la inclusión de la etiqueta MPLS

Fuente: (Sánchez, 2010, p. 15)

2.2.1. FEC (Forwarding Equivalence Class).

La FEC es un grupo de paquetes que tienen el mismo comportamiento cuando es transportado a través de una red MPLS (Cisco Systems, 2016). Es decir, que este grupo de paquetes tienen un destino o una interface de salida común, o en general cualquier tipo de tratamiento que involucre a que un grupo de paquetes tengan un fin común.

2.2.2. Etiquetas/Labels MPLS.

El principio fundamental de MPLS es la transmisión de paquetes por conmutación de etiquetas, en la figura 2.2 se muestra la adición del label MPLS entre las cabeceras de un paquete.

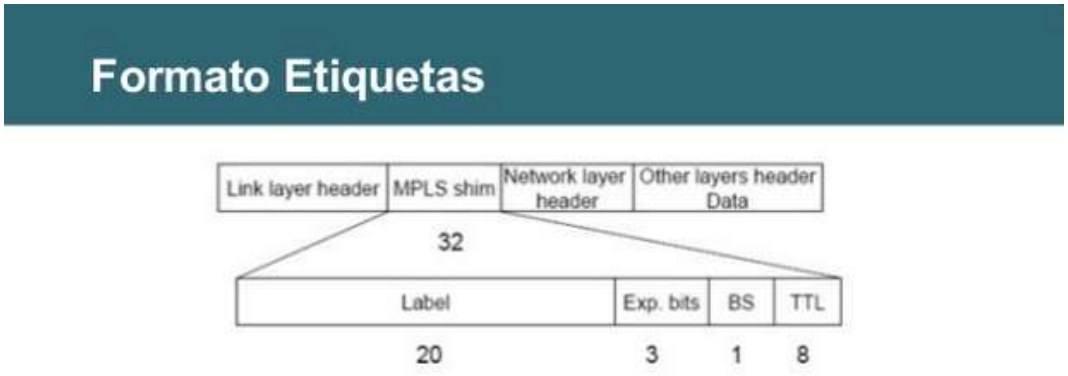


Figura 2. 2: Estructura del paquete IP con la inclusión de la etiqueta MPLS

Fuente: (Medina, 2006, p. 6)

Las etiquetas MPLS sirven para identificar una FEC y en la estructura del paquete es colocada entre la capa de enlace de datos y la capa de red, haciendo referencia al modelo OSI (Open System Interconnection).

El formato de etiqueta se compone de la siguiente manera (Cisco Systems Learning, 2004, p. 30):

20 bits para identificación de la etiqueta.
3 bits nombrados como bits experimentales EXP, utilizados para DiffServ (Servicios Diferenciados) /CoS (Clases de Servicio).
1 bit para stack S de etiquetas, lo cual indica que existen más etiquetas añadidas al paquete ip, s=0 existen más etiquetas S=1 no existen más etiquetas.
8 bits correspondientes al campo TTL (Time to Live), representa el número de saltos máximo para que el paquete no se descarte.

2.2.3. LSR (Label Switch Router).

La función del LSR es conmutar los paquetes que ingresan al dominio MPLS en base a etiquetas. A su vez, los LSR también pueden conmutar paquetes basado en IP destino en caso de que el paquete no tenga asignada una etiqueta (dominio IP).

El LSR de acuerdo a los requerimientos de la red, asocia dentro de su estructura tablas de enrutamiento tanto para el dominio IP llamada FIB (Fordwarding Information Base) como para el dominio MPLS llamada LFIB (Label Fordwarding Information Base).

Las funciones principales del LSR son las siguientes (Cisco Systems Learning, 2004, p. 32):

Plano de Control: Intercambiar información de protocolos de enrutamiento, intercambiar información de etiquetas.
Plano de Datos: Enviar paquetes basado en etiquetas (Frame Mode) y enviar paquetes basado en VPI/VCI (Cell mode)

2.2.4. LER (Label Edge Router).

Al Igual que el LSR, el LER puede realizar el enrutamiento de paquetes en base a IP destino, así como también en base a etiquetas. Sin embargo, el LER se ubica en el borde del dominio MPLS (entrada y salida).

El LER tiene funciones específicas dependiendo de la perspectiva de análisis , es decir, desde el punto de vista en que los paquetes IP ingresan al dominio MPLS, así como también de los paquetes IP que salen del dominio MPLS. Estas funciones se describen a continuación (Sánchez, 2010, p. 14):

LER de entrada: Analiza el paquete IP que ingresa al dominio MPLS, lo asocia a un FEC y finalmente el LER asigna una etiqueta MPLS a la FEC para que el paquete sea transportado en el dominio MPLS.

LER de salida: A la salida ocurre el proceso inverso, el paquete es analizado y el LER remueve la etiqueta MPLS para luego consultar su FIB y enviar el paquete a su dirección de destino en el dominio IP.

2.2.5. LSP (Label Switched Path).

El LSP es un camino construido por los LSR del dominio MPLS, este camino sirve de tránsito para los paquetes previamente etiquetados por el LER. Como observación, pueden existir varios LSP formados por los LSR dentro de un mismo dominio MPLS. Cabe recalcar que todos los paquetes asociados a una misma FEC recorrerán el mismo LSP.

2.2.6. LDP (Label Distribution Protocol).

El protocolo de distribución de etiquetas es usado por los LSR del dominio MPLS, el cual se encarga de mantener las asignaciones de etiquetas a las FEC (Viswanathan et al., 2001).

El establecimiento de las sesiones LDP entre los LSR es muy importante para mantener activos los LSP por donde transitarán los paquetes.

2.2.7. Asignación de etiquetas.

Existen 2 métodos de asignación de etiquetas en un dominio MPLS:

Downstream-on-demand

Distribución de etiquetas bajo demanda, el LSR upstream solicita una etiqueta para una determinada FEC a un LSR de downstream figura 2.3.

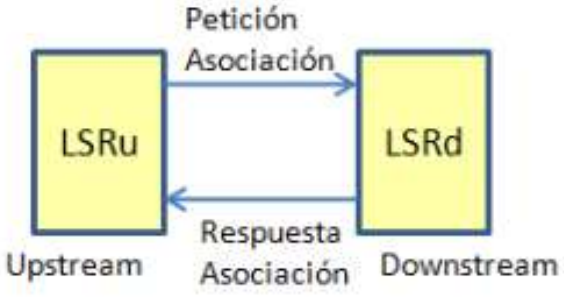


Figura 2. 3: Flujo de señalización método Downstream-on-demand

Fuente: (Sánchez 2010:28)

Unsolicited-downstream

En este método, el LSR de downstream asigna una etiqueta a las FEC sin que los LSR de upstream la hayan solicitado, figura 2.4.

Figura 2. 4: Flujo de señalización método Unsolicited-downstream

Fuente: (Sánchez 2010:28)

2.3. Fundamentos de BGP y servicios VPN sobre redes MPLS

El protocolo más utilizado y de mayores prestaciones para el enrutamiento de redes ip, es sin lugar a duda BGP (Border Gateway Protocol). Esta sección resumirá los fundamentos básicos de BGP, su terminología y un breve recuento del uso de una VPN (Virtual Private Network) sobre redes MPLS.

2.3.1. Puntos de referencia en redes MEN.

BGP es un protocolo de enrutamiento avanzado, que permite el enrutamiento entre ASes (Autonomous Systems). Es decir, que este protocolo brinda la capacidad de compartir información del mapa de rutas entre 2 ASes y a su vez aplicar mecanismos de filtrado y políticas de enrutamiento para la optimización del flujo de paquetes IPs (Rekhter, 2006).

Para efectos teóricos, BGP utiliza el puerto TCP (Transport Control Protocol) 179 para escuchar los mensajes de señalización entre los routers que establecen la sesión BGP. A continuación, los mensajes utilizados en BGP:

Open

Es el mensaje de inicio de sesión, que permite el intercambio y negociación de los parámetros BGP, entre ellos (AS Local, versión, holdtime, entre otros).

Keepalive

Mantiene la sesión BGP abierta ante la ausencia de un mensaje de UPDATE. (“hans-reyes-tutorial-enrutamiento-bgp.pdf”, s/f, p. 21).

Update

Mediante este mensaje, los speakers de BGP intercambian información de rutas junto con sus atributos. Multiples rutas que tienen el mismo path de atributos, pueden ser advertidas en un mismo mensaje de update.

Notification

Reporta a los speakers errores en la sesión BGP, una vez notificado el error, la sesión se cierra hasta que exista un nuevo mensaje de OPEN.

2.3.2. MP-BGP.

Es una extensión del protocolo BGP que permite propagar por medio de sus sesiones, varias familias de direcciones tales como ipv4 Unicast, ipv4 Multicast, ipv6 unicast, ipv6 multicast, etc. MP-BGP (Multiprotocol-Border Gateway Protocol), conserva todos los atributos de enrutamiento del protocolo BGP y por ende todos los mecanismos de selección de ruta.

El uso más común del protocolo MP-BGP es intercambiar información de una VPN en una red MPLS como por ejemplo el prefijo, la etiqueta, y demás atributos (Katz <dkatz@juniper.com>, 2007).

2.3.3. VPN de capa 3 sobre redes MPLS.

Una VPN de capa 3, es un servicio ofrecido por proveedores que tienen un backbone MPLS, el propósito es brindar una red virtual a cada usuario sobre la misma infraestructura física de transporte.

Es importante conocer que cada VPN ofrecida, tendrá su propio direccionamiento, enrutamiento y atributos, que permitirá total independencia entre los clientes. La responsabilidad de enlazar los sitios de los clientes por medio de la creación de túneles será netamente del proveedor del servicio figura 2.5.

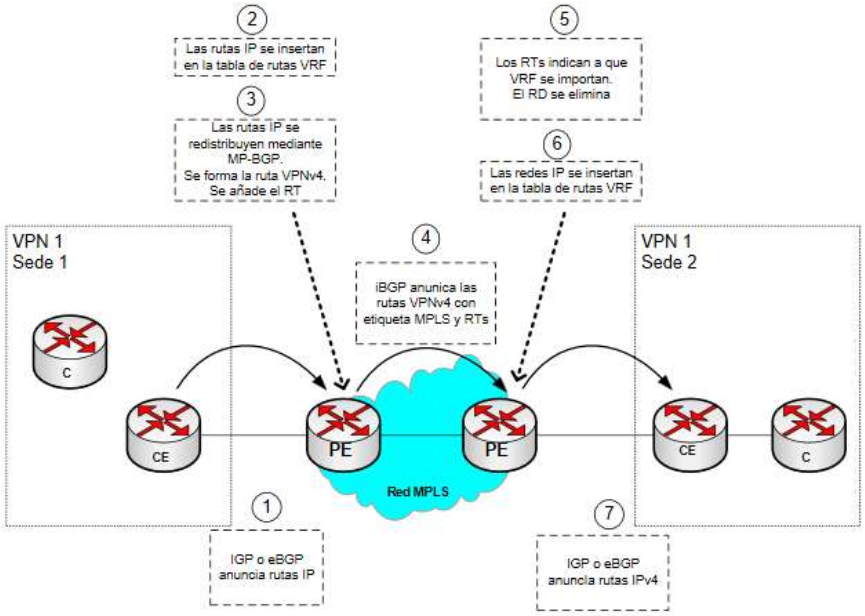


Figura 2. 5: Servicios VPN capa 3 sobre MPLS

Fuente: (“PFC_Alvaro_Gonzalez_Carrasco.pdf”, s/f, p. 58)

Para que se pueda crear una VPN de servicio, es necesario que el administrador del backbone MPLS defina correctamente los siguientes parámetros:

RD (Route Dintinguisher)

Se usa para identificar el origen de una ruta, es un identificador numérico de 64 bits que tiene como objetivo principal asociar un grupo de prefijos a una VPN en particular.

Prefijo VPNv4

A las rutas transportadas por el protocolo MP-BGP se las conoce como rutas o prefijos VPNv4. Estas rutas se las representa de la siguiente manera:

RD+ Prefijo ipv4+ Máscara de red= 128 bits
RD= 64 bits
Prefijo Ipv4= 32 bits
Máscara de red= 32 bits

Route Target

Es un identificador numérico que se utiliza para asociar las rutas de una VPN y compartir dichas rutas entre varias VPNs. Este identificador numérico tiene 64 bits de longitud.

2.3.4. Transmisión de paquetes en una red VPN MPLS.

Es claro que en una red MPLS el envío de tráfico se lo hace por conmutación de etiquetas, que a su vez están asociadas a paquetes ips. No existe la transmisión de rutas VPNv4 a través de una red ip pura, debido a que se necesita información de las VRF´s. Se denomina VRF (Virtual Routing and Forwarding) a una instancia virtual de ruteo y envío de paquetes.

La transmisión empieza con el intercambio de rutas ipv4 entre el CE (Customer Edge) y el PE (Provider Edge), en este tramo de conexión, el cliente y el

proveedor pueden utilizar enrutamiento estático o enrutamiento dinámico como BGP, OSP, entre otros, para intercambiar rutas ipv4 figura 2.6.

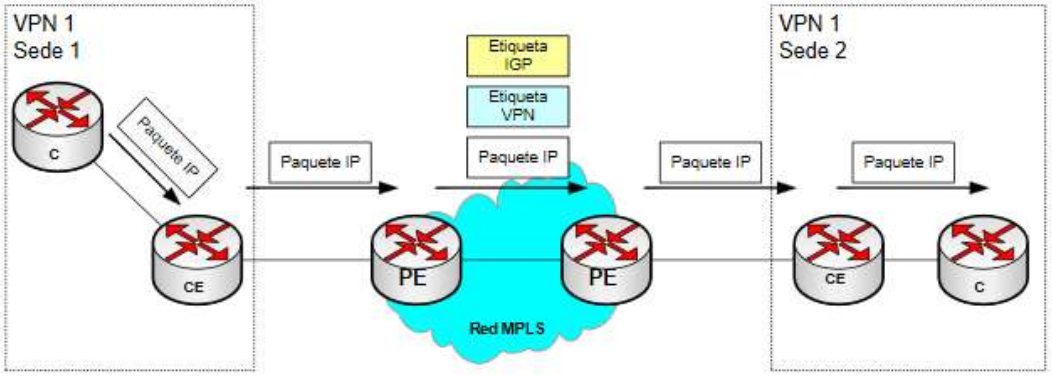


Figura 2. 6: Servicios VPN capa 3 sobre MPLS labels
Fuente: ("PFC_Alvaro_Gonzalez_Carrasco.pdf", s/f, p. 59)

En la red MPLS del proveedor, todo tráfico de ingreso es etiquetado para luego ser transmitido entre los elementos que conforman la red. De esta forma, el PE de ingreso asigna 2 etiquetas; una etiqueta externa que es la etiqueta IGP, la cual se distribuye utilizando LDP o RSVP. Es decir, que cada ruta que se encuentra instalada en la tabla global del IGP y que contiene la información de ruteo hacia los P (Provider), PE de ingreso y PE de Egreso, es etiquetada para formar la tabla conocida como LFIB (Label Fordward Information Base), de esta manera se conocen los destinos del paquete etiquetado dentro de la red MPLS.

La otra etiqueta es de tipo interna y es la que asigna el protocolo MP-BGP a la VPN para anunciar las rutas VPNv4 de PE a PE. Una vez que llega el paquete al PE de egreso, las etiquetas son retiradas y entregadas al CE en una sesión ipv4 pura. (Rosen and Rekhter n.d.)

2.4. Introducción al INTER AS

El concepto de INTER-AS se denota en la interconexión de 2 o más redes con sistemas autónomos distintos. Es decir la interconexión de dominios MPLS con la

finalidad de extender servicios VPNs capa 2 y capa 3 de filiales u operadoras distintas.

Existen 3 tipos de interconexión INTER-AS, que dependen mucho de las necesidades y recursos disponibles de cada empresa, a continuación los tipos de INTER-AS:

Opción A

Es la conexión lógica back to back de las VPNs de servicio entre los ASBRs. Para lograr esto, se asocia una VPN por interface lógica en los ASBRs que están conectados directamente y se establece una sesión MP-BGP para intercambiar paquetes sin etiquetas entre los dominios MPLS. Esta es la opción más segura y de mayor rapidez de despliegue.

Opción B

En esta opción, los ASBRs tienen la mayor carga de procesamiento de paquetes. Los ASBRs levantan una sesión MP-BPG con sus PEs internos para aprender las rutas VPNv4 y posterior a eso intercambian estas rutas con el ASBR del otro operador por medio de una sesión MP-BGP.
Para finalizar los tipos de INTER-AS, se tiene la opción C que se describe a continuación.

2.4.1. Inter AS Opción C.

Una de las opciones más eficaces y escalables para interconectar distintos sistemas autónomos es sin lugar a duda INTER-AS Opción C.

La utilidad es sumamente importante, debido a que permite optimizar recursos de infraestructura entre empresas aleadas. Por ejemplo, una empresa de servicio con

infraestructura MPLS cuya cobertura se limita a brindar servicios de hosting en una determinada ciudad, puede extender su dominio MPLS a través de otra empresa que tenga presencia de red MPLS en varias localidades. En esta sección se resumirá la arquitectura y los beneficios de utilizar INTER-AS Opción C.

2.4.2. Fundamentos del Inter AS Opción C.

La interconexión INTER-AS opción C se fundamenta en el RFC 4364 y es la opción más escalable en lo que respecta a tipos de conexión entre dominios MPLS.

La RFC 4364 indica que las rutas VPNv4 no son advertidas por los ASBRs (Autonomous System Boundary Routers) sino más bien, son distribuidas por un elemento de red dedicado a la replicación de rutas como lo es el RR (Route Reflector).

En la formación del LSP (Label Switch Path) y transporte de los paquetes entre los ASs se utilizan 3 etiquetas, la etiqueta más externa es asignada por el PE de ingreso y corresponde a la ip de la loopback del ASBR (conocida a través del IGP), la etiqueta del medio hace referencia a la ip del PE de egreso y es asignada por el ASBR y por último la etiqueta que se encuentra más abajo en la pila, corresponde a la ruta VPNv4 y es asignada por el PE de egreso. (Rosen and Rekhter n.d.:33)

2.4.3. Arquitectura del Inter AS Opción C.

Para realizar el caso de estudio es importante conocer la arquitectura y el funcionamiento lógico del INTER AS, de esta forma se obtendrá una conclusión basada en un hecho demostrativo que será contrastado con el conocimiento teórico.

En la figura 2.7 se observan los elementos y consideraciones técnicas que se deben analizar para entender el funcionamiento de la solución.

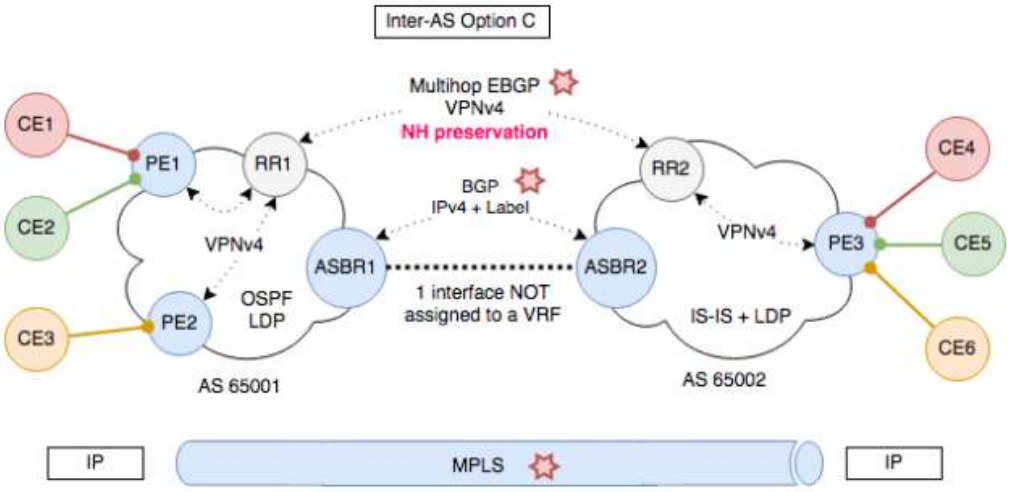


Figura 2. 7: Arquitectura de INTER AS opción C
Fuente: ("Inter-AS Option C - 118339 - The Cisco Learning Network", s/f)

A continuación un breve resumen de los elementos que intervienen en la interconexión de sistemas autónomos:

CE

Es el dispositivo final de la red MPLS y es colocado en las premisas del cliente, en esta arquitectura es nombrado Customer Edge.

PE

El Provider Edge es el equipo que dependiendo del sentido del tráfico puede ser de egreso o ingreso. Cuando el flujo de tráfico ingresa a la red MPLS el PE asigna una etiqueta para que los paquetes puedan ser transportados dentro de la red MPLS y cuando el flujo de tráfico sale de la red MPLS, el PE retira la etiqueta y entrega el paquete en ip puro al equipo destino.

ASBR

En la arquitectura representa el router de borde de la red MPLS, su acrónimo significa Autonomous System Boundary Router. La función de este equipo es encaminar los paquetes en función de la etiqueta, debe ser lo suficientemente robusto para procesar, clasificar y conmutar los paquetes sin agregar retardo.

RR

Los Route Reflectors son los encargados de replicar las rutas de las distintas familias IPv4, IPv6, VPNv4, etc a los PEs de ingreso y egreso de una red MPLS.

2.4.4. Plano de control del INTER-AS opción C.

El plano de control hace referencia a los mensajes de señalización de los equipos de comunicación que son necesarios para operar, gestionar y mantener el estado de la red. A diferencia del plano de control (ambiente lógico), el plano de datos se encarga del reenvío de paquetes a nivel de hardware, basado en el establecimiento de sesiones previamente definidas en el plano de control figura 2.8.

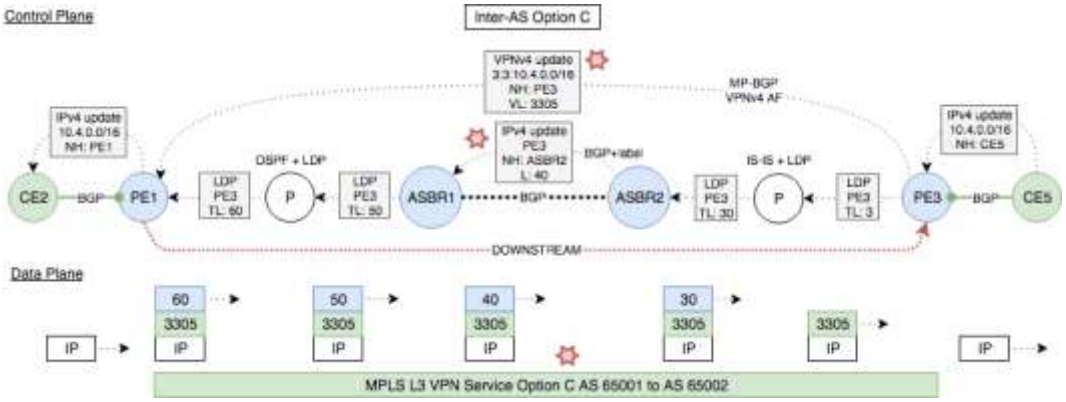


Figura 2. 8: Arquitectura Plano de Control y de Datos del INTER AS opción C.
Fuente: ("Inter-AS Option C - 118339 - The Cisco Learning Network", s/f)

El establecimiento de las sesiones en este caso particular se lo realiza de la siguiente manera:

I. En el gráfico se observan 2 dominios MPLS, el uno utiliza OSPF como IGP más LDP para distribución de etiquetas y el otro dominio utiliza ISIS como IGP más LDP para distribución de etiquetas.

II. El CE5 por medio de una sesión BGPv4 anuncia el prefijo 10.4.0.0/16 al PE3 que es el PE de ingreso.

III. El PE3 levanta una sesión MP-BGP VPNv4 para anunciar el prefijo VPNv4 con su respectiva etiqueta hacia el PE de egreso.

IV. Entre los ASBR1 y ASBR2, se establece una sesión BGP más etiquetas para continuar el LSP entre los dominios MPLS, es imperioso habilitar la capacidad de procesar etiquetas en esta sesión, de lo contrario el paquete en ese tramo se descartaría.

V. Por último, el prefijo es anunciado vía BGPv4 desde el PE1 que es el PE de egreso hacia el CE2, completando de esta forma el LSP.

2.4.5. Plano de datos del INTER-AS opción C.

El plano de datos se encarga del reenvío de paquetes basado en hardware, es decir es el dispositivo de red tiene conocimiento de sus interfaces físicas y en base al establecimiento previo de las sesiones lógicas (Plano de Control), decide que interfaces utilizará para enviar o recibir tráfico tanto de ingreso como de egreso.

El reenvío de paquetes entre los dominios MPLS se lo realiza de la siguiente manera:

I. El CE2 hace una búsqueda en su tabla de rutas IPv4 y encuentra que el paquete debe ser enviado hacia el PE1.

II. El PE1 hace una búsqueda en la LFIB y una de sus entradas indica que el prefijo VPNv4 10.4.0.0/16 es alcanzable a través del PE3 por medio de la etiqueta 3305. En ese momento, el PE1 hace una búsqueda recursiva en la LFIB para saber cómo alcanzar el PE3 y encuentra una entrada que le indica que debe utilizar la etiqueta 60 que lo lleva al P.

III. Cuando el paquete llega al P, este realiza una búsqueda en la LFIB y encuentra que el paquete debe ser enviado ASBR1 por medio de la etiqueta 50.

IV. El ASBR1 envía el paquete al ASBR2 basándose en la etiqueta que asignó BGP (etiqueta 40).

V. El ASBR2 envía el paquete hacia el P por medio de la etiqueta 30.

VI. EL P recibe una etiqueta 3 que le indica que debe remover la etiqueta más externa (IGP) antes de enviar a su último salto PE3.

VII. Finalmente el PE3 remueve la etiqueta de la VPNv4 y entrega el paquete por medio de la sesión BGPv4 al CE5.

Capítulo 3: Simulación de un servicio Inter AS VPN opción C.

Este capítulo detalla los recursos necesarios para que el lector pueda entender de manera práctica el funcionamiento del Inter AS VPN opción C y al mismo tiempo pueda asociar la teoría y la práctica al caso de negocio planteado como problemática para la interconexión de 2 empresas con AS distintos.

3.1. Descripción del caso de uso de Inter AS VPN opción C.

La principal propuesta de este trabajo de titulación es transmitir al lector el conocimiento necesario para aplicar el INTER AS en casos de negocios en los que se requiera un servicio extremo a extremo entre empresas de distinto AS.

Muchas veces se detallan conceptos teóricos muy abstractos que dificultan entendimiento para el lector. En esta ocasión se explicarán los conceptos fundamentales del INTER AS basados en un caso práctico que expresa la necesidad de 2 empresas de telecomunicaciones; una de ellas brinda servicios de conexión a Internet y entretenimiento con servicios de películas bajo demanda para sus clientes, de ahora en adelante nombrada empresa A y la otra que también brinda servicios de Internet pero que su gran fortaleza es tener cobertura a nivel Nacional a excepción de Guayaquil, de ahora en adelante llamada empresa B.

En este caso de negocio la empresa B tiene puntos de presencia o cobertura en la mayor parte del país, además, esta empresa es parte del mismo grupo empresarial a la que pertenece la empresa A. La empresa A como se lo expresó en el párrafo anterior, tuvo la visión de desarrollar un servicio de entretenimiento que era muy popular, pero que lamentablemente tenía como limitante las zonas de cobertura de la empresa (únicamente en la ciudad de Guayaquil).

En vista de esta particularidad y de mejoras de rentabilidad del negocio, se propone aplicar INTER AS opción C para brindar servicios de VPN extremo-

extremo. Lo que se pretende es brindar el servicio de entretenimiento a los clientes existentes de la empresa B y a su vez extender las zonas de cobertura de la empresa A para que este servicio sea Nacional.

Afortunadamente la empresa A y la empresa B tienen puntos de presencia en la ciudad de Guayaquil y cuentan con equipos sumamente robustos para realizar conexiones de alta capacidad de transmisión de datos.

En capítulos anteriores se abordaron conceptos teóricos que contribuyeron con el enriquecimiento conceptual del lector, ahora se utilizará el método experimental para consolidar la base de conocimiento mediante la simulación del INTER AS y las fases de planeación y diseño.

3.2. Software de simulación GNS3.

El software de simulación GNS3 permite reproducir escenarios de pruebas controlados que luego servirán para implementar soluciones escalables y libres de errores en equipos reales.

En la siguiente tabla 3-1 se detallan los principales beneficios que brinda el software de simulación:

Tabla 3-1. Beneficios de GNS3

Software de simulación GNS3	
Conectividad	Permite definir las interfaces necesarias e implementar protocolos acordes a las necesidades del diseño.
Virtualización	Brinda la posibilidad de virtualizar dispositivos de red de los fabricantes más empleados en implementaciones de soluciones tecnológicas.
Estabilidad	GNS3 es un software de altas prestaciones, cuyos pre-requisitos de instalación definen la estabilidad de las simulaciones.
Documentación	Al ser uno de los simuladores más utilizados en el medio tecnológico, GNS3 se ha convertido en una de las mayores bases de conocimiento gracias a la contribución de experiencia de muchos expertos IT.

Fuente: Autor 2018

En base a estos beneficios, se resumirán los principales puntos a considerar para la implementación de la solución en el simulador.

La conectividad es un punto muy importante y GNS3 permite simular varios tipos de interfaces cuando simulas un dispositivo de red, tal como se ilustra en la figura 3.1.

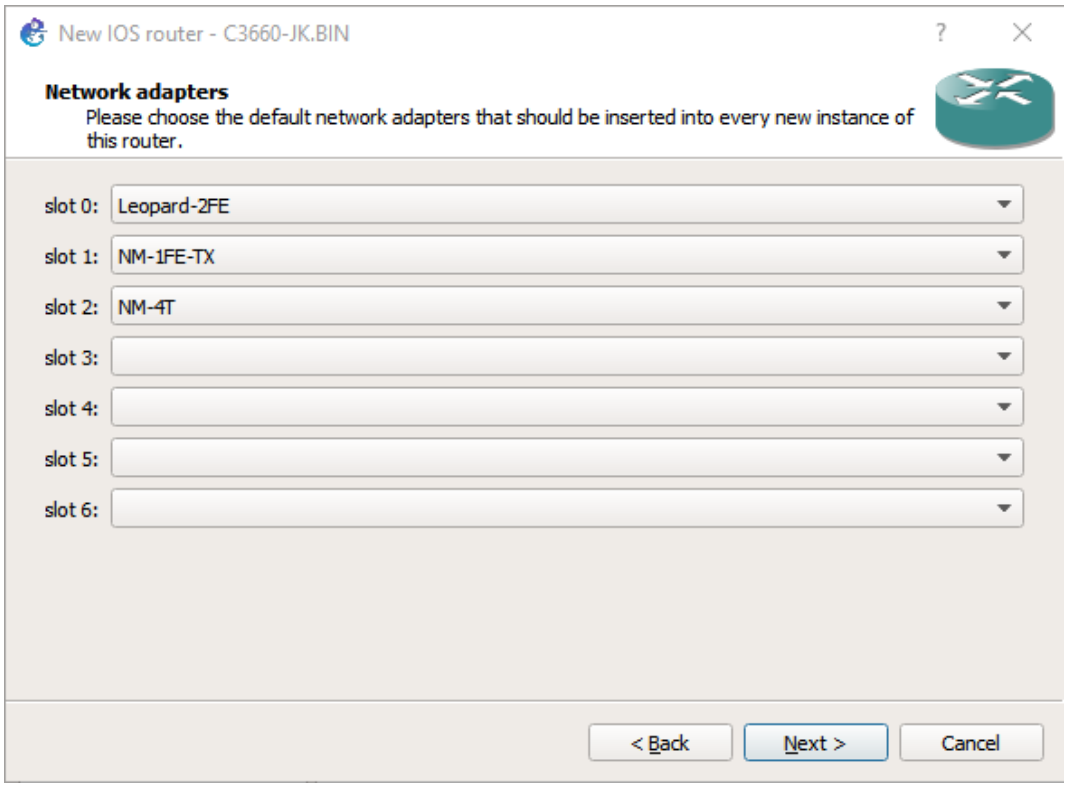


Figura 3. 1: Interfaces de red

Fuente: (GNS3 2018)

En este caso en particular brinda la opción de escoger ya sea una tarjeta de 2 puertos fastethernet, un módulo de red de 1 puerto fastethernet y finalmente un módulo de red de 4 puerto fastethernet.

GNS3 como valor agregado te permite simular ambientes virtuales como se ilustra en la figura 3.2, lo cual es una gran ventaja con respecto a otros simuladores. Puedes simular desde una máquina con sistema operativo Windows hasta un firewall o servidor web.

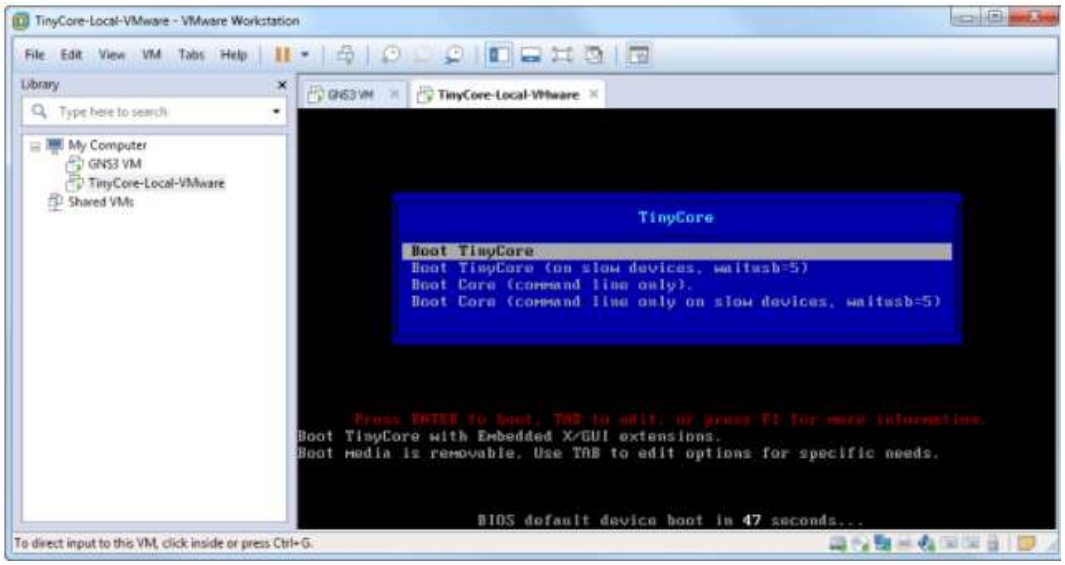


Figura 3. 2: Virtualización de dispositivos de red

Fuente: (GNS3 2018)

En lo que respecta a estabilidad, GNS3 establece parámetros mínimos para el correcto funcionamiento de los diseños a implementar. Los requerimientos básicos se los detalla en la tabla 3-2.

Tabla 3-2. Requisitos mínimos de instalación

Requisitos Mínimos	
Sistema Operativo	Windows 7 (64 bits) o versiones más recientes.
Procesador	2 o más núcleos lógicos
Virtualización	La virtualización de extensiones es requerida.
Memoria	4 GB de memoria RAM
Almacenamiento	1GB de espacio disponible.

Fuente: (GNS3 2018)

Las implementaciones en GNS3 se vuelven cada vez más sencillas gracias a la contribución de expertos que exponen sus casos de éxito, estos casos e información específica del funcionamiento de la plataforma se la puede encontrar en la sección de documentación, tal como se muestra en la figura 3.3.

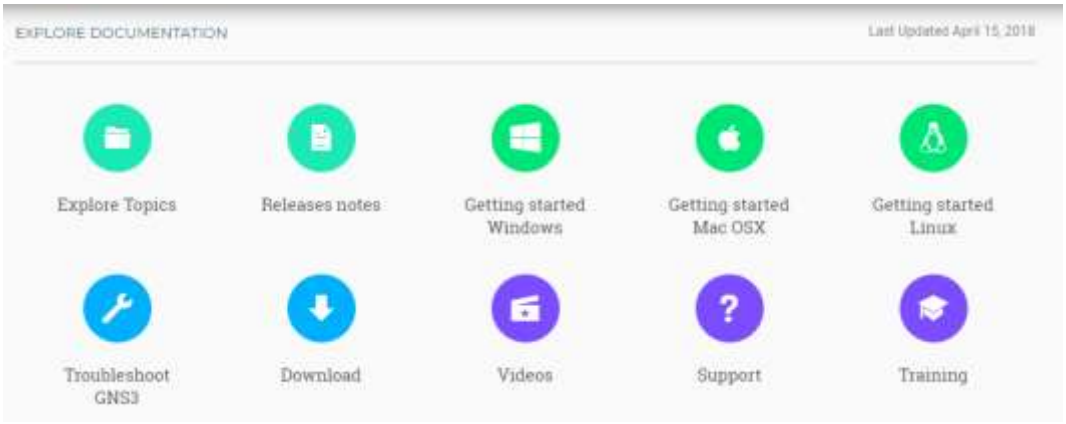


Figura 3. 3: Sección de documentación GNS3

Fuente: (GNS3 2018)

3.3. Diseño de la solución.

Para realizar un buen diseño es importante tener en cuenta las fases o ciclos de vida que tiene una red de servicios, este ciclo se resume en 6 siglas PPDIOO (Preparación, Planeación, Diseño, Implementación, Operación y Optimización) (Wilkins 2011). En razón de que este trabajo de titulación busca implementar la solución INTERAS opción C utilizando el simulador GNS3, se profundizará en 3 fases específicas que detallan los principios para alcanzar el objetivo propuesto del trabajo de titulación, estas fases son: Planeación, Diseño e Implementación.

Preparación

Es la fase de mayor relevancia debido a que es el inicio de un proyecto sustentado en un caso de negocio que conlleva el análisis financiero, la estrategia de red y la propuesta tecnológica para su desarrollo. En este caso, la estrategia es la

unificación de redes para continuidad de servicios y la propuesta tecnológica es utilizar Inter AS Opción C como solución para este caso de negocio.

Planeación

En esta fase se identifican los requerimientos tecnológicos de la solución, así como también la definición de recursos, responsables e hitos del proyecto. Esto permite evaluar los tiempos de ejecución de cada etapa del proyecto con información detallada de tareas y responsables que intervienen en el diseño e implementación de la solución.

Diseño

El diseño se basa en los requerimientos previamente definidos en fases anteriores pero con una notable diferencia, en esta fase se abarcan temas más específicos como por ejemplo el diagrama de red de la solución, el equipamiento a utilizar y el plan de acción que da paso a la fase de implementación.

Implementación

Esta fase abre paso a la instalación de la solución y la ejecución del plan trazado en fases previas. En caso de que exista algún cambio en el tiempo de ejecución de tareas o en la viabilidad del diseño, se debe imperiosamente convocar a reuniones de control de cambio donde se analicen y resuelvan las situaciones que obstaculizan el plan de acción previamente definido y adicionalmente se actualice en plan de trabajo con los nuevos tiempos de implementación.

Operación

Se enfoca en las tareas de administración, monitoreo y mantenimiento de la red. Esta fase es la prueba final del diseño y arroja resultados que permiten evaluar de

forma efectiva si el diseño es escalable y si permite adaptarse a las necesidades de los servicios que quiere brindar la empresa.

Optimización

Es la fase donde se buscan mejoras al diseño, esto se da luego de un largo tiempo de estabilización de la operación de la red. En muchos casos se centra en la optimización de los procesos que intervienen en la operación.

3.3.1. Planificación de infraestructura

Una vez validado el modelo de negocio en la fase de preparación y luego de haber establecido los acuerdos por las empresas participantes en el INTER AS, se debe iniciar la planeación de red. Esta planeación conlleva la definición de la topología de interconexión, nomenclatura de equipos, interfaces, direccionamiento ip, protocolos ip y los servicios que se pretenden brindar.

3.3.1.1. Topología de red.

Las empresas bajo acuerdos de confidencialidad comparten sus topologías de red para evaluar los puntos de interconexión entre las redes participantes en el INTER AS y a su vez tener visibilidad de las características, funcionalidades, fortalezas y debilidades en la infraestructura de red de cada empresa.

Luego de las validaciones respectivas, se estableció la topología de interconexión física que se muestra en la figura 3.4

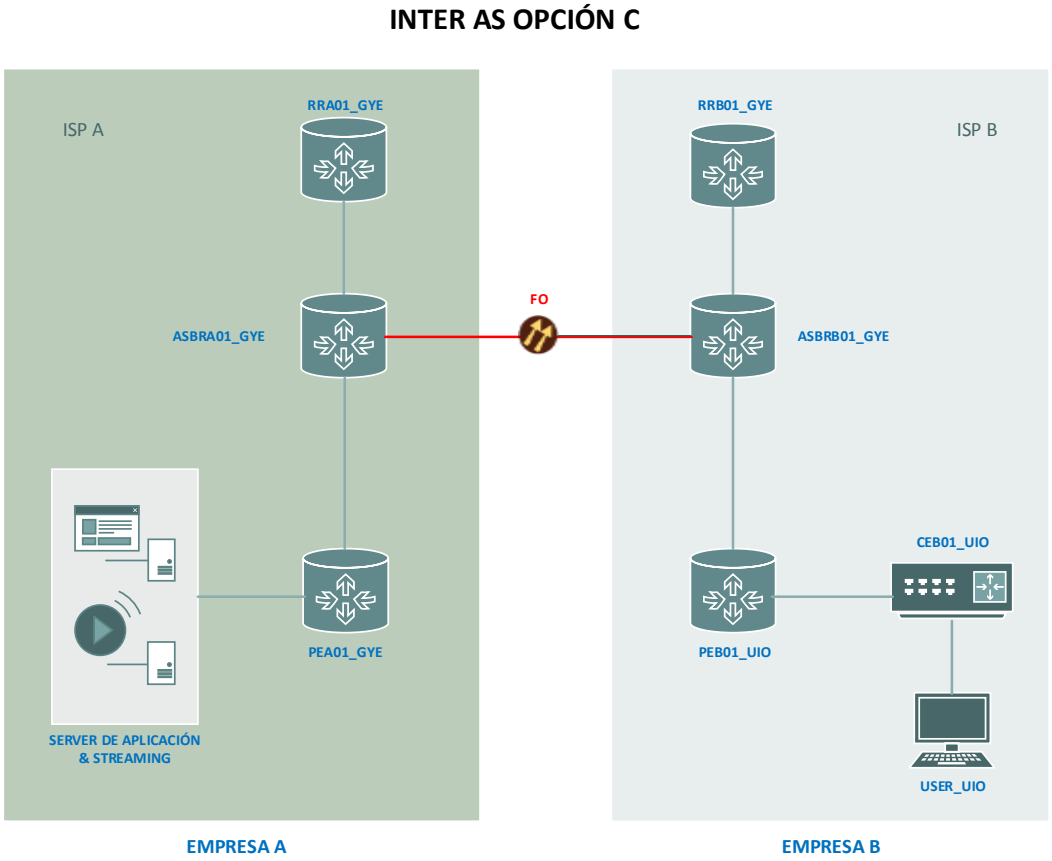


Figura 3. 4: Topología física Inter AS Opción C

Fuente: Autor 2018

En la topología se detallan los equipos principales que intervienen en el INTER-AS tanto para la empresa A como para a empresa B. En el desarrollo del caso de estudio se demostrará la conectividad extremo a extremo entre el usuario de la empresa B y el servidor de aplicación de la empresa A.

3.3.1.2. Nomenclatura de los equipos de red.

Las mejores prácticas dictan que la nomenclatura es uno de los pilares fundamentales para el administrador de red en lo que respecta al diseño e implementación de la topología de red.

Muchos de los errores en la planeación de las topologías de red en la que intervienen una gran cantidad de equipos es precisamente la nomenclatura. Por lo cual se requiere tener en cuenta parámetros de identificación necesarios, como por

ejemplo: el rol del equipo en la red, la localidad en la que está instalado el equipo y un número de identificación de 2 dígitos.

En la tabla 3-3 se detalla el formato de la nomenclatura asignada a los equipos del ISP A:

Tabla 3-1. Identificadores de red ISP A

ASBR	A	01	GYE
IDENTIFICADOR 1	IDENTIFICADOR 2	IDENTIFICADOR 3	IDENTIFICADOR 4

Fuente: Autor

Identificador 1: Funcionalidad de equipo en la topología de red.

Identificador 2: Nombre del ISP en este caso A.

Identificador 3: Secuencia numérica de los equipos.

Identificador 4: Localidad en la que se encuentra instalado el equipo.

En base a este formato, se describe en la tabla 3-4 la nomenclatura de los equipos pertenecientes al ISP A.

Tabla 3-2. Identificadores de red ISP A

Nomenclatura	Descripción
RRA01_GYE	Route Reflector ISP A Guayaquil
ASBRA01_GYE	Autonomous System Router ISP A Guayaquil
PEA01_GYE	Provider Edge ISP A Guayaquil

Fuente: Autor

En la tabla 3-5 se detalla el formato de los equipos pertenecientes al ISP B:

Tabla 3-3. Identificadores de red ISP B

ASBR	B	01	GYE
IDENT 1	IDENT 2	IDENT 3	IDENT 4

Fuente: Autor

Identificador 1: Funcionalidad de equipo en la topología de red.

Identificador 2: Nombre del ISP en este caso B.

Identificador 3: Secuencia numérica de los equipos.

Identificador 4: Localidad en la que se encuentra instalado el equipo.

La descripción de los equipos del ISP B se detallan en la tabla 3-6, la cual es presentada a continuación:

Tabla 3-4. Nomenclatura de los equipos red ISP B

Nomenclatura	Descripción
RRB01_GYE	Route Reflector ISP B Guayaquil
ASBRB01_GYE	Autonomous System Router ISP B Guayaquil
PEB01_UIO	Provider Edge ISP B Quito
CEB01_UIO	Customer Edge ISP B Quito

Fuente: Autor

3.3.1.3. Direccionamiento IP

Para asegurar el correcto funcionamiento de la red y brindar escalabilidad a la hora de incrementar equipamiento, enlaces, interconexiones o número de clientes, es importante hacer una buena planificación del direccionamiento IP.

Lo más importante a la hora de planificar el direccionamiento IP, es conocer el plan estratégico o de expansión de la empresa a corto y a largo plazo. El direccionamiento IP es la base de una red de servicios, la mala planificación conlleva riesgos futuros en la continuidad de servicios que se ven reflejados en grandes pérdidas económicas para las empresas.

En la figura 3.5 se puede observar la topología de la interconexión con el direccionamiento IP asignado a cada enlace de red.

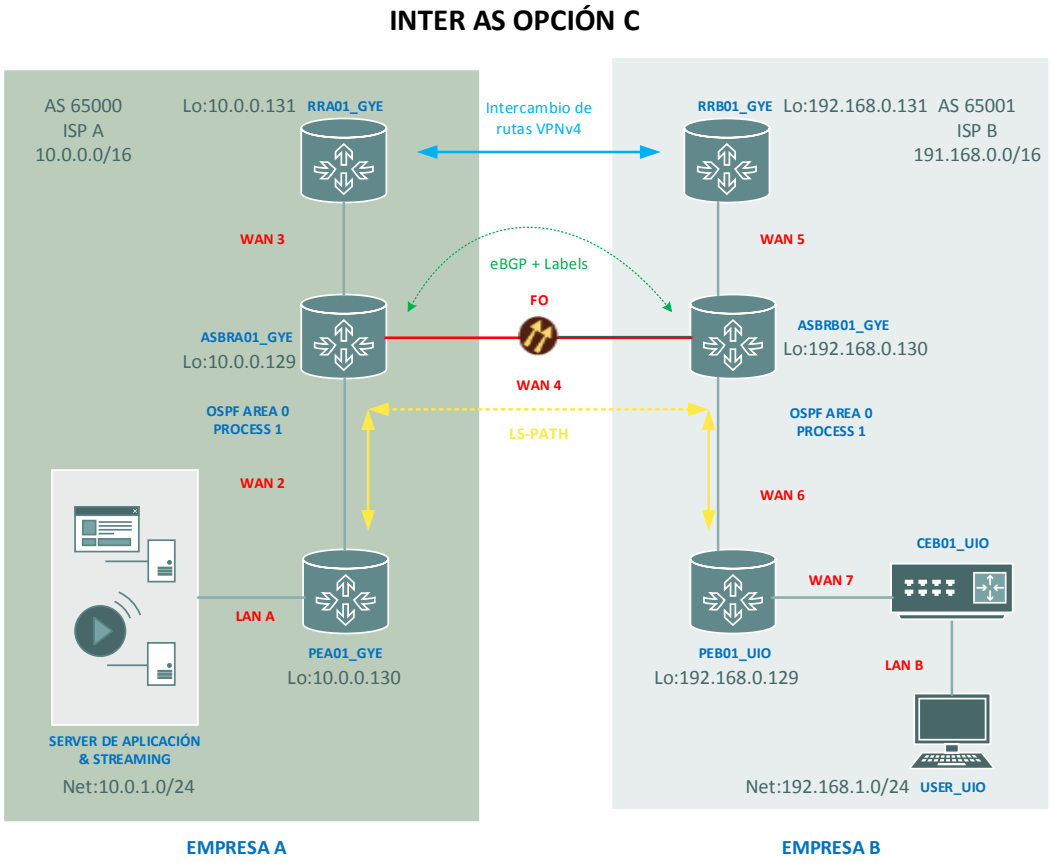


Figura 3. 5: Topología Inter AS Opción C con direccionamiento IP

Fuente: Autor 2018

Se observa que dentro de la planificación de red de la empresa A, se consideró una red tipo C para una granja de servidores de contenido. La visión de esta empresa es brindar a sus abonados, servicios de valor agregado como por ejemplo: video streaming, facturación electrónica o demás servicios de entretenimiento o de

utilidad al abonado. El detalle del direccionamiento es presentado en la tabla 3-7 y muestra el direccionamiento utilizado en la red del ISP A.

Tabla 3-5. Direccionamiento de red del ISP A

ISP A	
LAN	10.0.1.0/24
WAN 2	10.0.0.4/30
WAN 3	10.0.0.8/30
WAN 4	10.0.0.12/30
LoopBack PEA	10.0.0.130
LoopBack PA	10.0.0.129
LoopBack RRA	10.0.0.131

Fuente: Autor

La planificación de red del ISP B fue hecha para brindar servicios de internet a los abonados a nivel nacional, la visión es un poco distinta a la primera empresa debido a que, si bien es cierto que el direccionamiento de red permite la adhesión de nuevos equipos al backbone IP para expandirse a nivel nacional, a diferencia de la otra empresa no hay direccionamiento reservado para servidores de contenido que brinden al abonado servicios de valor agregado.

El direccionamiento del ISP B es detallado en la tabla 3-8, esta tabla refleja el direccionamiento utilizado en los enlaces de red del ISP B.

Tabla 3-6. Direccionamiento de red del ISP B

ISP A	
LAN	10.0.1.0/24
WAN 2	10.0.0.4/30
WAN 3	10.0.0.8/30
WAN 4	10.0.0.12/30
LoopBack PEA	10.0.0.130
LoopBack PA	10.0.0.129
LoopBack RRA	10.0.0.131

Fuente: Autor

3.3.2. Definición de interfaces y enlaces de red.

Como parte de la planificación de red, es importante definir el tipo de interfaces que utilizan los equipos para interconectarse entre sí. Al igual que el direccionamiento IP, la planificación depende de la visión a corto y a largo plazo de las empresas.

El no planificar correctamente la red de servicio, incurrirá en gastos de inversión relacionados a equipamientos y recursos de red que disminuyen la rentabilidad de la inversión. Por ejemplo, si una empresa concibe que en 5 años va a traficar por su red un estimado de 50 Mbps y al primer año ya tiene el 80% de ocupación de sus enlaces, quiere decir que la planificación no estuvo acorde con la estrategia de mercado de la empresa.

Para esta simulación se consideran interfaces de prueba, las cuales se detallan en las tablas 3-9 y 3-10, estas tablas describen el tipo de interface y la nomenclatura utilizada en los equipos del ISP A y el ISP B respectivamente.

Tabla 3-7. Interfaces de red del ISP A

ISP A			
Equipo	**Interface**	**Tasa de transmisión**	**Descripción**
RRA01_GYE	Loopback0	Interface Lógica	Loopback_RRA
RRA01_GYE	FastEthernet0/1	100 Mbps	TO_ASBRA
ASBRA01_GYE	Loopback0	Interface Lógica	Loopback_ASBRA
ASBRA01_GYE	FastEthernet0/0	100 Mbps	TO_ASBRB
ASBRA01_GYE	FastEthernet0/1	100 Mbps	TO_RRA
ASBRA01_GYE	FastEthernet1/0	100 Mbps	TO_PEA
PEA01_GYE	Loopback0	Interface Lógica	Loopback_PEA
PEA01_GYE	FastEthernet1/0	100 Mbps	TO_ASBRA
PEA01_GYE	FastEthernet2/0	100 Mbps	TO_SERVER

Fuente: Autor

Tabla 3-8. Interfaces de red del ISP B

ISP B			
Equipo	Interface	Tasa de transmisión	Descripción
RRB01_GYE	Loopback0	Interface Lógica	Loopback_RRB
RRB01_GYE	FastEthernet0/1	100 Mbps	TO_ASBRB
ASBRB01_GYE	Loopback0	Interface Lógica	Loopback_ASBRB
ASBRB01_GYE	FastEthernet0/0	100 Mbps	TO_ASBRA
ASBRB01_GYE	FastEthernet0/1	100 Mbps	TO_RRB
ASBRB01_GYE	FastEthernet1/0	100 Mbps	TO_PEB
PEB01_UIO	Loopback0	Interface Lógica	Loopback_PEB
PEB01_UIO	FastEthernet1/0	100 Mbps	TO_ASBRB
PEB01_UIO	FastEthernet2/0	100 Mbps	TO_CEB
CEB01_UIO	FastEthernet0/0	100 Mbps	TERMINAL_SERVER

Fuente: Autor

De igual manera es importante conocer la correspondencia tanto en la capa de enlace como en la capa de red de los equipos que intervienen en el INTER AS. La tabla 3-11 resume la conectividad de los equipos a nivel lógico.

Tabla 3-9. IPs en los enlaces de red

ORIGEN			DESTINO		
Equipo	Interface	Dirección IP	Equipo	Interface	Dirección IP
RRA01_GYE	FastEthernet0/1	10.0.0.10	ASBRA01_GYE	FastEthernet0/1	10.0.0.9
ASBRA01_GYE	FastEthernet0/0	10.0.0.13	ASBRB01_GYE	FastEthernet0/0	10.0.0.14
ASBRA01_GYE	FastEthernet1/0	10.0.0.6	PEA01_GYE	FastEthernet1/0	10.0.0.5
PEA01_GYE	FastEthernet2/0	10.0.0.2	TO_SERVER	FastEthernet2/0	10.0.0.10
RRB01_GYE	FastEthernet0/1	192.168.0.2	ASBRB01_GYE	FastEthernet0/1	192.168.0.1
ASBRB01_GYE	FastEthernet1/0	192.168.0.5	PEB01_UIO	FastEthernet1/0	192.168.0.6
PEB01_UIO	FastEthernet2/0	192.168.0.9	CEB01_UIO	FastEthernet2/0	192.168.0.10
CEB01_UIO	FastEthernet0/0	192.168.1.1	TERMINAL_SERVER	eth0	10.0.1.1

Fuente: Autor

3.3.3. Configuraciones iniciales

En todo proceso es importante establecer el orden de las cosas y para este caso en particular el ordenamiento de las configuraciones. Dentro de las configuraciones iniciales se destacan el hostname o nombre del equipo, interfaces con sus

respectivas IPs y usuarios de administrador en caso de existir. Estas configuraciones se detallan en las tablas 3-12, 3-13, 3-14, 3-15 y en la figura 3.6.

Tabla 3-10. Configuraciones iniciales Route Reflectors

RRA01_GYE	RRB01_GYE
! hostname RRA ! ip cef ! ! no ip domain lookup ! ! interface Loopback0 description Loopback_RRA ip address 10.0.0.131 255.255.255.255 ! ! interface FastEthernet0/1 description TO_ASBRA ip address 10.0.0.10 255.255.255.252 ! ! no ip http server no ip http secure-server ! ! control-plane ! ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous line aux 0 exec-timeout 0 0 privilege level 15 logging synchronous line vty 0 4 login !	! hostname RRB ! ip cef ! ! no ip domain lookup ! ! interface Loopback0 description Loopback_RRB ip address 192.168.0.131 255.255.255.255 ! ! interface FastEthernet0/1 description TO_ASBRB ip address 192.168.0.2 255.255.255.252 ! ! no ip http server no ip http secure-server ! ! control-plane ! ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous line aux 0 exec-timeout 0 0 privilege level 15 logging synchronous line vty 0 4 login !

Fuente: Autor

Tabla 3-11. Configuraciones iniciales ASBRs

ASBRA01_GYE	ASBRB01_GYE
!	!
hostname ASBRA	hostname ASBRB
!	!
ip cef	ip cef
!	!
!	!
no ip domain lookup	no ip domain lookup
!	!
!	!
interface Loopback0	interface Loopback0
description Loopback_ASBRA	description Loopback_ASBRB
ip address 10.0.0.129 255.255.255.255	ip address 192.168.0.130 255.255.255.255
!	!
interface FastEthernet0/0	interface FastEthernet0/0
description TO_ASBRB	description TO_ASBRA
ip address 10.0.0.13 255.255.255.252	ip address 10.0.0.14 255.255.255.252
!	!
!	!
interface FastEthernet0/1	interface FastEthernet0/1
description TO_RRA	description TO_RRB
ip address 10.0.0.9 255.255.255.252	ip address 192.168.0.1 255.255.255.252
!	!
!	!
interface FastEthernet1/0	interface FastEthernet1/0
description TO_PEA	description TO_PEB
ip address 10.0.0.6 255.255.255.252	ip address 192.168.0.5 255.255.255.252
!	!
no ip http server	no ip http server
no ip http secure-server	no ip http secure-server
!	!
!	!
line con 0	line con 0
exec-timeout 0 0	exec-timeout 0 0
privilege level 15	privilege level 15
logging synchronous	logging synchronous
line aux 0	line aux 0
exec-timeout 0 0	exec-timeout 0 0
privilege level 15	privilege level 15
logging synchronous	logging synchronous
line vty 0 4	line vty 0 4
login	login

! ! end	! ! end

Fuente: Autor

Tabla 3-12. Configuraciones iniciales PEs

PEA01_GYE	PEB01_UIO
! hostname PEA ! ip cef ! ! no ip domain lookup ! ! interface Loopback0 description Loopback_PEA ip address 10.0.0.130 255.255.255.255 ! ! interface FastEthernet1/0 description TO_ASBRA ip address 10.0.0.5 255.255.255.252 ! ! interface FastEthernet2/0 description TO_SERVER ip address 10.0.0.2 255.255.255.252 ! no ip http server no ip http secure-server ! ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous line aux 0 exec-timeout 0 0 privilege level 15 logging synchronous	! hostname PEB ! ip cef ! ! no ip domain lookup ! ! interface Loopback0 description Loopback_PEB ip address 192.168.0.129 255.255.255.255 ! ! interface FastEthernet1/0 description TO_ASBRB ip address 192.168.0.6 255.255.255.252 ! interface FastEthernet2/0 description TO_CEB ip address 192.168.0.9 255.255.255.252 ! no ip http server no ip http secure-server ! ! line con 1 exec-timeout 0 1 privilege level 16 logging synchronous line aux 1 exec-timeout 0 1 privilege level 16 logging synchronous

line vty 0 4 login ! ! end	line vty 0 5 login ! ! end

Fuente: Autor

Tabla 3-13. Configuraciones iniciales CEs

CEA01_GYE	CEB01_UIO
! hostname CEA ! ip cef ! ! no ip domain lookup ! ! username cisco privilege 15 password 0 cisco ! ! interface Loopback0 description SERVER_HTTP ip address 10.0.1.1 255.255.255.0 ! ! interface FastEthernet2/0 description TO_PEA ip address 10.0.0.1 255.255.255.252 ! ip route 0.0.0.0 0.0.0.0 10.0.0.2 name DEFAULT ! ! ip http server ip http authentication local ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous	! hostname CEB ! ip cef ! ! no ip domain lookup ! ! ! interface FastEthernet0/0 description TERMINAL_SERVER ip address 192.168.1.1 255.255.255.0 ! ! interface FastEthernet2/0 description To_PEB ip address 192.168.0.10 255.255.255.252 ! ip route 0.0.0.0 0.0.0.0 192.168.0.9 name DEFAULT ! ! no ip http server no ip http secure-server ! line con 0 exec-timeout 0 0 privilege level 15 logging synchronous

line aux 0 exec-timeout 0 0 privilege level 15 logging synchronous line vty 0 4 login ! ! end	line aux 0 exec-timeout 0 0 privilege level 15 logging synchronous line vty 0 4 login ! ! end

Fuente: Autor

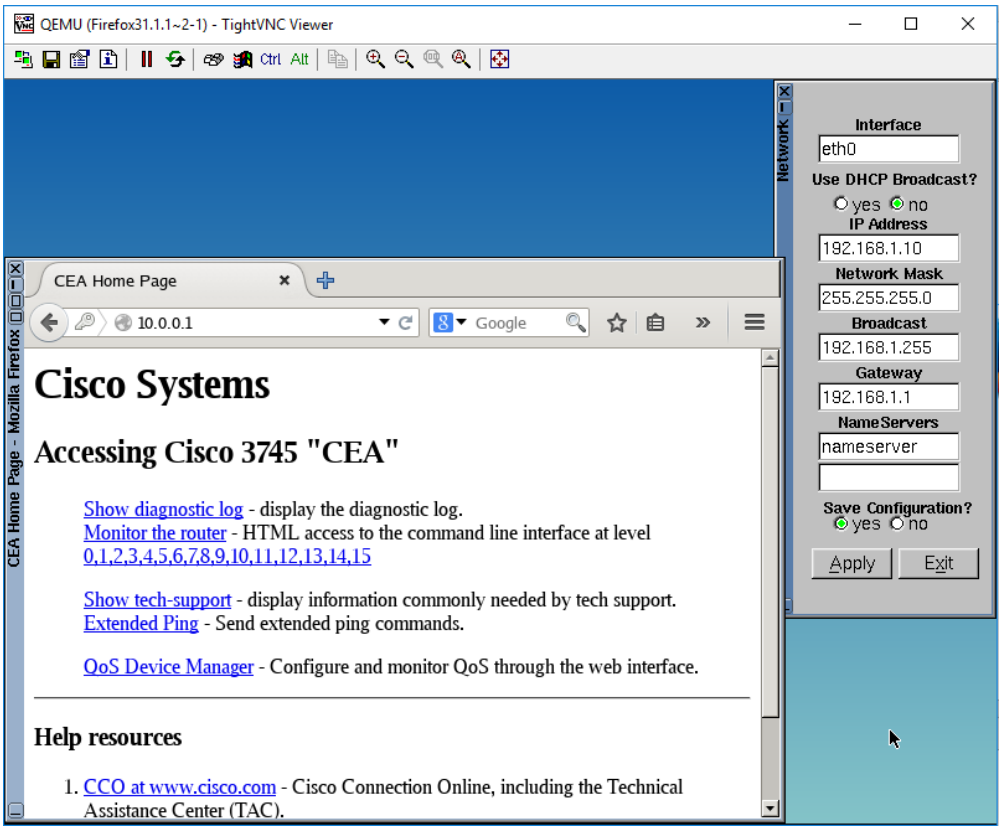


Figura 3. 6: Configuración de red del terminal server

Fuente: Autor

Estas son las configuraciones base con las cuales los equipos tienen conectividad a nivel de enlace punto a punto. Una vez comprobada la conectividad entre los equipos, la red está preparada para realizar las configuraciones de enrutamiento y servicios.

3.3.4. Configuración del IGP, MPLS e Inter AS opción C

En las redes de los 2 ISPs utilizan como IGP el protocolo de enrutamiento OSPF. En las tablas 3-16, 3-17 y 3-18 se detallan dichas configuraciones.

Tabla 3-14. Configuración del IGP en los Route Reflectors

RRA01_GYE	RRB01_GYE
! router ospf 1 log-adjacency-changes network 10.0.0.8 0.0.0.3 area 0 network 10.0.0.131 0.0.0.0 area 0 !	! router ospf 1 log-adjacency-changes network 192.168.0.0 0.0.0.3 area 0 network 192.168.0.131 0.0.0.0 area 0 !

Fuente: Autor

Tabla 3-15. Configuración del IGP en los ASBRs

ASBRA01_GYE	ASBRB01_GYE
! router ospf 1 log-adjacency-changes redistribute static subnets redistribute bgp 65000 subnets network 10.0.0.4 0.0.0.3 area 0 network 10.0.0.8 0.0.0.3 area 0 network 10.0.0.129 0.0.0.0 area 0 !	! router ospf 1 log-adjacency-changes redistribute static subnets redistribute bgp 65001 subnets network 192.168.0.0 0.0.0.3 area 0 network 192.168.0.4 0.0.0.3 area 0 network 192.168.0.130 0.0.0.0 area 0 !

Fuente: Autor

Tabla 3-16. Configuración del IGP en los PEs

PEA01_GYE	PEB01_UIO
! router ospf 1 log-adjacency-changes network 10.0.0.0 0.0.0.3 area 0 network 10.0.0.4 0.0.0.3 area 0 network 10.0.0.130 0.0.0.0 area 0 !	! router ospf 1 log-adjacency-changes network 192.168.0.4 0.0.0.3 area 0 network 192.168.0.129 0.0.0.0 area 0 ! !

Fuente: Autor

Para verificar que las sesiones OSPF están activas entre los equipos vecinos, se ingresa el comando “sh ip ospf neighbor” en la consola de administración de los equipos, ejemplo:

ASBRA#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.0.0.131	1	FULL/DR	00:00:33	10.0.0.10	FastEthernet0/1
10.0.0.130	1	FULL/DR	00:00:32	10.0.0.5	FastEthernet1/0

ASBRB#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.0.129	1	FULL/BDR	00:00:38	192.168.0.6	FastEthernet1/0
192.168.0.131	1	FULL/DR	00:00:39	192.168.0.2	FastEthernet0/1

PEA#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
10.0.0.129	1	FULL/BDR	00:00:32	10.0.0.6	FastEthernet1/0

PEB#sh ip ospf neighbor

Neighbor ID	Pri	State	Dead Time	Address	Interface
192.168.0.130	1	FULL/DR	00:00:30	192.168.0.5	FastEthernet1/0

Una vez establecidas las vecindades, se configura MPLS en las redes para etiquetar lo paquetes y que la conmutación de paquetes no sea por IP sino por etiquetas/labels. En las tablas 3-19 y 3-20 se detallan las configuraciones en los equipos.

Tabla 3-17. Configuración del MPLS en los ASBRs

ASBRA01_GYE	ASBRB01_GYE
! mpls label protocol ldp ! ! interface FastEthernet1/0 description TO_PEA ip address 10.0.0.6 255.255.255.252 duplex auto speed auto mpls label protocol ldp mpls ip !	! mpls label protocol ldp ! ! interface FastEthernet1/0 description TO_PEB ip address 192.168.0.5 255.255.255.252 duplex auto speed auto mpls label protocol ldp mpls ip !

Fuente: Autor

Tabla 3-18. Configuración del MPLS en los PEs

PEA01_GYE	PEB01_UIO
! mpls label protocol ldp ! ! interface FastEthernet1/0 description TO_ASBRA ip address 10.0.0.5 255.255.255.252 mpls label protocol ldp mpls ip !	! mpls label protocol ldp ! ! interface FastEthernet1/0 description TO_ASBRB ip address 192.168.0.6 255.255.255.252 mpls label protocol ldp mpls ip !

Fuente: Autor

Para finalizar la preparación de la red antes de la configuración de un servicio, es necesario realizar las configuraciones del INTER AS Opción C, esto consiste en configurar las sesiones BGP+label entre los ASBRs y las sesiones MP-BGP entre los RRs de los 2 ISPs. Las configuraciones se resumen en las tablas 3-21 y 3-22.

Tabla 3-19. Configuración Inter AS opción C en ASBRs

ASBRA01_GYE	ASBRB01_GYE
!	!
router bgp 65000	router bgp 65001
no synchronization	no synchronization
bgp router-id 10.0.0.129	bgp router-id 192.168.0.130
bgp log-neighbor-changes	bgp log-neighbor-changes
network 10.0.0.130 mask 255.255.255.255	network 192.168.0.129 mask 255.255.255.255
neighbor 10.0.0.14 remote-as 65001	neighbor 10.0.0.13 remote-as 65000
neighbor 10.0.0.14 send-label	neighbor 10.0.0.13 send-label
no auto-summary	no auto-summary
!	!
ip route 192.168.0.131 255.255.255.255 10.0.0.14 name TO_RRB	ip route 10.0.0.131 255.255.255.255 10.0.0.13 name TO_RRA
!	!

Fuente: Autor

Tabla 3-20. Configuración Inter AS opción C en Route Reflectors

RRA01_GYE	RRB01_GYE
!	!
router bgp 65000	router bgp 65001
no synchronization	no synchronization
bgp router-id 10.0.0.131	bgp router-id 192.168.0.131
bgp log-neighbor-changes	bgp log-neighbor-changes
neighbor 10.0.0.130 remote-as 65000	neighbor 10.0.0.131 remote-as 65000
neighbor 10.0.0.130 update-source Loopback0	neighbor 10.0.0.131 ebgp-multihop 10
neighbor 10.0.0.130 route-reflector-client	neighbor 10.0.0.131 update-source Loopback0
neighbor 10.0.0.130 soft-reconfiguration inbound	neighbor 192.168.0.129 remote-as 65001
neighbor 192.168.0.131 remote-as 65001	neighbor 192.168.0.129 update-source Loopback0
neighbor 192.168.0.131 ebgp-multihop 10	neighbor 192.168.0.129 route-reflector-client
neighbor 192.168.0.131 update-source Loopback0	neighbor 192.168.0.129 soft-reconfiguration inbound
no auto-summary	no auto-summary
!	!
address-family vpnv4	address-family vpnv4
neighbor 10.0.0.130 activate	neighbor 10.0.0.131 activate
neighbor 10.0.0.130 send-community both	neighbor 10.0.0.131 send-community both
neighbor 10.0.0.130 route-reflector-client	neighbor 10.0.0.131 next-hop-unchanged
neighbor 192.168.0.131 activate	neighbor 192.168.0.129 activate
neighbor 192.168.0.131 send-community both	neighbor 192.168.0.129 send-community both
neighbor 192.168.0.131 next-hop-unchanged	neighbor 192.168.0.129 route-reflector-client
exit-address-family	exit-address-family
!	!

Fuente: Autor

3.4. Configuración de un servicio VPN de capa 3 sobre el Inter AS

La finalidad del Inter As opción C es establecer servicios extremo a extremo entre 2 dominios IP MPLS, en este caso la comunicación se establece entre un terminal server del dominio IP MPLS del ISP A y un HTTP (Hypertext Transfer Protocol) server del dominio IP MPLS del ISP B.

Para comprobar la continuidad de los servicios en estas redes, se plantea la configuración de una VPN de capa 3 llamadas VRF SERVER. La VRF SERVER se la configura en tanto en el PEA01_GYE y en el PEB01_UIO respectivamente. En la tabla 3-23 se detalla la configuración de la VRF.

Tabla 3-21. Configuración de VRF SERVER en los PEs

PEA01_GYE	PEB01_UIO
!	!
ip vrf SERVER	ip vrf SERVER
rd 100:100	rd 100:100
route-target export 100:101	route-target export 100:101
route-target import 100:101	route-target import 100:101
!	!
interface FastEthernet2/0	interface FastEthernet2/0
description TO_SERVER	description TO_CEB
ip vrf forwarding SERVER	ip vrf forwarding SERVER
ip address 10.0.0.2 255.255.255.252	ip address 192.168.0.9 255.255.255.252
!	!
router bgp 65000	router bgp 65001
no synchronization	no synchronization
bgp router-id 10.0.0.130	bgp router-id 192.168.0.129
bgp log-neighbor-changes	bgp log-neighbor-changes
neighbor 10.0.0.131 remote-as 65000	neighbor 192.168.0.131 remote-as 65001
neighbor 10.0.0.131 update-source Loopback0	neighbor 192.168.0.131 update-source Loopback0
neighbor 10.0.0.131 soft-reconfiguration inbound	neighbor 192.168.0.131 soft-reconfiguration inbound
no auto-summary	no auto-summary
!	!
address-family vpnv4	address-family vpnv4
neighbor 10.0.0.131 activate	neighbor 192.168.0.131 activate
neighbor 10.0.0.131 send-community both	neighbor 192.168.0.131 send-community both
exit-address-family	exit-address-family

! address-family ipv4 vrf SERVER redistribute connected redistribute static no synchronization exit-address-family ! ip route vrf SERVER 10.0.1.0 255.255.255.0 10.0.0.1 name HTTP_SERVER !	! address-family ipv4 vrf SERVER redistribute connected redistribute static no synchronization exit-address-family ! ip route vrf SERVER 192.168.1.0 255.255.255.0 192.168.0.10 name TERMINAL_SERVER !

Fuente: Autor

Luego de la configuración del servicio VPN, se comprueba que las rutas VPNv4 tanto del HTTP server del ISP A como del Terminal Server del ISP A pertenezcan a la misma instancia de ruteo. Esto se lo puede corroborar ingresando el comando "sh ip route vrf SERVER" en los PEs:

PEA#sh ip route vrf SERVER

Routing Table: SERVER
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
C 10.0.0.0/30 is directly connected, FastEthernet2/0
S 10.0.1.0/24 [1/0] via 10.0.0.1
192.168.0.0/30 is subnetted, 1 subnets
B 192.168.0.8 [200/0] via 192.168.0.129, 00:25:14

```
B    192.168.1.0/24 [200/0] via 192.168.0.129, 00:25:14
```

```
PEB#sh ip route vrf SERVER

Routing Table: SERVER
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks
B       10.0.0.0/30 [200/0] via 10.0.0.130, 00:23:30
B       10.0.1.0/24 [200/0] via 10.0.0.130, 00:23:30
     192.168.0.0/30 is subnetted, 1 subnets
C       192.168.0.8 is directly connected, FastEthernet2/0
S    192.168.1.0/24 [1/0] via 192.168.0.10
```

Luego de comprobar que en los PEs de los ISPs se aprenden las rutas VPNv4 de los equipos que requieren conexión, resta probar conectividad entre ellos. En la figura 3. 7 se observa la prueba de PING entre el terminal server (usuario final del ISP B en UIO) y el Web server que es representado por un acceso HTTP en un router cisco.

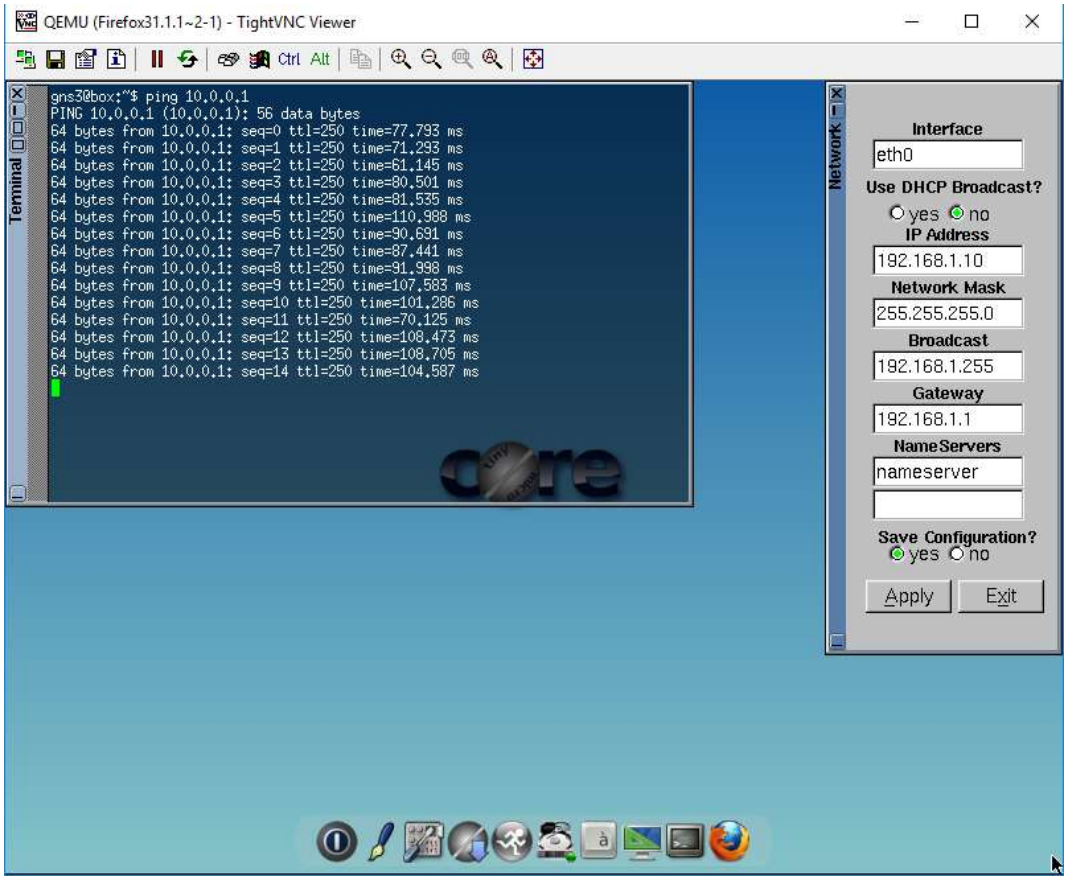


Figura 3. 7: Prueba de PING al Web Server ISP A

Fuente: Autor

Esta prueba válida la conectividad a nivel de capa 3, lo que significa que la comunicación está establecida de forma bidireccional para que los equipos envíen y reciban paquetes ip.

En la figura 3.8 finalmente es presentado el portal HTTP que se fue configurado en el router cisco para demostrar que la capa de Aplicación del modelo OSI está operando.

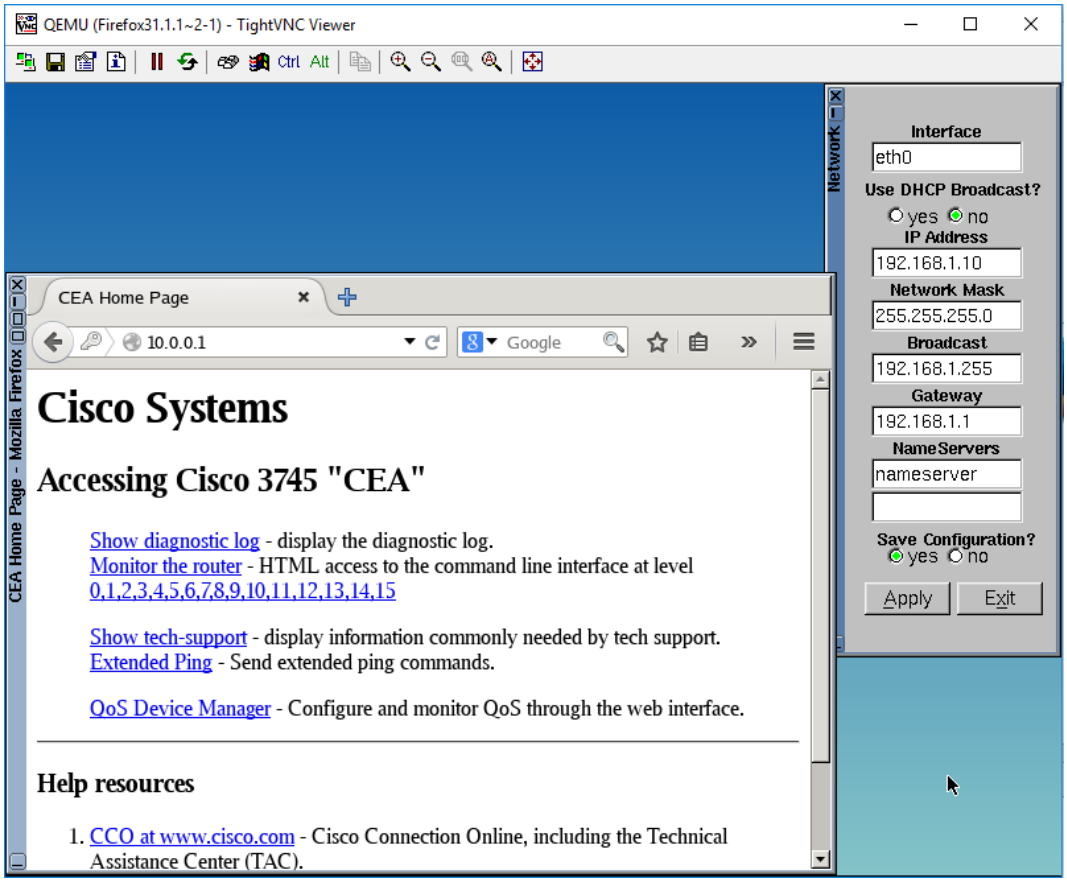


Figura 3. 8: Acceso HTTP al Web Server ISP A

Fuente: Autor

Conclusiones

- Se detallaron los fundamentos teóricos del Inter As que permiten al lector desarrollar las destrezas necesarias para implementar este tipo de soluciones a sus redes de datos.

- Se utilizaron las mejores prácticas de diseño para esquematizar y simular el Inter AS opción C. Queda demostrado que la metodología PPDIOO es la mejor forma de diseñar una solución.

- Las especificaciones de diseño, los diagramas y planificación de las redes simuladas de los ISPs en este trabajo, permiten ejemplificar cualquier topología MPLS y más aún replicar la solución Inter As en este tipo de redes.

- El éxito de la simulación y la constatación de la continuidad del servicio VPNL3 a través de los dominios MPLS, validan los objetivos específicos del proyecto y por ende confirman que se ha cumplido el objetivo general de este trabajo.

  .

Recomendaciones

- Realizar un estudio que monetice la solución Inter As aplicado a la innovación de redes MPLS.

- Dar a conocer esta tecnología a las empresas del Ecuador por medio de un integrador tecnológico. Cabe recalcar que es importante realizar un estudio de mercado y un caso de negocio para brindar la solución como un producto.

- Es importante realizar un estudio adicional que permita medir los ahorros en infraestructura que el Inter AS opción C puede llegar a brindar.

Referencias Bibliográficas

C. S. (2014). *Cisco CPT Configuration Guide–CTC and Documentation Release 9.5.x and Cisco IOS Release 15.2(01).* San Jose, CA.

Cisco Systems Inc. (2013). *Carrier Ethernet 2.0 Certification Understanding and Layer 2 Control Protocol Behaviour Across Cisco Carrier Ethernet Platforms.* San Jose, CA: Cisco Systems Inc.

CiscoSystems. (2015). *Carrier Ethernet Configuration Guide, Cisco IOS Release 15S.* San Jose, CA.

GNS3. (2017). Obtenido de https://gns3.com/

Green, H., Monette, S., Olsson, J., Saltsidis, P., & Takács, A. (2007). *Carrier Ethernet: The native approach.* Ericsson.

Industry Authors. (2016). *An Industry Initiative for Third Generation Network and Services.* Metro Ethernet Forum.

MEF. (2004). *Introduction to Circuit Emulation Services over Ethernet.* Metro Ethernet Forum.

MEF. (2004). *MEF 11 User Network Interface (UNI) Requirements and Framework.* Metro Ethernet Forum.

MEF. (2004). *MEF 4 Metro Ethernet Network Architecture Framework - Part 1: Generic Framework.* Metro Ethernet Forum.

MEF. (2010). *Understanding Carrier Ethernet Throughput.* Metro Ethernet Forum.

MEF. (2012). *MEF 33 Ethernet Access Services Definition.* Metro Ethernet Forum.

MEF. (2013). *CE 2.0 Ethernet Access Services.* Metro Ethernet Forum.

MEF. (2013). *MEF 10.3 Ethernet Services Attributes Phase 3.* Metro Ethernet Forum.

MEF. (2014). *Carrier Ethernet and SDN Part 1 : An Industry Perspective.* Metro Ethernet Forum.

MEF. (2014). *Carrier Ethernet and SDN Part 2: Practical Considerations.* Metro Ethernet Forum.

MEF. (2014). *MEF 12.2 Carrier Ethernet Network Architecture Framework Part 2: Ethernet Services Layer.* Metro Ethernet Forum.

MEF. (2014). *MEF 6.2 EVC Ethernet Services Definitions Phase 3.* Metro Ethernet Forum.

MEF. (2016). *MEF 23.2 Carrier Ethernet Class of Service – Phase 3.* Metro Ethernet Forum.

MEF. (2016). *MEF 26.2 External Network Network Interfaces (ENNI) and Operator Service Attributes.* Metro Ethernet Forum.

MEF. (2016). *Understanding Carrier Ethernet Service Assurance Part 1.* Metro Ethernet Forum.

MEF. (2016). *Understanding Carrier Ethernet Service Assurance Part 2.* Metro Ethernet Forum.

MEF, & Santitoro, R. (2003). *Ethernet Access Services Definition.* Metro Ethernet Forum.

Mizrahi, T., & Safrai, U. (2015). *Carrier Ethernet 2.0: A Chipmaker's Perspective.* MARVELL.

Morency, I. (2012). *Carrier Ethernet 2.0 Services, Technical Foundation Document.* Iometrix.

NTT. (2010). *The Evolution of Ethernet.* NTT Communications.

Oña, G. (2016). *Diseño y comparación de redes de acceso MPLS y Metro Ethernet integradas a un backbone MPLS para un proveedor de servicios y realización de un prototipo base.* Quito.

Salcedo, O., Pedraza, L. F., & Espinosa, M. (2012). *Evaluación de redes MPLS/VPN/BGP con rutas reflejadas.* Tecnura.

Yerushalmi, I., & Mizrahi, T. (2011). *The OAM Jigsaw Puzzle.* MARVELL.

Glosario de Términos

AS (Automous System, Sistema Autónomo)

BGP (Border Gateway Protocol, Protocolo de Puerta de Enlace de Borde)

CE (Client Edge, Equipo del Cliente)

IEEE (Institute of Electrical and Electronics Engineers, Instituto de Ingeniería Eléctrica y Electrónica)

IETF (Internet Engineering Task Force, Grupo de Trabajo de Ingeniería de Internet)

IGP (Interior Gateway Protocol, Protocolo de Puerta de Enlace Interna)

IP (Internet Protocol, Protocolo de Internet)

L3VPN (Layer 3 Virtual Private Network, Red Privada Virtual de Capa 3)

LAN (Local Area Network, Red de Area Local)

LER (Label Edge Router, Router de Etiquetas de Borde)

LSP (Label Switched Path, Camino de Conmutación de Etiquetas)

LSR (Label Switch Router, Router de Conmutación de Etiquetas)

Mbps (Mega bits per second, Mega bits por segundo)

MP-BGP (Multi-Protocol Border Gateway Protocol, Protocolo de Puerta de Enlace de Borde - Multi Protocolo)

MPLS (Multi-Protocol Label Switching, Conmutación de Etiquetas Multi-Protocolo)

OSI (Open System Interconnection, Sistema Abierto de Interconexión)

OSPF (Open Shortest Path First, Primer Camino Más Corto)

P (Provider, Proveedor)

PC (Personal Computer, Computador Personal)

PE (Provider Edge, Borde del Proveedor)

RD (Route Distinguisher, Distinguidor de Ruta)

RR (Route Reflector, Reflector de Ruta)

RT (Route Target, Objetivo de Ruta)

SLA (Service Level Agreement, Acuerdo de Nivel de Servicio)

VLAN (Virtual Local Area Network, Red de Area Local Virtual)

VPN (Virtual Private Network, Red Privada Virtual)

WAN (Wide Area Network, Red de Area Amplia)

DECLARACIÓN Y AUTORIZACIÓN

Yo, **Carlos Luis Álvarez Cuesta**, con C.C: # **0703684985** autor/a del trabajo de titulación: **Implementación del modelo Inter-AS VPN opción C para continuidad de servicios VPN entre dos redes MPLS en el Ecuador utilizando el simulador GNS3,** previo a la obtención del título de **Magister en Telecomunicaciones** en la Universidad Católica de Santiago de Guayaquil.

1.- Declaro tener pleno conocimiento de la obligación que tienen las instituciones de educación superior, de conformidad con el Artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de titulación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2.- Autorizo a la SENESCYT a tener una copia del referido trabajo de titulación, con el propósito de generar un repositorio que democratice la información, respetando las políticas de propiedad intelectual vigentes.

Guayaquil, 29 de octubre del 2018

f. _____

Nombre: Carlos Luis Álvarez Cuesta

C.C: 0703684985

REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA			
FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN			
TÍTULO Y SUBTÍTULO:	Implementación del modelo Inter-AS VPN opción C para continuidad de servicios VPN entre dos redes MPLS en el Ecuador utilizando el simulador GNS3.		
AUTOR(ES)	Carlos Luis Álvarez Cuesta		
REVISOR(ES)/TUTOR(ES)	MSc. Luis Córdova Rivadeneira, MSc. Orlando Philco Asqui/MSc. Manuel Romero Paz		
INSTITUCIÓN:	Universidad Católica de Santiago de Guayaquil		
FACULTAD:	Sistema de Posgrado		
CARRERA:	Maestría en Telecomunicaciones		
TITULO OBTENIDO:	Magister en Telecomunicaciones		
FECHA DE PUBLICACIÓN:	29 de octubre del 2018	**No. DE PÁGINAS:**	72
ÁREAS TEMÁTICAS:	Protocolo IP, MPLS, Ethernet. Características de Servicios Carrier Ethernet y arquitectura de redes Metro Ethernet. Simulación e implementación de redes de Proveedores de Servicio IP/MPLS con Carrier Ethernet (E-Line)		
PALABRAS CLAVES/ KEYWORDS:	VPN, Inter AS, BGP, MPLS, MP-BGP, GNS3.		
RESUMEN/ABSTRACT: El presente trabajo de titulación comparte la experiencia de simulación del Inter AS opción C como solución escalable para la continuidad de servicios VPN (Virtual Private Network) capa 3 a través de sistemas autónomos. Para brindar esta experiencia al lector, es necesario detallar fundamentos teóricos del Inter AS opción C tales como: BGP (Border Gateway Protocol), MPLS (Muliprotocol Label Switching), MP-BGP (Multiprotocol Border Gateway Protocol). De igual manera, se dará a conocer el software de simulación GNS3 que servirá para simular dos dominios MPLS en los cuales se levantará un servicio Inter AS. Los clientes constantemente buscan mejoras en sus redes de datos y más aún optimizar costos de infraestructura. La simulación del Inter AS le permitirá al lector constatar los beneficios y usos del Inter AS, los cuales servirán para aplicarlos a casos reales que permitan monetizar la solución.			
ADJUNTO PDF:	☒ SI	☐ NO	
CONTACTO CON AUTOR/ES:	**Teléfono:** 0997845767	E-mail: clac_11@hotmail.com	
CONTACTO CON LA INSTITUCIÓN (C00RDINADOR DEL PROCESO UTE)::	**Nombre:** Manuel de Jesús Romero Paz		
	Teléfono: +593-4-2202935 /0994606932		
	E-mail: manuel.romero@cu.ucsg.edu.ec / mromeropaz@yahoo.com		
SECCIÓN PARA USO DE BIBLIOTECA			
Nº. DE REGISTRO (en base a datos):			
Nº. DE CLASIFICACIÓN:			
DIRECCIÓN URL (tesis en la web):			