Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE DISTRIBUCIÓN DE TRÁFICO *MULTICAST* PARA CLIENTES CORPORATIVOS SOBRE UNA RED MPLS DE UN PROVEEDOR DE SERVICIO DE INTERNET EN LA CIUDAD DE GUATEMALA

Héctor Antonio Portillo Lemus
Asesorado por el Ing. Christian Antonio Orellana

Guatemala, noviembre de 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE DISTRIBUCIÓN DE TRÁFICO *MULTICAST* PARA CLIENTES CORPORATIVOS SOBRE UNA RED MPLS DE UN PROVEEDOR DE SERVICIO DE INTERNET EN LA CIUDAD DE GUATEMALA

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

HÉCTOR ANTONIO PORTILLO LEMUS
ASESORADO POR EL ING. CHRISTIAN ANTONIO ORELLANA

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, NOVIEMBRE DE 2021

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Inga. Aurelia Anabela Córdova Estrada
VOCAL I	Ing. José Francisco Gómez Rivera
VOCAL II	Ing. Mario Renato Escobedo Martinez
VOCAL III	Ing. José Milton de León Bran
VOCAL IV	Br. Kevin Vladimir Cruz Lorente
VOCAL V	Br. Fernando José Paz González
SECRETARIA	Ing. Hugo Humberto Rivera Pérez

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

DECANO	Ing. Pedro Antonio Aguilar Polanco
EXAMINADOR	Ing. Helmunt Federico Chicol Cabrera
EXAMINADOR	Ing. Armando Alonso Rivera Carrillo
EXAMINADOR	Ing. Julio César Solares Peñate
SECRETARIA	Inga. Lesbia Magalí Herrera López

HONORABLE TRIBUNAL EXAMINADOR

En cumplimiento con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE DISTRIBUCIÓN DE TRÁFICO *MULTICAST* PARA CLIENTES CORPORATIVOS SOBRE UNA RED MPLS DE UN PROVEEDOR DE SERVICIO DE INTERNET EN LA CIUDAD DE GUATEMALA

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 18 de agosto del 2020.

Héctor Antonio Portillo Lemus

Guatemala, 09 de Junio de 2021

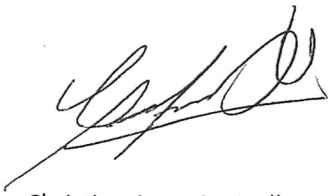
Ingeniero Julio Solares
Coordinador Área de Electrónica
Facultad de Ingeniería
Presente

Por este medio me permito dar aprobación al trabajo de Graduación titulado: **DISEÑO DE DISTRIBUCIÓN DE TRÁFICO MULTICAST PARA CLIENTES CORPORATIVOS SOBRE UNA RED MPLS DE UN PROVEEDOR DE SERVICIO DE INTERNET EN LA CIUDAD DE GUATEMALA**, desarrollado por el estudiante **Héctor Antonio Portillo Lemus**, ya que considero que cumple con los requisitos establecidos.

Por lo tanto, el autor de este trabajo y yo como asesor, nos hacemos responsables del contenido y conclusiones del mismo.

Sin otro en particular, aprovecho la oportunidad para saludarlo.

Atentamente,



Ing. Christian Antonio Orellana
Ingeniero Electrónico
Asesor de trabajo de Graduación
Área de Ingeniería Mecánica Eléctrica

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Guatemala, 15 de junio de 2021

Señor director
Armando Alonso Rivera Carrillo
Escuela de Ingeniería Mecánica Eléctrica
Facultad de Ingeniería, USAC

Estimado Señor director:

Por este medio me permito dar aprobación al Trabajo de Graduación titulado: **DISEÑO DE DISTRIBUCIÓN DE TRÁFICO MULTICAST PARA CLIENTES CORPORATIVOS SOBRE UNA RED MPLS DE UN PROVEEDOR DE SERVICIO DE INTERNET EN LA CIUDAD DE GUATEMALA,** desarrollado por el estudiante **Héctor Antonio Portillo Lemus**, ya que considero que cumple con los requisitos establecidos.

Sin otro particular, aprovecho la oportunidad para saludarlo.

Atentamente,

ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

Ing. Julio César Solares Peñate
Coordinador de Electrónica

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA MECÁNICA ELÉCTRICA
FACULTAD DE INGENIERÍA
UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

REF. EIME 168. 2021.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; HÉCTOR ANTONIO PORTILLO LEMUS titulado: DISEÑO DE DISTRIBUCIÓN DE TRÁFICO MULTICAST PARA CLIENTES CORPORATIVOS SOBRE UNA RED MPLS DE UN PROVEEDOR DE SERVICIO DE INTERNET EN LA CIUDAD DE GUATEMALA, procede a la autorización del mismo.

Ing. Armando Alonso Rivera Carrillo

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DIRECCION ESCUELA DE INGENIERIA MECANICA ELECTRICA
FACULTAD DE INGENIERIA

GUATEMALA, 23 DE NOVIEMBRE 2,021.

USAC
TRICENTENARIA
Universidad de San Carlos de Guatemala

Decanato
Facultad de Ingeniería
24189101 – 24189102

DTG. 706-2021

La Decana de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al Trabajo de Graduación titulado: **DISEÑO DE DISTRIBUCIÓN DE TRÁFICO MULTICAST PARA CLIENTES CORPORATIVOS SOBRE UNA RED MPLS DE UN PROVEEDOR DE SERVICIO DE INTERNET EN LA CIUDAD DE GUATEMALA**, presentado por el estudiante universitario: **Héctor Antonio Portillo Lemus,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, autoriza la impresión del mismo.

IMPRÍMASE:

Inga. Anabela Cordova Estrada
Decana

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, noviembre de 2021

AACE/cc

ACTO QUE DEDICO A:

Dios	Por darme todo lo que tengo.
Mis padres	Por poyarme y motivarme con amor a lo largo de mi vida.
Mi esposa	Por ser mí apoyo incondicional.
Mis hijos	Por ser mi inspiración.

AGRADECIMIENTOS A:

Dios	Por darme todo lo que tengo.
Mis padres	Por haberme apoyado y motivado con amor en mis estudios.
Universidad de San Carlos de Guatemala	Por ser la institución de educación superior que me dio un lugar en sus aulas.
Facultad de Ingeniería	Por formarme como profesional.

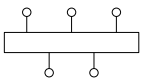
ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
	Computadora de escritorio
	Computadora portátil
	Conexión de fibra óptica
	Conexión Ethernet
	Enrutador
	Enrutador CPE
	Impresora
	Punto de acceso inalámbrico

Servidor

Tableta

GLOSARIO

ABR Por sus siglas en inglés *Area Border Router*, es un enrutador que tiene una interfaz en el área 0 y una interfaz en otra área distinta al área 0.

Address-family Se utiliza para indicarle a un enrutador cómo comportarse con las direcciones de red que reciba.

Anycast Comunicación especial de uno a varios con el servidor más cercano.

AS Por sus siglas en inglés *Autonomous System*, o sistema autónomo, es una red la cual tiene una administración única.

BGP Por sus siglas en inglés *Border Gateway Protocol* o Protocolo de Puerta de Enlace, es un protocolo de frontera utilizado ampliamente por los ISP para el intercambio de rutas.

Bit Es el acrónimo de *binary digit* o dígito binario.

CE Por sus siglas en inglés *Customer Equipment* o Equipo del Cliente.

CIDR	Por sus siglas en ingles *Classless Inter-domain Routing* o Enrutamiento inter dominios sin clase, el cual se utilizan máscaras de subred de longitud variable VLSM.
DBR	Por sus siglas en inglés *BackUp Designated Router* o enrutador designado de respaldo. En OSPF es el enrutador elegido para intercambiar información de enrutamiento con los otros enrutadores de la red en caso de fallar el DR.
DoS	Por sus siglas en inglés *Denial of Service* o denegación de servicio, es un ataque en el cual se satura un servicio hasta hacerlo inaccesible.
DR	Por sus siglas en inglés *Designated Router* o enrutador designado. En OSPF es el enrutador encargado de intercambiar información de enrutamiento con los otros enrutadores de la red.
eBGP	Por sus siglas en inglés *External* BGP, se utiliza para intercambiar rutas entre dos AS distintos.
EIGRP	Por sus siglas en inglés *Enhanced Interior Gateway Routing Protocol* o Protocolo de Enrutamiento de Puerta de enlace Interior Mejorado, es un protocolo de enrutamiento del tipo Vector Distancia avanzado que incluye características de protocolo de estado de enlace.

IANA	Por sus siglas en inglés *Internet Assigned Numbers Authority* o Autoridad para la asignación de números de internet. Es una organización de estándares IANA asigna y mantiene códigos y sistemas de numeración únicos utilizados en los estándares técnicos (“protocolos”) que permiten que los ordenadores y otros dispositivos se comuniquen entre sí a través de Internet
iBGP	Por sus siglas en inglés *Internal* BGP, se utiliza para intercambiar rutas dentro de en un AS.
IGMP	Por sus siglas en ingles *Internet Group Management Protocol* es un protocolo de capa 2 que nos sirve para poder transportar tráfico *multicast* a nivel de capa 2.
IPTV	Por sus siglas en inglés *Internet Protocol Television* o Protocolo de internet para la televisión, se utiliza para proveer servicio de Televisión por internet.
ISP	ISP por sus siglas en inglés *Internet Service Provider* Proveedor de Servicio de Internet, es la empresa que brinda servicios de Internet a usuarios finales, así como también servicios de voz, telefonía y datos a Empresas.
LAN	Por sus siglas en inglés *Local Área Network* o Red de Área Local, es la red que conectan Dispositivos

	electrónicos de una casa, oficina, edificio o campus dentro de un área geográficamente pequeña.
LDP	Por sus siglas en inglés *Label Distribution Protocol* o protocolo de distribución de etiquetas, es un protocolo que genera etiquetas de las redes que tiene conectadas y las anuncia a sus vecinos.
LSA	Por sus siglas en inglés *Link Satate Advertisement* o anuncio de estado de enlace, son registros de la base de datos que proporcionan destalles específicos de la red OSPF.
MDT	Por sus siglas en inglés *Multicast Distribution Tree* o árbol de distribución *multicast*.
mLDP	Por sus siglas en inglés *Multicast* LDP o LDP *multicast*.
MPLS	Por sus siglas en inglés *Multi Protocol Label Switching* o Protocolo múltiple de cambio de etiquetas. Es una técnica de enrutamiento en la cual se re direcciona un paquete hacia el próximo nodo utilizando el camino más corto por medio de etiquetas en lugar de direcciones de red largas con la finalidad de evitar búsquedas complejas en la tabla de enrutamiento.
Multicast	Es un método de enrutamiento que permite a un emisor o grupo de emisores comunicarse

	eficientemente con un grupo de receptores. Comunicación de uno a varios.
mVPN	Por sus siglas en inglés *Multicast* VPN o VPN *multicast*.
NAT	Por sus siglas en inglés *Network Address Translation* o Traducción de direcciones de red. Es una técnica que se utiliza para traducir de direcciones privadas a públicas y viceversa.
Nibble	Es una agrupación de 4 bits.
NLRI	Por sus siglas en inglés *Network Layer Reachability Information* o Información de accesibilidad de la capa de red, son un conjunto de atributos de red que intercambia el protocolo BGP.
OSPF	Por sus siglas en inglés *Open Shorest Path First* o Camino Abierto más Corto, es un protocolo abierto de enrutamiento de estado de enlace el cual se creó para reemplazar a RIP. Este es un protocolo de enrutamiento sin clase el cual utiliza el costo como métrica.
PE	Por sus siglas en inglés *Provider Equipment* o equipo del proveedor de servicio de internet.

PIM	Por sus siglas en inglés *Protocol Independent Multicast* o Protocolo *Multicast* Independiente. Es un protocolo de enrutamiento *multicast*.
RD	Por sus siglas en inglés *Route Distinguisher* se utiliza para mantener todas las redes únicas.
RIP	Es un protocolo de enrutamiento dinámico del tipo vector distancia y utiliza una métrica de conteo de saltos para elegir la mejor ruta.
RIPE	En francés es Redes IP Europeas, similar a la IANA asigna números de internet en Europa.
RP	Por sus siglas en inglés *Rendezvous Point* o Punto de Encuentro, es un enrutador especial en *multicast sparse mode* el cual conecta los flujos de datos de la fuente a los receptores.
RPF	Por sus siglas en inglés *Reverse Path Forwarding* es una técnica utilizada para el envío de paquetes *multicast* sin bucles.
RT	Por sus siglas en inglés *Route Target* se utiliza para transferir redes entre VRFs o VPNs de capa 3.
RTP	Por sus siglas en inglés *Reliable Transport Protocol* o Protocolo de transporte confiable, es el protocolo

	responsable para la comunicación entre enrutadores en EIGRP.
TCP	Por sus siglas en inglés *Transmission Control Protocol* o Protocolo de control de Transmisión, permite la comunicación entre 2 computadoras el cual garantiza la entrega de datos.
UDP	Por sus siglas en inglés *User Datagram Protocol* o Protocolo de Datagramas de Usuario, permite la comunicación entre 2 computadoras y la entrega de datos se hace con el mejor esfuerzo.
VLSM	Por sus siglas en inglés *Variable Length Subnet Mask* o máscaras de subred de longitud variable.
VPN	Por sus siglas en inglés *Virtual Private Network* o Red Privada Virtual, permite la conexión segura entre 2 redes privadas a través de una red pública.
VRF	Por sus siglas en inglés *Virtual Routing and Forwarding* o Enrutamiento Virtual y reenvío, permite a un enrutador tener tablas de enrutamiento separadas.
WLAN	Por sus siglas en Inglés *Wireless Local Area Network* o Red de Área Local Inalámbrica en la cual se conectan todos nuestros dispositivos con capacidad a

conectarse a una red Inalámbrica dentro de un área geográficamente pequeña.

RESUMEN

Las redes empiezan con la necesidad de compartir recursos entre computadoras, estas pueden ser redes LAN o WLAN, esta misma necesidad de mantener comunicación entre computadoras hizo que las redes evolucionaran en redes WAN.

Para la creación de redes WAN se necesita una gran infraestructura de red que pueda conectar computadoras en sitios geográficamente alejados, esta infraestructura es costosa para las empresas y recurren a un ISP para realizar la conexión entre sucursales.

El ISP cuenta con una infraestructura de red y protocolos MPLS y BGP que le ayudan a conectar sucursales de distintos clientes manteniendo el tráfico separado y privado para cada uno de ellos.

El tráfico *multicast* ha empezado a ser utilizado cada vez más por las empresas lo que obliga a los ISP a transportarlo entre sucursales. Para transportar este tráfico se crean las *multicast* VPN.

Existen diferentes formas de configurar estas *multicast* VPN llamados perfiles que ayudarán al momento de realizar un diseño de distribución de tráfico *multicast* para clientes corporativos sobre una red MPLS de un ISP.

OBJETIVOS

General

Realizar un diseño de distribución de tráfico *multicast* para clientes corporativos sobre una red MPLS de un proveedor de Servicio de Internet basado en un estudio bibliográfico.

Específicos

1. Describir los elementos que conforman una red MPLS de un Proveedor de Servicio de Internet.

2. Describir cómo funciona el tráfico *multicast* en un Proveedor de Servicio de Internet, y confirmar si es factible realizar el transporte y distribución de tráfico *multicast* de un cliente corporativo.

3. Describir el equipamiento mínimo que se debe proveer al cliente corporativo para brindarle el servicio de transporte y distribución de tráfico *multicast*.

4. Establecer recomendaciones para implementar el transporte y distribución de tráfico *multicast* como servicio para clientes corporativos.

INTRODUCCIÓN

El presente informe ayuda a comprender el funcionamiento de tráfico *multicast*, su importancia, y cómo se transporta en una red MPLS de un proveedor de servicio de Internet. Lo que permitirá hacer un diseño para la distribución de tráfico *multicast* de clientes corporativos.

Se está en una era de comunicación digital, en ella la comunicación se realiza en segundos, algo que sucede en Europa, se sabe en América casi de inmediato, y a pesar de esto muchas empresas tienen problemas de comunicación interna.

Muchas empresas tienen carteleras o televisores en los que publican información importante, pero en muchas ocasiones mantener estas carteleras o televisores con información actualizada es un reto. La tecnología les ha dado una solución, poder utilizar un servidor *multicast* y los receptores, en este caso los televisores o las propias computadoras pueden acceder al grupo *multicast* y poder informarse inmediatamente y con información actualizada.

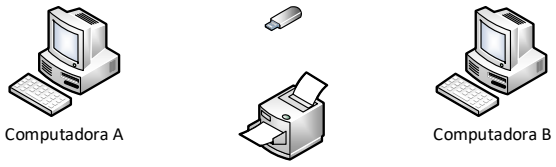
Cuando una empresa necesita transportar datos desde la central hacia las sucursales, generalmente, contrata un enlace de datos o enlaces privados a un Proveedor de Servicios de Internet. Pero, ¿Qué pasa si la transmisión que necesita hacer es *multicast*? Para este caso, como proveedores de servicio de internet, se estará realizando un diseño para el transporte de tráfico *multicast* de estas empresas, a las que se les llamará clientes corporativos.

1. INTRODUCCIÓN A LAS REDES

Las redes iniciaron con el invento de las computadoras, las computadoras empezaron a ser indispensables en las empresas y utilizaban memorias de almacenamiento externo para compartir archivos, se debía insertar en una computadora a la que llamaremos computadora A y luego pasarla a otra computadora la cual llamaremos computadora B.

Para poder imprimir, se tenía que conectar la impresora a la computadora A para que ella imprimiera y luego trasladar la impresora a la computadora B para que pudiera imprimir. Estas tareas se vuelven complicadas cuando se tiene una empresa con 50 computadoras.

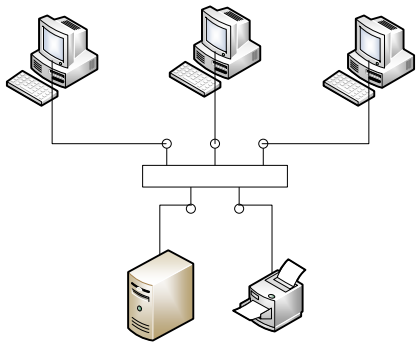
Figura 1. **Compartir archivos con almacenamiento externo**



Fuente: elaboración propia, empleando Visio 2013.

La solución a este problema fue crear una red de computadoras donde se pudieran compartir los recursos de la empresa, los archivos se pueden compartir desde un servidor y de la misma manera una impresora se puede compartir sin tener que estarla cambiando de lugar.

Figura 2. **Compartir archivos por medio de una red LAN**



Fuente: elaboración propia, empleando Visio 2013.

1.1. Tipos de redes

Mientras las empresas empezaron a tener más computadoras nacieron las redes LAN, cuando surgieron las computadoras portátiles y la conexión inalámbrica se crearon las redes WLAN y cuando las empresas tuvieron varias sucursales y tuvieron la necesidad de conectarlas surgieron las redes WAN.

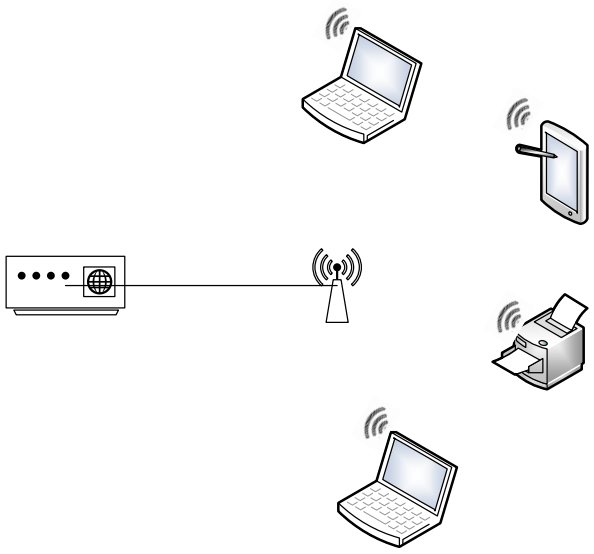
1.1.1. Red LAN

Por sus siglas en inglés *Local Area Network* o red de área local, es la red que conectan Dispositivos electrónicos de una casa, oficina, edificio o campus dentro de un área geográficamente pequeña. Es una red alámbrica o cableada tal como se observa en la figura 2.

1.1.2. Red WLAN

Por sus siglas en Inglés *Wireless Local Area Network* o red de área local inalámbrica en la cual se conectan todos los dispositivos con capacidad a conectarse a una red Inalámbrica dentro de un área geográficamente pequeña.

Figura 3. **Compartir archivos por medio de una red WLAN**

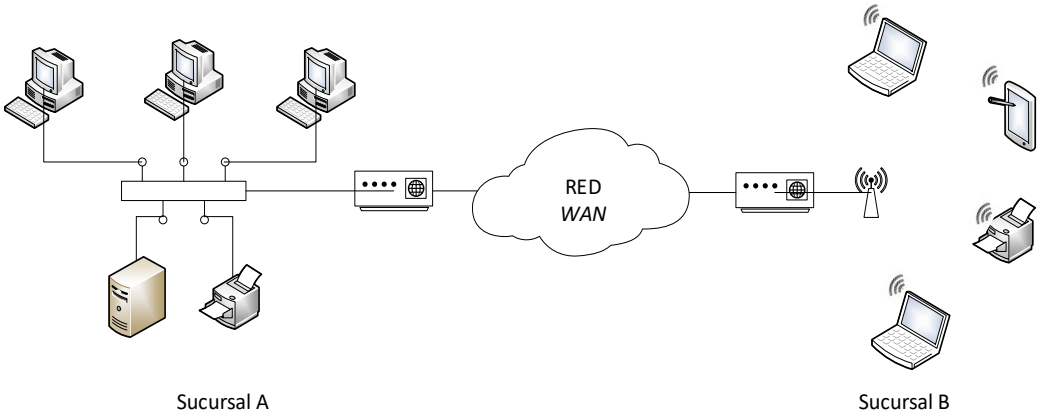


Fuente: elaboración propia, empleando Visio 2013.

1.1.3. Red WAN

Por sus siglas en Inglés *Wide Area Network* o red de área amplia que conecta varias redes de área local. Generalmente este tipo de red las provee un proveedor de servicios de internet.

Figura 4. **Red WAN**



Fuente: elaboración propia, empleando Visio 2013.

1.2. Tipos de tráfico

Las computadoras se comunican con diferentes tipos de tráficos dependiendo de su necesidad, los distintos tipos de tráfico que existen son los siguientes:

1.2.1. Tráfico Unicast

Así se le llama al tráfico que genera una computadora cuando se quiere comunicar con otra computadora, es una comunicación de uno a uno.

1.2.2. Tráfico Broadcast

Así se le llama al tráfico que se genera cuando una computadora se comunica con todas las otras computadoras en la red que se encuentra, esta es una dirección bien conocida dentro del segmento de red asignado. Es una comunicación de uno a todas.

1.2.3. Tráfico Multicast

Así se le llama al tráfico que se genera cuando una computadora se comunica con varias computadoras, y no con todas las demás computadoras, se utiliza el direccionamiento *multicast* para esta comunicación. Es una comunicación de uno a varios.

1.2.4. Tráfico Anycast

Así se le llama al tráfico que se genera cuando una computadora se comunica hacia un servidor dentro de un conjunto de servidores que prestan el mismo servicio y comparten la misma dirección *anycast*.

Esta es una comunicación especial de uno a varios, comunicándose con el servidor más cercano.

1.3. Direccionamiento IP

Las redes se crearon para que las computadoras se puedan comunicar y para que esto suceda las computadoras deben tener configurada una dirección IP única que las identifica de manera lógica.

Esta dirección IP no se puede repetir entre dos o más computadoras de lo contrario no sabríamos con quien deseamos comunicarnos.

Figura 5. **Direccionamiento red de 2 computadoras**

Fuente: elaboración propia, empleando Visio 2013.

Como observamos en la Figura 5, la computadora A tiene el direccionamiento 192.168.0.4 y la computadora B tiene el direccionamiento 192.168.0.5 donde la /24 en la dirección IP nos indica la máscara de subred la cual nos indica en que red esta esa dirección IP.

1.3.1. Direccionamiento IPv4

Una dirección IPv4 está formada por 32 bits las cuales están separadas por 8 octetos los cuales se convierten a notación decimal para su fácil manejo. Por ejemplo:

Tabla I. **Notación decimal y binaria de dirección IP**

Dirección IP notación decimal	**Dirección IP notación binaria**
192.168.0.4	11000000.10101000.00000000. 00000100
192.168.0.5	11000000.10101000.00000000. 00000101

Fuente: elaboración propia.

Tabla II. **Notaciones de máscara de sub red**

Máscara de sub red longitud del prefijo	**Máscara de sub red notación decimal**	**Máscara de sub red notación binaria**
/24	255.255.255.0	11111111.11111111.11111111.00000000
/24	255.255.255.0	11111111.11111111.11111111.00000000

Fuente: elaboración propia.

Podemos observar que en la máscara de subred los bits que tienen unos son los que son considerados los bits de red en el ejemplo de arriba las redes son /24 lo que significa que los primeros 3 octetos son unos y estos bits son considerados los bits de red. Entonces para el ejemplo anterior la dirección de red es: 192.168.0.0 para ambas direcciones lo que significa que ambas IP están en la misma red. El direccionamiento IPv4 se creó con las siguientes clases:

Tabla III. **Clases de direcciones IPv4**

CLASE	**Rango de direcciones**	**Bits de inicio**	**Bits de red**	**Bits de *hosts***	**Número de redes**	**Número de IP**
A	0.0.0.0 - 127.255.255.255	0	8	24	128 (2^7)	167,77,216 (2^24)
B	128.0.0.0 - 191.255.255.255	10	16	16	16,384 (2^14)	65,536 (2^16)
C	192.0.0.0 - 223.255.255.255	110	24	8	2,097,152 (2^21)	256 (2^8)
D	224.0.0.0 - 239.255.255.255	1110	No definido	No definido	No definido	No definido
E	240.0.0.0 - 255.255.255.255	1111	No definido	No definido	No definido	No definido

Fuente: elaboración propia.

Al inicio se asignaba una red pública de las arriba definida a las empresas hasta que poco a poco se fueron acabando y se tuvo la necesidad de crear otra forma de administrar las IP para que no se acabarán en un corto plazo, debido a esto se creó el *CIDR* por sus siglas en ingles *Classless Inter-domain Routing* en la cual se utilizan máscaras de subred de longitud variable *VLSM.*

Esto libero la forma de asignar las IPs, entonces, en lugar de asignar a una empresa un segmento de red /24 de las que probablemente solamente utilizarían unas 5 IPs para servidores que tuvieran que tener publicados hacia el Internet bien se podía ahora asignar una red /29 la cual puede cumplir con esta función:

Por ejemplo, si la empresa A necesita publicar 5 servidores de cara al internet bien se le puede asignar la IP 200.200.200.0/29:

IP: 200.200.200.0	11001000.11001000.11001000.00000 000
Ms: 255.255.255.248	11111111.11111111.11111111.11111 000

Los cuales nos deja con 3 bits para *host*, pero por convención la primera dirección no se utiliza por ser la dirección de red y la última tampoco se utiliza por ser la dirección de *broadcast*:

Red: 200.200.200.0/29	11001000.11001000.11001000.00000 000
HostMin: 200.200.200.1	11001000.11001000.11001000.00000 001
HostMax: 200.200.200.6	11001000.11001000.11001000.00000 110
Broadcast: 200.200.200.7	11001000.11001000.11001000.00000 111

Se podría utilizar del a dirección 200.200.200.1 a la 200.200.200.6 que nos deja con 6 direcciones IPs utilizables.

Esto creo otro tipo de rango de direcciones un tipo privado y un tipo público los hosts dentro de la empresa tenían que poderse seguir comunicando internamente, además de existir comunicación entre las computadoras de la empresa o red privada, deben existir IPs que puedan comunicarse a la red pública o Internet. A continuación, el listado de las IPs que se pueden comunicar internamente o mejor conocidas como IPs Privadas:

Tabla IV. **Direcciones privadas por clase IPv4**

CLASE	Rango de direcciones	Número de Redes	Número de IP	Bits de *Hosts*
A	10.0.0.0 - 10.255.255.255	1	16,777,214	24
B	172.16.0.0 - 172.31.255.255	16	65,534	16
C	192.168.0.0 - 192.168.255.255	256	254	16
B Simple	169.254.0.0 - 169.254.255.255	1	65,534	16

Fuente: elaboración propia.

Pero esto genera con otro problema, algunas de estas computadoras de la empresa también necesitan acceder a servicios de internet como, por ejemplo, si un gerente quiere consultar la bolsa de valores en internet, dado que las IPs de las maquinas que no son servidores se les asigna una IP privada ¿cómo se puede resolver este inconveniente?

Esto se resolvió colocando dispositivos de cara al internet que pudieran realizar NAT por sus siglas en ingles *Network Address Translation*.

1.3.2. Direccionamiento IPv6

A pesar de la creación del CIDR y debido al crecimiento del Internet de las Cosas, que es conectar cada dispositivo de la casa a una red para que pueda ser controlado mediante una aplicación. Se tuvo que crear otro direccionamiento que pudiera satisfacer esta nueva demanda.

Este direccionamiento es el IPv6 el cual está formado por 128 bits que se representan con 32 números Hexadecimales y para que sea más fácil de leer se agrupan en 8 grupos de 4 dígitos separados por dos puntos (:). Por ejemplo, la siguiente dirección es una dirección IPv6:

FE80:0000:0000:00A0:0000:0000: 0000:0006

Pero esta es una dirección muy larga de aprender por lo que IPv6 define las siguientes 2 reglas para abreviarla:

- Dentro de cada cuarteto (grupo de 4 dígitos) se remueven los primeros 0 de la izquierda, si todos son 0 (0000) en el cuarteto, se deja un 0.
- Si existen cuartetos consecutivos en los cuales todos los dígitos son 0, entonces se reemplazan estos cuartetos por dos pares de dos puntos (::). Tomar en cuenta que esto solo se puede utilizar una vez en cada dirección.

Según estas dos reglas anteriores, volvamos a escribir la dirección IPv6 de arriba:

FE80:0:0: A0::6

Como podemos observar, antes del cuarteto 00A0 habían 2 cuartetos en los cuales todos eran 0 y se reemplazó por un 0 cada cuarteto y después de este habían 3 cuartetos todos 0 por lo que se reemplazó por (::), se ve que la mayor cantidad de 0 se reemplazó por :: el cuarteto 00A0 si vemos se quitaron los 0 de la izquierda pero se conservó el 0 de la derecha y así cumplimos con las 2 reglas para abreviar las direcciones IPv6.

Para expandir debemos de realizar el procedimiento contrario tomando en cuenta que los (::) deben de reemplazarse por cuartetos de 0 sin pasar de 8 grupos de cuartetos en toda la dirección IPv6.

Para el direccionamiento IPv6 también se utiliza un concepto muy parecido al de máscara de subred y se llama Longitud del prefijo, este ya se ha explicado anteriormente en IPv4 que no es mas de colocar la cantidad de 1 que forman la IP de red.

- FE80:0:0: A0::6/64

  Para este caso la dirección de red sería:

- FE80:0:0: A0::0/64

  Los diferentes tipos de direccionamiento que se encuentran en IPv6 son:

Tabla V. **Direcciones privadas por clase IPv6**

Tipo de Dirección	**Primeros dígitos hexagesimales**
Global Unicast	2 o 3 originalmente, actualmente no son todos los de este segmento
Unique Local	FD
Multicast	FF
Link Local	FE80
Loopback	::1/128

Fuente: elaboración propia.

Donde:

- *Global Unicast*: Este tipo de direccionamiento son las que se pueden enrutar por internet, son similares a las direcciones IPv4 públicas.
- *Unique Local*: Este tipo de direccionamiento es similar al direccionamiento privado de IPv4 y se utilizan para ser configuradas en un sitio local y no deben ser enrutables a internet.
- *Multicast*: Al igual que en IPv4 este tipo de direcciones nos permiten enviar paquetes a un grupo de computadoras.
- *Link Local*: Este tipo de direccionamiento se utiliza para comunicarse en el mimo enlace local. Las cuales no se pueden enrutar más allá del link local.
- *Loopback*: Al igual que en IPv4 se utiliza para enviar paquetes a sí misma y este direccionamiento no se puede asignar a ninguna interfaz física.

1.4. Modelo TCP/IP

El modelo TCP/IP se desarrolló junto con el inicio de Internet. Antes del internet cada marca creaba su propio protocolo de red que solo funcionaban con

sus equipos. Un modelo se crea para la interoperabilidad de los distintos dispositivos no importando la marca y con el surgimiento de Internet esto era muy importante.

El modelo TCP/IP consta de 4 capas las cuales cada una tiene distinta función y así asegurar que la comunicación entre dispositivos se lleve correctamente:

Tabla VI. **Modelo TCP/IP**

	Arquitectura TCP/IP	**Descripción**	**Protocolos**
4	**Aplicación**	**Datos:** Representa datos para el usuario, más el control de codificación de diálogo	**HTTP, POP3, SMTP**
3	**Transporte**	**Segmento:** Admite la comunicación entre distintos dispositivos a través de diversas redes	**TCP, UDP**
2	**Internet**	**Paquetes:** Determina el mejor camino a través de la red	**IP, ICMP**
1	**Acceso a la red**	**Tramas:** Controla los dispositivos de hardware y los medios que crean la red	**Ethernte, 802.11 (Wi-Fi)**

Fuente: elaboración propia.

1.5. Modelo OSI

Este sistema se llama Modelo de Interconexión de Sistema Abierto originalmente creado por la ISO con el fin de crear una suite de protocolos abiertos para la interconexión de computadoras, pero con la velocidad a la que

creció el internet adoptando el protocolo TCP/IP hizo que la suite de protocolos del Modelo OSI no fuera adoptado.

El modelo OSI es muy importante debido a que es un modelo de referencia que ayuda al desarrollo de otros protocolos y productos para todo tipo de redes nuevas. Este protocolo cuenta con 7 capas las cuales son:

Tabla VII. **Modelo OSI**

7	**Aplicaión**	Proporciona los medios para la conectividad de extremo a extremo entre individuos de la red humana
6	**Presentación**	Proporciona una representación de datos transferidos entre servicios de la capa de aplicación
5	**Sesión**	Proporciona servicios para organizar su diálogo y organizar el intercambio de datos
4	**Transporte**	Define los servicios para segmentar, transferir y rearmar los datos para las comunicaciones entre dispositivos
3	**Red**	Proporciona servicios para intercambiar datos en la red.
2	**Enlace de datos**	Describe los métodos para intercambiar tramas de datos.
1	**Física**	Describe los medios mecánicos, eléctricos y ópticos para activar, mantener y desactivar conexiones físicas para la transmisión de bits.

Fuente: elaboración propia.

1.6. Comparación modelo OSI y TCP/IP

EL modelo OSI y TCP/IP tiene varias similitudes, la siguiente tabla compara la funcionalidad de las distintas capas:

Tabla VIII. **Comparación modelo OSI y TCP/IP**

	TCP/IP	PROTOCOLOS	MODELO OSI	
			Aplicación	7
			Presentación	6
4	**Aplicación**	**HTTP, POP3, SMTP**	**Sesión**	5
3	**Transporte**	**TCP, UDP**	**Transporte**	4
2	**Internet**	**IP, ICMP**	**Red**	3
			Enlace de datos	2
1	**Acceso a la red**	**Ethernte, 802.11 (Wi-Fi)**	**Física**	1

Fuente: elaboración propia.

2. PROTOCOLOS DE ENRUTAMIENTO

Hasta este momento hemos visto que las computadoras necesitan una dirección IP para poder comunicarse con otra computadora y hemos visto que un ejemplo de esto cuando las computadoras están en la misma red y con esto podemos compartir archivos.

En las empresas generalmente no todas las personas deben de acceder a la misma información y no queremos eso. Por lo cual se utilizan diferentes segmentos de red para diferentes departamentos y así poder controlar quien puede acceder a que recurso. Es ahí cuando vemos la necesidad de comunicarnos entre redes. Esto se logra mediante un protocolo de enrutamiento.

Los protocolos de enrutamiento pueden ser de 2 tipos:

- IGP: Dentro de un sistema autónomo
- EGP: Entre sistemas autónomos

2.1. IGP

Por sus siglas en inglés *Interior Gateway Protocol* estos son protocolos de enrutamiento dentro de un Sistema Autónomo, un sistema autónomo es una red la cual tiene una administración única, por ejemplo, el de una empresa, la cual la administra la empresa misma.

Los protocolos de enrutamiento IGP más utilizados son los siguientes:

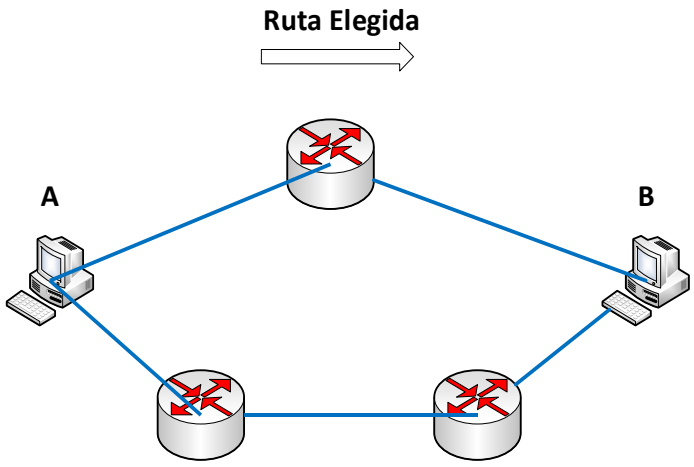
- RIP
- EIGRP
- OSPF

2.1.1. RIP

Es un protocolo de enrutamiento dinámico del tipo vector distancia y utiliza una métrica de conteo de saltos para elegir la mejor ruta. RIP considera una distancia infinita cuando tiene 16 saltos o más. RIP tiene una distancia administrativa de 120.

En la figura 6 se tienen 2 rutas para llegar de la computadora A, y a la computadora B. RIP elegirá la ruta con menos saltos.

Figura 6. **Elección de ruta rip**



Fuente: elaboración propia, empleando Visio 2013.

RIP crea vecinos con los enrutadores que son adyacentes a él y envía mensajes de actualización de las rutas que conoce cada 30 segundos incluso sin que haya habido un cambio en la topología para mantener actualizadas las rutas.

Para evitar *Loops* RIP cuenta con las siguientes herramientas:

- *Split Horizon:* No anuncia una red por la interfaz que la aprendió
- *Poison Reverse:* Cuando pierde conectividad a una red la anuncia con métrica infinita (16 saltos) para que todos los enrutadores que la aprendieron por medio de él la desinstalen de su tabla de enrutamiento.

Existen 3 versiones de RIP:

2.1.1.1. RIPv1

- Envía actualización a sus vecinos por medio de dirección *Broadcast*
- No Soporta VLSM
- Para direccionamiento IPv4

Configuración:

router rip
_network [Red 1 del Router]
_network [Red 2 del Router]

2.1.1.2. RIPv2

- Envía actualizaciones a sus vecinos por la dirección *multicast* (224.0.0.9)
- Soporta VLSM

- Para direccionamiento IPv4

Configuración:

router rip
_version 2
_network [Red 1 del Router]
_network [Red 2 del Router]
_no auto-summary

2.1.1.3. RIPng

- Envía actualizaciones a sus vecinos por la dirección *multicast* (FF02::9)
- Soporta VLSM
- IPv6

Configuración:

ipv6 unicast-routing
ipv6 routing rip [Nombre_del_proceso_RIP]
int S0/0
_ipv6 rip [Nombre_del_proceso_RIP] enable
int S0/1
_ipv6 rip [Nombre_del_proceso_RIP] enable

Comandos de comprobación:

show ip protocols
show ip route

show ip route rip
show ip protocols
show ip rip
show ip rip next-hops
show ipv6 route
show ipv6 route rip
show ipv6 protocols
show ipv6 rip
show ipv6 rip next-hops

Aunque RIP es un protocolo que ya casi no se usa, aún se encuentra configurado en algunas empresas pequeñas.

2.1.2. EIGRP

EIGRP también es un protocolo de enrutamiento del tipo Vector Distancia avanzado que incluye características de protocolo de estado de enlace, la métrica que utiliza es la distancia y para calcular su métrica utiliza un algoritmo DUAL que está dada por la siguiente fórmula:

Métrica = {([K1*BW] + [K2*BW]/[256- Carga] + [K3*_Delay_])*(K5/[Confiabilidad+K4])} * 256

Donde los valores de K están representados por:

K1 = Ancho de Banda (BW), 1 por defecto
K2 = Carga, 0 por defecto
K3 = *Delay*, 1 por defecto
K4 = K5 = Confiabilidad, 0 por defecto

Este protocolo de enrutamiento fue creado por CISCO con una distancia administrativa de 90 fue publicado como un estándar abierto en el 2013 y publicado en el RFC 7868 en 2016.

EIGRP crea vecindades con los enrutadores adyacentes utilizando el protocolo de transporte confiable RTP que solo lo utiliza EIGRP y a diferencia de RIP, EIGRP envía actualizaciones parciales y limitadas, lo que significa que en la actualización solo se incluye la información de la ruta que sufre cambios y solo se le envía a los enrutadores que se ven afectados por este cambio.

2.1.2.1. Características de EIGRP

- Convergencia rápida
- Escalable hasta 500 enrutadores
- Puede enrutar tanto IPv4 como IPv6.
- Soporta VLSM
- Se comunica a través de la *multicast* 224.0.0.10
- Balanceo de Carga con rutas de igual o distintas métricas
- Utiliza *Split Horizon* para evitar *loops*

EIGRP mantiene 2 rutas hacia una red las cuales son:

- *Succesor:* Es el siguiente salto de la mejor ruta hacia una red, esta se instala en la tabla de enrutamiento.
- *Feasible Succesor:* Es el siguiente salto de la siguiente mejor ruta (distinta al *Succesor*), hacia una red en la no se forma un *loop* de enrutamiento.

Se debe tener claro que el salto del *Feasible Succesor* puede o no puede existir dependiendo si existe otro camino hacia la red destino y se garantice que no cree un *loop* de enrutamiento.

EIGRP maneja 3 tablas:

- Tabla de vecinos: En esta podemos observar los estados de los vecinos. (*show* ip eigrp *neighbors*).
- Tabla de interfaces: En esta podemos observar las interfaces que están participando en EIGRP. (*show* ip eigrp *interfaces*).
- Tabla de topología: En esta podemos observar que salto es del *Succesor* o *Feasible Succesor*. (*show* ip eigrp *topology*).

EIGRP cuenta con *timers* los cuales no deben ser iguales entre vecinos, estos se pueden modificar e indican cuanto tiempo tiene que esperar el vecino para saber del enrutador local, estos los podemos consultar con los siguientes comandos:

- show ip eigrp int detail
- show ip eigrp neighbors

EIGRP utiliza para identificar el enrutador un valor de 32 bits esta puede ser la dirección *loopback* más alta en estado *up/up* y de no existir interfaz *loopback* utiliza la dirección de más alta configurada en una interfaz. También podemos utilizar un comando para poder configurar el identificador del enrutador (eigrp router-id [dirección-ipv4].

2.1.2.2. Configuración EIGRP IPv4

conf t

_router eigrp [Sistema Autónomo]

__eigrp router-id [dirección-ipv4]

__network [RED 1] [*Wildcard* 1]

__network [RED 2] [*Wildcard* 2]

__network [RED 3] [*Wildcard* 3]

La máscara *wildcard* es lo inverso a la máscara de subred. Si la máscara de subred es 255.255.255.0 la máscara *wildcard* es 0.0.0.255.

2.1.2.3. Comandos de comprobación EIGRP

show ip route

show ip eigrp interfaces

show ip eigrp neighbors

show ip eigrp topology

2.1.2.4. Caracterísitcas EIGRP IPv6

- La dirección del siguiente salto es el *link* local
- Utiliza autenticación propia de IPv6
- No existe la auto sumarización
- Los vecinos no requieren estar en la misma sub red.
- Envía actualizaciones a la dirección *multicast* FF02::A

2.1.2.5. Configuración IPv6

conf t
_ipv6 unicast-routing
_ipv6 router eigrp [Sistema Autónomo]
__eigrp router-id [Dirección IPv4]
_intereface [Interfaz]
__ipv6 address [Dirección IPv6]
__ipv6 eigrp [Sistema Autónomo]

2.1.2.6. Comandos de validación IPv6

show ipv6 route
show ipv6 route eigrp
show ipv6 route [Dirección IPv6]
show ipv6 protocols
show ipv6 eigrp neighbors
show ipv6 eigrp interfaces
show ipv6 eigrp interfaces
show ipv6 eigrp topology
show ipv6 eigrp topology all-link

2.1.3. OSPF

Por sus siglas en inglés *Open Shortest Path First,* es un procolo abierto de enrutamiento de estado de enlace el cual se creó para reemplazar a RIP. Este es un protocolo de enrutamiento sin clase el cual utiliza el costo como métrica y tiene una distancia administrativa de 110.

2.1.3.1. Características de OSPF

- Establece adyacencia con otros enrutadores
- Envía *Link Sate Advertisements* (LSAs) a otros enrutadores en las áreas
- Construye una base de datos de estado de enlace con los LSAs recibidos
- Corre el algoritmo Dijkstra *Shortest Path First* (SPF) para determinar la mejor ruta hacia una red.
- Inyecta la mejor ruta hacia una red en la tabla de enrutamiento.
- Los vecinos se encuentran en la misma red.
- Intercambia mensajes de Hola para formar vecinos.
- Utiliza la dirección *multicast* 224.0.0.5 para enviar mensajes de Hola a los vecinos.
- Utiliza la dirección *multicast* 224.0.0.6 para enviar mensajes a los enrutadores DR (solo los DR y BDR escuchan estos mensajes).

Pasos para formar adyacencia:

- State init
- 2 Way
- ExStart
- Exchange
- Loading
- Fulll

Para calcular las mejores rutas de una red a otra OSPF utiliza el algoritmo Dijkstra el cual se ejecuta cada vez que existe un cambio en la red, si la red es muy grande OSPF utiliza áreas para que no se tenga que correr este algoritmo en toda la red y optimizar los recursos del enrutador. Siempre vamos a tener el

área 0 o 0.0.0.0 que es el área de *Backbone* al cual todas las otras redes se deben de conectar y comunicarse a través de esta.

OSPF hace elección de DR y BDR para evitar que las adyacencias de los enrutadores sea *full mesh*, lo que significa que todos los enrutadores tendrán adyacencia solo con el DR y BDR optimizando los recursos del enrutador y evitar que se sature el Ancho de Banda disponible con los mensajes LSA. Estos DR y BDR serán los encargados de enviar a todos los enrutadores los cambios topológicos que sucedan.

2.1.3.2. Elección del enrutador DR

- Se utiliza el protocolo de Hola para elegir al DR.
- Durante la elección del DR el enrutador con la prioridad más alta gana.
- La prioridad de OSPF está asociada a una interfaz y puede ser un valor entre 0 – 255.
- Una prioridad de OSPF 0 significa que ese enrutador se convertirá en el DR.
- Por defecto la prioridad OSPF de las interfaces tiene un valor de 1.
- La prioridad en una interfaz se puede configurar con el comando: "ip ospf priority [vlaue]".
- Si existe un empate en la prioridad el enrutador con el router ID (RID) más alto gana.
- El RID se configure con el siguiente comando: “router-id [ID]".
- Si el enrutador no tiene configurado RID la IP más alta de una interfaz *loopback* que se encuentre arriba se toma como RID.
- Si el enrutador no tiene *loopback* la interfaz con la IP más grande se convierte en el RID.

Enrutador (ABR): Es un enrutador que tiene una interfaz en el área 0 y al menos una en otra área.

2.1.3.3. Configuration de OSPF

Conf t
_router ospf [Sistema Autonomo]
__network [Red 1] area 1
__network [Red 2] area 0
__network [Red 3] area 0
_int [Interfaz 1]
__ip ospf [Sistema Autonomo] area 1
_int [Interfaz 2]
__ip ospf [Sistema Autonomo] area 0

2.1.3.4. Comandos de validación

show ip ospf interface brief
show ip protocols
show ip ospf neighbor
show ip ospf database

2.1.3.5. Tipos de redes OSPF

Estos tipos de Redes se hicieron para poder configurar OSPF sobre distintos tipos de enlaces, por defecto ospf se comporta de manera distinta dependiendo del enlace al que haga referencia, por ejemplo:

- *Broadcast* es el tipo de red por defecto que utiliza OSPF en redes *Ethernet.*
- *Point-to-Point* es el tipo de red por defecto que utiliza OSPF sobre un enlace de *Frame Relay* subinterfaces *point-to-point*.
- *Non Broadcast* (NBMA) es el tipo de red por defecto que utiliza OSPF sobre un enlace *Frame Rellay* interfaces físicas y sub interfaces mutli punto.

2.1.3.5.1. Broadcast Network

- Elije un DR y BDR: Si
- Intervalo del hola son 10 segundos
- No requiere configuración del comando Neighbor

2.1.3.5.2. Point to Point Network

- Elije un DR y BDR: Si
- Intervalo del hola son 10 segundos
- No requiere configuración del comando Neighbor

2.1.3.5.3. Non-Broadcast (NBMA) (Non Broadcast Multiple Access)

- Elije un DR y BDR: Si
- Intervalo del Hola son 30 segundos
- Si requiere configuración del comando Neighbor

2.1.3.5.4. Point to Multipoing

- Elije un DR y BDR: No
- Intervalo del Hola son 30 segundos
- No requiere configuración del comando Neighbor

Existen 2 Intervalos que utiliza OSPF para mantener la adyacencia con otros enrutadores, como vmos en las tablas anteriores son distintas dependiendo del tipo de red:

- Intervalo hola: del mensaje Hola está dado en segundos y generalmente es el intervalo en el que se envían los paquetes Hola indicando que el vecino está operativo.
- Intervalo muerto: Generalmente es 4 veces el Intervalo Hola y es el tiempo que espera el enrutador para dar por perdida una adyacencia.

Los intervalos deben de coincidir entre enrutadores adyacentes al igual que el tipo de redes para que se forme adyacencia y vecindad entre enrutadores.

2.2. EGP

Por sus siglas en inglés *Exterior Gateway Protocol* estos son protocolos de enrutamiento entre varios Sistemas Autónomos, por ejemplo, entre un ISP y una empresa, estos tienen una administración de red distinta cada uno.

2.2.1. BGP

Actualmente el único protocolo de enrutamiento EGP es BGP.

2.2.1.1. Qué es BGP

BGP es un protocolo de enrutamiento vector ruta, que fue creado para intercambiar rutas de redes entre Sistemas Autónomos (AS), el cual provee escalabilidad, estabilidad y flexibilidad. Es un protocolo de enrutamiento creado para las redes públicas como el internet.

2.2.1.2. ¿Qué es un sistema autónomo?

Un sistema autónomo es una red bajo una misma administración. Para la red pública estos números son asignados por la IANA y para Europa por el RIPE o por un ISP.

Al inicio el sistema autónomo tenía un tamaño de 16 bits 65,535 números de AS pero debido a que se estaban acabando se cambió el tamaño a 32 bits y ahora existen 4,294,967,295 números de AS únicos.

Los bloques de números de AS privados, lo que significa que no van a salir a la red pública de Internet, son del 64,512 – 65,5353 y del 4,200,000,000 – 4,294,967,294.

2.2.1.3. Características de BGP

- Forma *Peerings* (puede ser con su vecino o no).
- No forma vecindades automáticamente, se debe de configurar el *peer* explícitamente.
- Utiliza sesiones TCP para establecer vecindades.
- Anuncia una dirección *prefix* con su longitud llamada NLRI (*network layer reachability information*).

- Anuncia una colección de atributos de ruta que pueden ser utilizados para la selección de la mejor ruta.

2.2.1.4. Atributos de ruta BGP

- Peso: Es un atributo con significado local específico de CISCO que se puede configurar en una ruta cuando se recibe. Mientras más alto el valor se prefiere más la ruta.
- Preferencia local: Es un parámetro que se configure en todo un AS, mientras más alto el valor se prefiere más la ruta.
- Originar: Si un enrutador es quien crea la ruta localmente, esta será preferida a la aprendida de otro enrutador.
- Longitud de la ruta: BGP siempre se puede ver la ruta de AS por la que pasa y la ruta que tenga menor número de AS será la preferida.
- Tipo de origen: Este atributo nos indica cómo fue aprendida la ruta en BGP: ¿I (IGP), ¿E (EGP), o? (información incompleta). I se prefiere sobre E, ¿y E se prefiere sobre?
- MED (*Multi-Exit Discriminator*): Es un parámetro que se puede utilizar entre 2 AS que tienen 2 conexiones entre ellos para influenciar sobre que conexión se estarán recibiendo los datos. Un valor más bajo de MED se prefiere sobre uno alto.
- Rutas: Las rutas eBGP son preferidas sobre las rutas iBGP.
- Métrica IGP del siguiente salto: Si todos los atributos son iguales en 2 rutas que se aprenden por BGP se prefiere la ruta la cual el siguiente salto tenga la métrica del IGP más pequeña.
- Rutas múltiples: Aquí se determina si se inyectan múltiples rutas hacia una red o sin no se ha elegido una, se sigue con los siguientes atributos para elegir una.

- Edad: Si todos los atributos anteriores son iguales el tiempo en el que se aprendió la ruta se utiliza para el desempate, la ruta aprendida antes se prefiere.
- Identificador del enrutador*:* Si todos los atributos anteriores son iguales, para la elección de la mejor ruta se utiliza el Identificador del Enrutador.
- Dirección IP del vecino: Si todos los atributos anteriores son iguales, se prefiere la ruta que tenga el siguiente salto con la dirección más pequeña.

2.2.1.5. Mensajes BGP

- *Open*: Este mensaje incluye la version de BGP, el número local del AS, el Tiempo *Hold*, el identificador del enrutador BGP, y parámetros adicionales y se utiliza para establecer la sesión BGP.
- *Keep Alive*: Este mensaje evita que expire el tiempo hold. Manteniendo la sesión BGP abierta.
- *Update*: Es un mensaje de actualización que contiene contiene información NLRI, atributos de ruta y nuevas rutas.
- *Notification*: Contiene información de código de errores cuando se Cierra una sesión BGP.

2.2.1.6. Estados de los vecinos BGP

- *Idle:* Escucha si existe algún intento de conexión por parte del vecino.
- *Connect:* Se inicia la conexión TCP.
- *Active:* BGP inicia una nueva conexión TCP.
- *OpenSent:* Envía un mensaje Open y deben de conicidir los siguientes parámetros:
    - Versión de BGP
    - La dirección origen debe ser igual a la del vecino configurado

- El AS debe ser igual a la del vecino configurado
- Los identificadores BGP (RDIs) deben ser únicos
- Los parámetros de seguridad deben de coincidir (pasword y TTL)

- *OpenConfirm:* BGP está a la espera de un mensaje *Keep Alive* o una Notificación.
- *Established:* La sesión BGP está establecida y se están intercambiando rutas.

2.2.1.7. iBGP y eBGP

Es importante saber que BGP se comporta de manera diferente si es iBGP (BGP interno), vecinos dentro del mismo AS o si es eBGP (BGP externo), vecino hacia otro AS.

- iBGP requiere full mesh entre vecino y eBGP no lo requiere.
- Si se aprende una ruta por medio de un eBGP, esta ruta se redistribuye a todos los vecinos no importando el tipo.
- Si se aprende una ruta por medio de un iBGP, esta ruta se redistribuye solo a los vecinos externos o eBGP.
- Los atributos Peso, preferencia local, solo se puede enviar a vecinos internos iBGP.
- La distania Adminitrativa (AD) es distinta iBGP tiene una AD de 200 eBGP tiene una AD de 20.

2.2.1.8. Configuración de BGP

conf t
_router bgp [AS local]
__bgp router-id [IPv4 ID del enrutador]

__networ [Red que participara en BGP]
__neighbor [Dirección IP del vecinoo] remote-as [AS del vecino]

Si AS local es igual a AS vecino entonces es iBGP
Si AS local es distinto a AS vecino entonces es eBGP

2.2.1.9. Enrutador reflector

El enrutador reflector es un enrutador configurado con iBGP que puede reflejar o transmitir las redes que aprendió de un vecino iBGP a otro, hay que recordar que se había dicho que esto no era posible, pero si es posible para un enrutador que está configurado como enrutador reflector.

A continuación, se indican los motivos por el cual se requiere un enrutador reflector:

- Para evitar tener que configurar demasiados *peerings* BGP lo cual no es escalable en redes muy grandes, esto debido a la condición que para iBGP se requiere full mesh, entonces solo es necesario crear peerings BGP para los enrutadores reflectores.
- Para poder transmitir las redes conocidas a otros *peers* BGP.
- Para prevenir *Loops* de enrutamiento.

2.2.1.10. Confguración enrutador reflector

conf t
_router bgp [AS local]
__bgp router-id [IPv4 ID del enrutador]
__networ [Red que participara en BGP]

__neighbor [Dirección IP del vecino] remote-as [AS del vecino]

__neighbor [Dirección IP del vecinoo] route-reflector-client

El comando que se marca en negritas convierte al enrutador en un enrutador reflector, para los otros enrutadores no es necesaria configuración adicional.

2.3. *Multicast*

Ahora ya se tiene una idea de que es *multicast* pero se necesita profundizar en el concepto.

2.3.1. *¿Qué es multicast?*

Como lo vimos anteriormente en los tipos de tráfico, el tráfico *multicast* es la comunicación de uno a varios. En donde se envía solo un paquete y este se replica entre las ramas del árbol de distribución de *multicast* (MDT).

Entonces *multicast* es una técnica para transmitir información de uno a varios o también de varios a varios.

El tráfico multicas se le llama flujo y se asignan un grupo de direcciones IPs especiales para este tráfico. El servidor *multicast* maneja una sola sesión con los distintos solicitantes del flujo de datos. Y este tráfico se utiliza en aplicaciones de Telepresencia, video en tiempo real, IPTV, capacitaciones remotas, conferencias de video y audio, música y *gaiming.*

2.3.2. Fundamentos de *multicast*

- Mejora la escalabilidad: Los recursos de red no dependen del número de receptores.
- Reduce la utilización de los recursos: Se tiene el control de utilización de ancho de banda, así como reduce la carga de los servidores.
- *Multicast* utiliza UDP: No existen retransmisiones, corrección de errores ni control de flujo.
- Entrega de tráfico con mejor esfuerzo.
- No tiene herramientas para evitar la congestión: No utiliza ventanas TCP.

2.3.2.1. Concepto de grupos multicast

Es un grupo de receptores que están interesados en algún flujo de datos, que se unen a un grupo llamado grupo que está formado por una dirección IP del rango de *multicast* utilizando IGMP, una vez en el grupo, los receptores pueden recibir el flujo de datos desde cualquier parte.

2.3.2.2. Direccionamiento IP multicast

Como ya hemos visto el direccionamiento de los grupos *Multicast* está dado por los siguientes rangos: 224.0.0.0 - 239.255.255.255 y FF para IPv6. En la página de la IANA hay un listado detallad de las direcciones *multicast* asignadas de las cuales podemos mencionar las siguientes:

Tabla IX. **Direccionamiento *multicast***

Local Network Control Block	224.0.0.0 - 224.0.0.255	224.0.0/24
Internetwork Control Block	224.0.1.0 - 224.0.1.255	224.0.1/24
AD-HOC Block I	224.0.2.0 - 224.0.255.255	
RESERVED	224.1.0.0-224.1.255.255	224.1/16
SDP/SAP Block	224.2.0.0-224.2.255.255	224.2/16
AD-HOC Block II	224.3.0.0-224.4.255.255	224.3/16, 224.4/16
RESERVED	224.5.0.0- 224.251.255.255	251 /16s
DIS Transient Groups	224.252.0.0- 224.255.255.255	224.252/14
RESERVED	225.0.0.0- 231.255.255.255	7 /8s
Source-Specific Multicast Block	232.0.0.0- 232.255.255.255	232/8
GLOP Block	233.0.0.0- 233.251.255.255	
AD-HOC Block III	233.252.0.0- 233.255.255.255	233.252/14
Unicast-Prefix-based IPv4 Multicast Addresses	234.0.0.0- 234.255.255.255	
Scoped Multicast Ranges Reserved	235.0.0.0- 238.255.255.255	
Organization-Local Scope	239.0.0.0- 239.255.255.255	

Fuente: IANA. *IPv4 Multicast Address Space Registry*.
https://www.iana.org/assignments/multicast-addresses/multicast-addresses.xhtml.
Consulta: mayo de 2021.

Tomar nota que la fuente del contenido no puede estar en este rango de direcciones IP, debe estar en otro rango de IPs.

2.3.2.3. Arboles de distribución *multicast*

Un árbol de distribución *multicast* es un árbol que crean los protocolos *multicast* para transmitir flujo de datos desde un grupo G de una fuente S hacia los receptores.

El objetivo de un árbol de distribución *multicast* es duplicar el paquete *multicast* cuando debe enviar el flujo de datos por 2 o más rutas y así llegar a todos los receptores del grupo *multicast*.

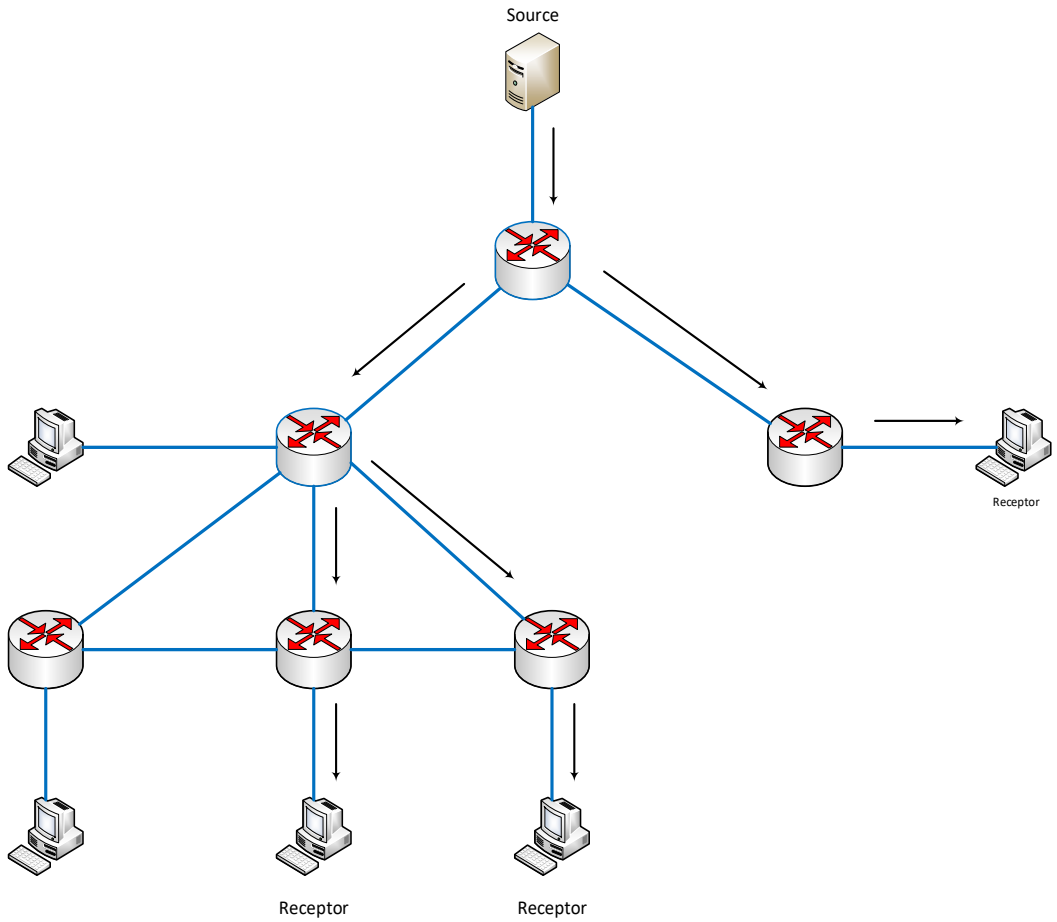
Existen 2 tipos de árboles:

- Árbol fuente (*Source Tree*)
- Árbol compartido (*Share Tree*)

2.3.2.3.1. Árbol fuente

La raíz de este camino es la fuente, y es el camino más corto u óptimo que el paquete *multicast* puede encontrar de la fuente hasta los receptores y se identifican en la tabla de distribución como (S, G), se especifica la fuente S y el grupo G.

Figura 7. **Árbol fuente**

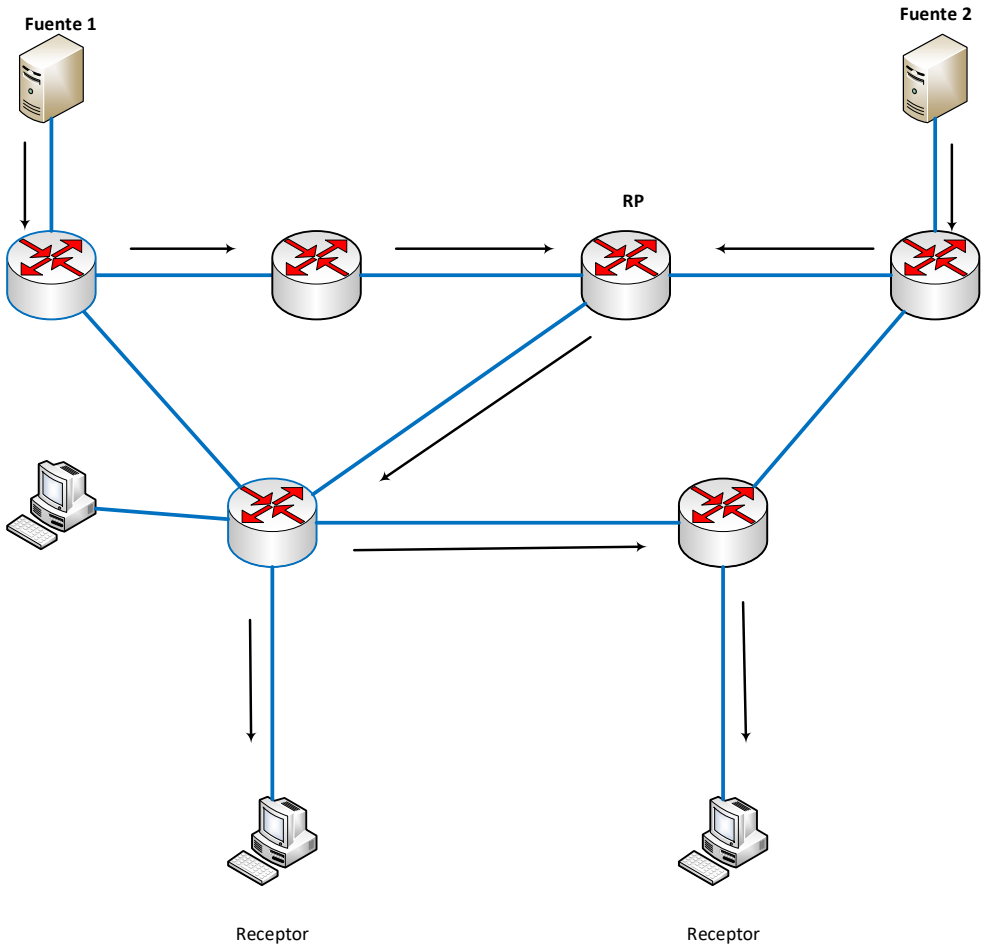


Fuente: elaboración propia, empleando Visio 2013.

2.3.2.3.2. Árbol compartido

La raíz de este camino es el RP (*Rendezvous Point* o Punto de Encuentro), por eso se le conoce a este tipo de árbol como RPT. Debido a que la raíz es el RP y no la fuente en la mayoría de las ocasiones no proporciona el camino más corto u óptimo. Este árbol se identifica en la tabla de distribución como (*, G), cualquier fuente * que proporcione el flujo de ese grupo G.

Figura 8. **Árbol compartido**



Fuente: elaboración propia, empleando Visio 2013.

2.3.3. Protocolo PIM

Por sus siglas en inglés Protocol Independent Multicast, Protocolo Multicast Independiente. Lo que significa este nombre es que es independiente del protocolo de enrutamiento *unicast* que se tenga en la red.

Es un protocolo de enrutamiento que crea árboles de distribución *multicast* para poder enrutar el flujo de datos *multicast*.

2.3.3.1. PIM Dense Mode

Este tipo de protocolo esta creado pensando en que todos los receptores están localizados en una parte de la red y lo que hace el enrutador es enviar el tráfico *multicast* hacia todas las interfaces activas para garantizar que la información llegue a los receptores, a esto se le llama inundaciones, estas inundaciones se realizan periódicamente para garantizar que no se quede sin el flujo de datos ningún receptor.

Debido a que no todos los enrutadores necesitan esta información, se realiza un *prunning* o poda la cual se realiza para que no lleguen paquetes duplicados o que no llegue tráfico innecesario a los enrutadores. El inconveniente con esto es que cada inundación puede tener un impacto muy grande en la red y posiblemente saturarla.

2.3.3.2. PIM Sparse Mode

Empieza utilizando un árbol de distribución compartido, utiliza un punto de encuentro RP (*Rendezvous Point*), y el receptor hace la solicitud del trafico *multicast* al punto de encuentro RP (*, G), debido a que el RP sabe dónde se encuentra la Fuente de este tráfico. El RP responde al receptor la dirección de la fuente y el receptor envía la solicitud directamente a la fuente (S, G), y poda el flujo que le envía el RP. A este cambio se le llama “cambio a la ruta óptima” sin tener que realizar inundaciones y podas constantemente haciendo uso óptimo del BW. Hay que notar que el árbol también cambia a árbol fuente.

2.3.3.3. PIM SSM

Por sus siglas en inglés Source Specific Multicast, en esta configuración de PIM requiere que el primer salto del receptor conozca la dirección de la fuente de cada grupo *multicast* el cual envía una solicitud (S, G), como tráfico *unicast* y el contenido ya lo recibe como tráfico *multicast*. Como vimos anteriormente utiliza el rango de direcciones *multicast* 232.0.0.0/8 y se requiere tener configurado IGMPv3 para poder utilizar este tipo de PIM. Si el receptor conoce la fuente, entonces ya no es necesario el RP.

2.3.3.4. PIM Bidir

Cuando existen varias fuentes que están enviando tráfico a varios receptores, existe el problema que hay demasiadas solicitudes (S, G), y el tráfico puede está distribuido en toda la red y no se tiene un control sobre este. Este inconveniente se puede reducir si tenemos árboles de distribución compartidos, lo que significa que tenemos un RP al cual llegan las solicitudes como (*, G) y el cual puede distribuir el contenido.

Esta es la manera cómo funciona PIM Bidir y nos ayuda a reducir los estados de enrutamiento *multicast* en los enrutadores de la red, el tráfico fluye del RP y hacia el RP, lo que ayuda a que fluya el tráfico de varios a varios de marera tal que se hace más escalable con conexiones prácticamente sin límite.

2.3.4. *Multicast* Capa 2

Para el transporte del tráfico *multicast* a nivel de capa 2 se requiere configurar un protocolo especial llamado IGMP.

2.3.4.1. IGMP

IGMP por sus siglas en ingles *Internet* Group Management Protocol tiene su propio protocolo IP y nos sirve para poder transportar tráfico *multicast* a nivel de capa 2.

Como bien hemos visto, a nivel de capa 3 el tráfico *multicast* utiliza el rango D IPv4 para transportar este tráfico, a nivel de capa 2 se debe de convertir la dirección IP en dirección MAC *multicast* y para eso se realiza lo siguiente:

- Toda dirección MAC *multicast* empieza con los siguientes números Hexadecimales: 01-00-5e.
- Convertir los últimos 3 octetos de la dirección IPv4 en binario.
- El bit más significativo se convierte en 0 de no ser 0.
- Convertir cada *nibble* (está formado por 4 bits) en hexadecimal.

Por ejemplo, si tenemos el grupo con la siguiente dirección IP: 224.128.10.3

La dirección MAC para este grupo sería:

- Iniciar la dirección MAC con 01-00-5e
- Los Bits de los últimos 3 octetos son: 10000001.00001010.00000011
- Cambiar el bit más significativo a 0: 0000.0001.0000.1010.000.0011
- Convirtiendo a Hexadecimal: 01-00-5e-01-0A-03

Favor tomar nota que debido a la regla 3 si la dirección IPv4 fuera 224.1.10.3 la dirección *multicast* MAC hubiera sido la misma. Tomar nota de esto al momento de diseñar los grupos *multicast*.

2.3.4.1.1. Mensajes IGMP

- *Membership report*: Es un paquete que genera un receptor para solicitar el flujo de datos de un grupo *multicast*.
- *General Memebership Queries*: Es un paquete que envía el enrutador para ver si aún existe receptores interesados en un grupo *multicast.* Utiliza la dirección 224.0.0.1 se llama todos los *hosts* de *multicast.* Los receptores que aún necesiten el flujo de datos responden con un paquete de *membership report.*
- Leave Group: Mensaje que envía un receptor indicando que ya no requiere el flujo *multicast.*
- Group-Specific Queries: Mensaje que envía el enrutador para saber si aún hay un receptor interesado en un flujo *multicast* luego de haber recibido un mensaje de *Leave Group*.

2.3.4.1.2. IGMPv1

- Utiliza mensajes de *Membership Query* enviada a la dirección 224.0.0.1 para encontrar receptores.
- Los receptores *multicast* envían mensajes de *Membership Report* al grupo que desean unirse.
- No existe manera de informar que ya no quieren participar en el grupo *multicast* al que se unieron.
-

2.3.4.1.3. IGMPv2

- Puede enviar un mensaje de *Membership Query* a la dirección 224.0.0.1 o al grupo directamente.
- Solo el enrutador con la dirección IP más baja puede enviar las solicitudes.

- Se introduce el mensaje *Leave Message* para que el receptor indique que quiere dejar el grupo.

2.3.4.1.4. IGMPv3

Es un protocolo de comunicación, es empleado para intercambiar información y forma parte de la familia de protocolos del internet.

- La característica de la versión es que ya soporta SSM

2.3.4.2. IGMP Snooping

Permite a un *Switch* escuchar las solicitudes de *multciast* y crear una tabla en la cual no enviará tráfico *multicast* a ningún puerto en el cual no haya recibido una solicitud de este tráfico. Con esto se protege a las computadoras de algún ataque de DoS.

2.3.5. mVPN

Por sus siglas en inglés *multicast* VPN o VPN *multicast.*

- Provee un servicio *multicast* a los clientes través del ISP.
- Lo PEs del ISP transportaran el protocolo PIM del cliente llamado CPIM (*Customer* PIM) dentro de una VRF.
- Los PEs formaran vecindades CPIM con los CEs.
- Los SP puede tener su propio *multicast*.

Existen varios perfiles de configuración mVPN dependiendo de la necesidad que se tenga, de los cuales en esta tesis haremos mención de 6:

2.3.5.1. Profile 0 Default MDT - GRE - PIM C-Mcast Signaling

- Se crea un túnel GRE para el transporte del *multicast* del cliente.
- El ISP debe tener configurado *multicast* para crear los árboles *multicast*.
- Se le asigna un grupo multicas de los que tiene disponible el ISP a la vrf del cliente para transportar su tráfico *multicast*.
- Se puede configurar como Default MDT o Data MDT.
- Se configura CPIM entre el CPE y la vrf del cliente en el PE.
- Todos los PEs forman adyacencias PIM entre ellos.

2.3.5.2. Profile 1 Default MDT - MLDP MP2MP - PIM C-Mcast Signaling

- Se utiliza MPLS para el transporte del multicast del cliente.
- El ISP no es necesario que tenga configurado multicast pero si debe estar habilitado el enrutamiento multicast globalmente en los PEs para recibir el multicast del cliente.
- Se le debe asignar una VPN id por cada mVPN la cual se configura en la vrf del cliente.
- Se debe de asignar un router como root que hace la función de RP.
- Todos los PEs forman adyacencias PIM entre ellos.

2.3.5.3. Profile 2 Partitioned MDT - MLDP MP2MP - PIM C-Mcast Signaling

- En el enfoque MDT particionado, solo los enrutadores PE de salida que reciben solicitudes de tráfico de un PE de entrada particular crean árboles

en el núcleo, limitando el número de árboles en el núcleo. Esta es la diferencia entre el perfil 1 y este perfil 2.

- Actualmente no lo soporta CISCO IOS se debe de utilizar IOS XR.
- Para IOS XR se configura una política de RPF en la cual se le define el árbol del núcleo como mldp *default*.

2.3.5.4. Profile 3 Default MDT - GRE - BGP-AD - PIM C-Mcast Signaling

- Forma parte de la nueva generación de mVPN.
- Ya no es necesario crear adyacencia PIM contra todos los PEs, solo con contra el RR.
- Los equipos core P ya no participan en la señalización.
- Se utiliza BGP para la señalización creando un *address-family* mVPN.
- En la VRF del cliente se configura el mdt *auto-discovery* pim.
- En el RR se debe de crear el *address-family* ipv4 mdt indicando que él es el RR e indicar cuáles serán sus vecinos activándolos.

2.3.5.5. Profile 4 Partitioned MDT - MLDP MP2MP - BGP-AD - PIM C-Mcast Signaling

- En el enfoque MDT particionado
- Actualmente no lo soporta CISCO IOS y se debe utilizar IOS XR
- Se utiliza MPLS para el transporte del *multicast* del cliente
- Utiliza BGP sobre mldp para señalización
- Se debe de configurar en la política RPF que es mldp mp2mp particionado

2.3.5.6. Profile 5 Partitioned MDT - MLDP P2MP - BGP-AD - PIM C-Mcast Signaling

- En el enfoque MDT particionado
- Actualmente no lo soporta CISCO IOS y se debe utilizar IOS XR
- Se utiliza MPLS para el transporte del *multicast* del cliente
- Utiliza BGP sobre mldp para señalización
- Se debe de configurar en la política RPF que es mldp p2mp particionado

2.3.5.7. Perfil 6 VRF MLDP - Señalización dentro de la banda

- Se utiliza MPLS para el transporte del *multicast* del cliente.
- El ISP no es necesario que tenga configurado *multicast* pero si debe estar habilitado el enrutamiento *multicast* globalmente en los PEs para recibir el *multicast* del cliente.
- Se configura mLDP para la señalización en banda.
- Los equipos core P participan en la señalización.

3. RED MPLS

3.1. ¿Qué es MPLS?

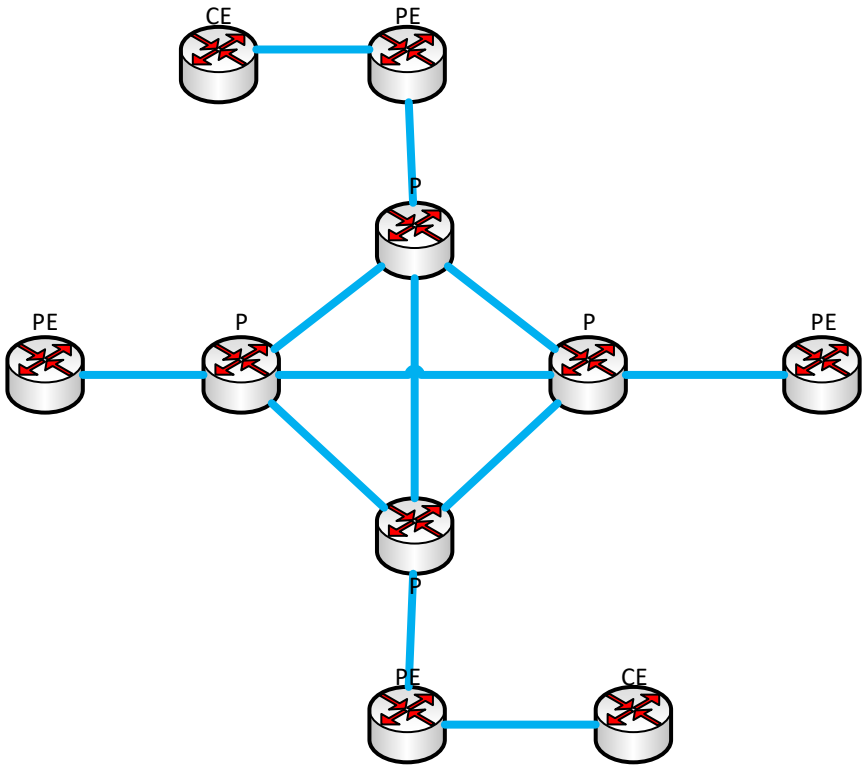
Por sus siglas en inglés Multi Protocol Label Switching. Es un método para la transmisión de paquetes y en el primer enrutador determina la ruta completa para enviar el paquete y le asigna una etiqueta corta de 32 bits. Se le llama protocolo de capa 2.5 debido a que esta etiqueta se coloca entre la capa 2 y la capa 3 del paquete.

3.2. Evolución de MPLS

MPLS surge por la necesidad de enrutar paquetes de una manera más rápida. Con los protocolos de enrutamiento tradicionales cada enrutador debe de inspeccionar la dirección destino y procesarla para luego transmitirla.

En MPLS el paquete es analizado por el primer enrutador y le asigna una etiqueta. Con esta etiqueta los demás enrutadores únicamente lo transmiten ahorrándose el procesamiento de los enrutadores siguientes. Esta agrega una etiqueta y con esta el enrutador sabe cómo enviar el paquete a su destino

Figura 9. **Red MPLS**



Fuente: elaboración propia, empleando Visio 2013.

Donde:

- P (*Provider*) significa Enrutador del Proveedor llamado también LSR *Laber Switching Router*.
- PE (*Provider Edge*) significa Enrutador de Borde del Proveedor conocido también como LER *Laber Edge Router*.
- CE (*Customer Edge*) significa Enrutador de Borde del Cliente.

Además, en el momento en que surgio MPLS las topologías que ofrecían los SP era *Hub and Spoke.* Con MPLS se dio la oportunidad de conectar *full mesh*.

3.3. ¿Dónde se utiliza MPLS?

MPLS lo utiliza el ISP para enrutar paquetes de los clientes y las ventajas son las siguientes:

- Reduce costos: Se pueden conectar los distintos sitios del cliente sin importar la tecnología con la que se conecten por ejemplo se puede conectar un sitio que se conecta por medio de DSL a otro sitio que se conecta por F.O. con otro que se conecta por medio de un E1.
- Red más eficiente y escalable: al poder tener comunicación todos los sitios en forma de *full mesh*.
- Red más fiable: Se puede implementar Calidad de Servicio e Ingeniería de Tráfico.

3.4. Distribución de etiquetas en una red MPLS

La distribución de etiquetas en una red MPLS se realiza a través del protocolo LDP, el cual le asigna una etiqueta a cada ruta aprendida.

3.4.1. LDP

Por sus siglas en inglés Label Distribution Protocol es un protocolo que genera etiquetas de las redes que tiene conectadas y las anuncia a sus vecinos. LDP les permite a los enrutadores crear una ruta de etiquetas. Utiliza el puerto UDP 646. Cuenta con los siguientes mensajes:

- Discovery Message
- Session Message
- Advertisements Message
- Notification Message

3.4.2. BGP

Cuando se transmiten rutas por medio de VRFs, BGP es responsable de generar una etiqueta para mantener únicas las redes dentro del enrutador y evitar traslapes.

3.5. Construcción de servicios basados en MPLS

MPLS soporta una variedad de servicios entre los cuales se encuentran servicios de Capa 2 y servicios de Capa3.

3.5.1. Servicios Capa 2

Estos servicios pueden transportar tramas Ethernet y se comporta como un switch. Entre estos servicios tenemos los siguientes:

Tabla X. **Servicios MPLS Capa 2**

Nombre MEF del servicio	Nombre MEF Corto	Topología	Descripción
Servicios Ethernet de Linea	E-lines	punto a punto	2 CPE pueden intercambiar tramas Ethernet, similar a una línea alquilada.
Servicio Ethernet de LAN	E-LAN	Full mesh	Se comporta como un LAN en la cual todos los dispositivos pueden intercambiar tramas Ethernet con todos los demás.
Servicio Ethernet de árbol	E-Tree	Hub and Spoke; mesh parcial; punto a multipunto	Un sitio central se puede comunicar con una cantidad definida de puntos remotos, los puntos remotos no se pueden comunicar directamente entre ellos.

Fuente: ODOM, Wendell. *Oflfial Cert Guide CCNA*. p. 306.

3.5.2. Servicios Capa 3

Conocidos como MPLS VPN de capa 3 estas VPN se crean gracias a la creación de VRFs.

3.5.2.1. VRF

Por sus siglas en ingles Virtual Routing Forwarding es una tecnología que permite tener más de una tabla de enrutamiento con esto se puede tener 2 tablas de enrutamiento con las misma IP sin que se traslapen. Esto permite a los ISP dar transporte a los clientes sin preocuparse que anuncien el mismo segmento de red. Tiene las siguientes características:

- Los clientes pueden utilizar cualquier direccionamiento en su red
- Los clientes tienen una conexión IP hacia el ISP, pueden utilizar cualquier protocolo de enrutamiento que deseen.
- El ISP utiliza MPLS para transmitir las rutas de CE a CE.
- El ISP puede realizar dar conectividad *full mesh* a los sitios del cliente.

3.6. Configuraciones

A continuación, se presentan las configuraciones necesarias para tener una red con MPLS y BGP.

3.6.1. Configuración MPLS

Para configurar MPLS se requiere lo siguiente:

- Que todos los enrutadores tengan configurado un IGP
- Para Cisco tener activado CEF
- Tener activado LDP

```
configure terminal
ip cef
interface [Interfaz]
_mpls ip

show ip cef
show mpls ip binding
show mpls ldp Discovery
```

3.6.2. Configuración de VRF

configure terminal
ip vrf [nombre de la VRF]
_rd [configurar el rd]
_rt import [configurar el rt]
_rt export [configurar el rt]

Interface [interfaz]
_vrf [nombre de la VRF]
_ip address [IP de la interfaz]

Donde:

- rd por sus siglas en inglés *Route Distinguisher* se utiliza para mantener todas las redes únicas.
- rt por sus siglas en inglés *Route Target* se utiliza para transferir redes entre VRFs o VPNs de capa 3.

4. DISEÑO DE DISTRIBUCIÓN DE TRÁFICO MULTICAST PARA CLIENTES CORPORATIVOS SOBRE UNA RED MPLS DE UN PROVEEDOR DE SERVICIO DE INTERNET

4.1. Requerimientos del cliente corporativo

Para la creación del diseño de distribución de tráfico multicas para clientes corporativos sobre una red MPLS de un proveedor de servicio de internet se necesita establecer de primero la necesidad del cliente.

4.1.1. Necesidad del cliente

La necesidad del cliente corporativo es simple, transportar su tráfico *multicast* desde su central a todas sus sucursales.

4.1.2. Servicio a transportar

Los servicios que se solicitan transportar son:

- Audio, para música ambiental y poder anunciar al público algún tipo de información importante.
- Video, para alguna capacitación a los empleados con su respectivo audio.
- Actualizaciones masivas para sus equipos, esto se realizará en la noche para no afectar horario laboral.

4.1.3. Servicios contratados con los cuales ya cuenta el cliente

Para que un ISP pueda transportar el tráfico *multicast* de un cliente corporativo, el cliente debe contar con un enlace de datos o enlace privado, este es un servicio VPN de capa 3, contratado para que esto se pueda llevar a cabo.

4.1.3.1. Medio de transporte

Existen distintos medios de transporte por los cuales se puede hacer llegar el servicio de datos al cliente, entre los cuales pueden ser:

- Cobre
- Fibra óptica
- Microonda

El transporte está ubicado en la capa 1 del modelo OSI y no tiene participación en *multicast*, por lo cual no son una limitante para nuestro diseño.

4.1.3.2. Equipos de última milla

Los equipos de última milla varían dependiendo del medio de transporte que tenga el cliente, estos pueden ser convertidores de medio de eléctrico a óptico y Microondas, este último para algunos sitios de difícil acceso. Estos equipos generalmente son de capa 2 y tienen una topología de punto a punto el cual no participa en igmp o pim, por lo que no son una limitante para nuestro diseño.

4.1.3.3. CE del cliente

Para la elección del CE, se debe elegir uno que soporte *multicast*, existen una gran variedad de equipos que se pueden instalar de los cuales mencionaremos 2:

"CISCO 1941."[1]
"CISCO 1921."[2]

Cabe mencionar que la mayoría de los CE utilizados por el ISP soportan PIM, es importante que se valide en la página oficial del proveedor del equipo para asegurarse que el modelo instalado soporte PIM.

4.2. RED MPLS de ISP

Todos los ISP tienen configurado MPLS para poder ofrecer servicios VPN de capa 3 y capa 2 a los clientes por lo que podemos afirmar que se cuentan con todos los componentes de una red MPLS mencionados en el capítulo anterior.

4.2.1. Protocolo de enrutamiento entre PE y CE

Este protocolo es a solicitud del cliente, en el cual generalmente se puede utilizar EIGRP, OSPF o BGP. No se recomienda RIP por ser un protocolo antiguo ni rutas estáticas debido al gran mantenimiento que se debe dar al momento de agregar una red nueva.

---

[1] Cisco, Products & Services. *Cisco 1941 Series integrated services routers data sheet*. https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78_556319.html. Consulta: mayo de 2021.

[2] Cisco, Products & Services. *Cisco 1921 Series integrated services routers data sheet*. https://www.cisco.com/c/en/us/products/collateral/routers/1900-series-integrated-services-routers-isr/data_sheet_c78-598389.html. Consulta: mayo de 2021.

4.2.2. Servicios que tiene configurado el ISP en su red

"Al momento de realizar esta tesis los 2 proveedores de servicio de internet ofrecen enlaces de datos."[3] o "también llamados enlaces privados."[4], los cuales son servicios VPN capa 2 o capa 3 por lo que a continuación se coloca un listado de servicio deben tener para ofrecer estos servicios:

4.2.2.1. MPLS

Los ISP tienen configurado MPLS debido a que ofrecen servicios de VPN Capa 3 y Capa 2. MPLS es necesario para poder transportar las etiquetas de las VPNs.

4.2.2.2. BGP

Los ISP para ofrecer servicios de VPN Capa 3 y Capa 2 es necesario que tengan BGP configurado. El protocolo BGP se en conjunto con las VRF se utilizan para proveer estos servicios mantener separadas las redes de los clientes y poder anunciar sus redes de una sucursal a otra.

[3]Claro Corporaciones. *Soluciones, conectividad, enlaces de datos*. https://www.claro.com.gt/corporaciones/soluciones/conectividad/enlaces-de-datos/. Consulta: mayo de 2021.
[4]Tigo. *Soluciones, conectividad, enlaces privados.* https://www.tigobusiness.com.gt/soluciones/conectividad/enlaces-privados. Consulta: mayo de 2021.

4.2.2.3. Multicast

En Claro “los ISP de Guatemala ofrecen servicios de cable y video.”[5]. En Tigo “los ISP de Guatemala ofrecen servicios de cable y video.”[6], y esto se logra teniendo configurado *multicast,* y se puede decir que los ISP descargan la señal de cable de una antena en un punto por lo cual es muy probable que en su configuración utilicen sea *sparse mode* con RP configurado.

4.3. Propuesta de diseño

Para la propuesta de diseño se debe elegir como se transportará el tráfico *multicast* del cliente corporativo.

4.3.1. Elección de *multicast*

Por los servicios que tiene configurado el ISP podemos decir lo siguiente:

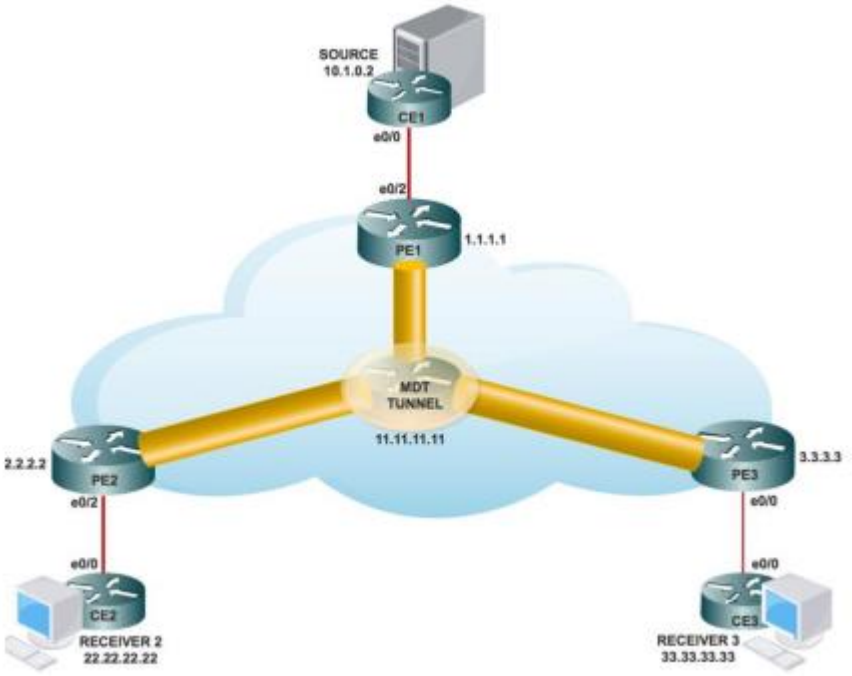
- Se hará uso del *multicast* ya configurado en el ISP partiendo que tienen configurado sparse mode y no SSM.
- Debido a que la solicitud es transportar audio, video en el día y algunas actualizaciones en la noche, no es necesario transportar demasiado tráfico y no requiere un ancho de banda elevado, por eso se puede configurar MDT por defecto y no *data* MDT.

Por lo anterior el diseño de distribución de tráfico *multicast* para clientes corporativos sobre una red MPLS de un proveedor de servicio de internet en la

[5] Claro. *Triple play.* https://www.claro.com.gt/personas/servicios/servicios-hogar/todo-claro/3-play/. Consulta: mayo de 2021.
[6] Tigo. *Residencial*. http://residencial.tigo.com.gt/. Consulta: mayo de 2021.

ciudad de Guatemala es utilizar una configuración mvpn con perfil 0, este utiliza túneles GRE, que transportarán el tráfico *multciast* del cliente y la señalización de estos túneles se realizará por medio del *multicast* del ISP al cliente.

Figura 10. **mVPN Perfil 0**



Fuente: CISCO. *Next Generation Multicast VPN & Advanced Design*. https://www.ciscolive.com/c/dam/r/ciscolive/us/docs/2017/pdf/LTRMP-3103.pdf. Consulta mayo de 2021.

4.3.2. Configuraciones requeridas

- Se debe de habilitar *multicast routing* de manera global en la vrf del cliente

#ip multicast-routing vrf [VRF del cliente] distributed

- Se debe de habilitar pim en la interfaz donde está configurada la VRF del cliente, con este comando se habilita automáticamente IGMPv2.

  int [interfaz que pega al cliente]
  ip pim sparse-mode

- Configuración de túnel GRE en la vrf del CLIENTE, en esta se debe de elegir un grupo *multicast* de los que tiene el ISP para su uso y asignarlo al cliente.

  vrf definition [VRF del cliente]
  address-family ipv4
  mdt default [IP multicas asignada por el ISP al cliente]

  Comandos para validación:

  Para validar que los túneles hayan levantado:
  show interface tunnel 0

  Para validar que se estén recibiendo las rutas *multicast*:
  show ip mroute [IP *multicast* asignada al cliente]

  Para validar que PIM esté funcionando y se formen vecindades:
  show ip pim vrf [VRF] neighbors

  Para validar que se esté recibiendo el RP del cliente:
  show ip pim vrf C1 rp mapping

CONCLUSIONES

1. Al momento de realizar esta tesis los dos proveedores de servicio de internet en Guatemala ofrecen servicios de cable, por lo que se concluye que los ISP de Guatemala cuentan con configuraciones *multicast* en su red.

2. La red de un ISP está conformada por enrutadores que tienen configurado MPLS y BGP para ofrecer servicios VPN capa 3 y capa 2, estos cuentan con equipos denominados P o LSR, PE o LER en ellos se configuran VPNs de capa 3 que se utilizan para crear túneles GRE y así poder transportar el tráfico *multicast* del cliente.

3. Para llevar a cabo el transporte de tráfico *multicast* de un cliente corporativo, al cliente se le debe de instalar un CE que soporte el protocolo PIM. Y contar con un enlace de datos o un enlace privado contratado al ISP con suficiente ancho de banda.

4. Existen métodos para realizar el transporte de *multicast* del cliente sobre una red MPLS estos se llaman mVPN o *multicast* VPN, y se pueden configurar de distintas maneras o con distintos perfiles. En el escenario el perfil 0, es el más recomendado para configurar.

RECOMENDACIONES

1. Realizar revisión de la configuración de MPLS y BGP en el ISP para garantizar su correcto funcionamiento para el transporte de tráfico *multicast* del cliente corporativo.

2. Realizar revisión de la configuración de *multicast* en el ISP para garantizar su correcto funcionamiento, al momento de configurar el transporte del tráfico *multicast* del cliente corporativo.

3. Revisar que el CE del cliente soporte el protocolo PIM, de no soportarlo reemplazarlo por un modelo que lo soporte, para poder configurar el transporte del tráfico *multicast* del cliente corporativo y garantizar que el ancho de banda sea suficiente para un correcto funcionamiento.

4. Considerar para la creación del diseño de transporte del tráfico *multicast* sobre la red MPLS de un ISP, tomar en cuenta que existen 26 perfiles dependiendo de las distintas necesidades que se tengan. Se debe evaluar los requerimientos del transporte para la elección del perfil para que el diseño sea el ideal.

BIBLIOGRAFÍA

1. DE GHEIN, Luc. *MPLS fundamentals*. United States of America: CISCO Press, 2007. 626 p.

2. EDGEWORTH, Bradley; GARZA RIOS, Ramiro; GOOLEY, Jason; HUCABAY, David. *CCNP, CCIE Enterprise Core ENCORE 350-401.* United States of America: CISCO Press, 2020. 973 p. ISBN-13: 978-1-58714-523-0. ISBN-10: 1-58714-523-5.

3. GUICHARD, Jim; PEPELNAK, Ivan; APCAR, Jeff. *MPLS, VPN. Architectures, Volume II*. United States of America: CISCO Press, 2003. 504 p.

4. MVPN, Multicast VPN. *Video series.* [en línea]. <https://www.youtube.com/playlist?list=PLVNDcRwt9SP2ni2a3kRRVB9_Rbe7vOMW>. [Consulta: 21 de mayo de 2021].

5. WALLACE, Kevin. *CCNP Routing and Switching ROUTE 300-101*. United States of America: CISCO Press, 2015. 880 p.

6. Youtube. *Canal decoding packets*. [en línea]. <https://www.youtube.com/playlist?list=PLVNDcRwt9SP2ni2a3kRRVB9_Rbe7vOMW>. [Consulta: 21 de mayo de 2021].