DISEÑO E IMPLEMENTACIÓN DE UN ENRUTAMIENTO REDUNDANTE USANDO EL PROTOCOLO BORDER GATEWAY PROTOCOL (BGP) PARA LA RED DE UN PROVEEDOR DE SERVICIOS DE INTERNET EN BOGOTÁ

AUTOR

CRISTHIAN SEBASTIAN PÉREZ SUAREZ

CÓDIGO: 2112897

ESTUDIANTE DE INGENIERÍA DE TELECOMUNICACIONES

UNIVERSIDAD SANTO TOMÁS

FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ, DC.

2017

DISEÑO E IMPLEMENTACIÓN DE UN ENRUTAMIENTO REDUNDANTE USANDO EL PROTOCOLO BORDER GATEWAY PROTOCOL (BGP) PARA LA RED DE UN PROVEEDOR DE SERVICIOS DE INTERNET EN BOGOTÁ

AUTOR

CRISTHIAN SEBASTIAN PÉREZ SUAREZ

CÓDIGO: 2112897

ESTUDIANTE DE INGENIERÍA DE TELECOMUNICACIONES

PROYECTO DE GRADO

DIRECTOR:

GUSTAVO ALONSO CHICA PEDRAZA

INGENIERO ELECTRÓNICO

MAGÍSTER EN INGENIERÍA DE TELECOMUNICACIONES

UNIVERSIDAD SANTO TOMÁS

FACULTAD DE INGENIERÍA DE TELECOMUNICACIONES

BOGOTÁ, DC.

2017

CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

INTRODUCCIÓN

Las grandes compañías que prestan servicio de telecomunicaciones (ISPs), se encuentran en constante crecimiento, por esta razón tienen la necesidad de aumentar y mejorar la calidad de sus redes para prestar un mejor servicio a los usuarios finales. En particular, los ISPs presentan un caso de estudio especial para ser abordado teniendo en cuenta que la tecnología que utilizan se encuentra en un cambio permanente que exige estar a la vanguardia para permanecer en un sector tan competitivo como el de las telecomunicaciones.

Considerando lo anterior, como estudiante de último semestre de ingeniería de telecomunicaciones se da la opción de realizar un diagnóstico técnico a la red de un ISP que por cuestiones de confidencialidad se llamará en el transcurso del documento **"ISP Ejemplo.Compañia"**. Este requerimiento se dio como resultado de los contactos realizados durante la realización de los módulos correspondientes al CCNP de Cisco.

Después de realizar el diagnostico, se encontraron las siguientes fallas: la red cuenta con dispositivos de red que no tienen utilidad en el diseño que se diagnostica, además de tener enlaces hacia Internet que se encuentran deshabilitados por el administrador, haciendo manual su redundancia y vulnerable a fallas, utiliza diversos protocolos de enrutamiento donde sería ideal utilizar uno solo, según la topología de la red LAN del ISP no se evidencia redundancia, sería ideal contar con un protocolo de redundancia ya sea Hot Standby Router Protocol (HSRP) o Virtual Router Redundancy Protocol (VRRP). A causa de las fallas mencionadas, los clientes del ISP se están quedando sin servicio de acceso a internet por prolongados lapsos de tiempo.

Con el presente documento se pone en práctica bases teóricas y prácticas de routing y switching que se adquirieron durante las asignaturas cursadas en la carrera y los módulos del curso CCNP de Cisco.

Este documento se encuentra estructurado de la siguiente manera: definición del problema, justificación, objetivo general, objetivos específicos, marco referencial, desarrollo del proyecto y, resultados de las pruebas realizadas del diseño de red del ISP Ejemplo.Compañia, conclusiones basadas en las mejoras del nuevo diseño implementado en la red del ISP y en las buenas prácticas para la configuración de los protocolos BGP y HSRP, obteniendo cono resultado una redundancia automática en la red LAN.

1. DEFINICIÓN DEL PROBLEMA

Al realizar el diagnostico técnico al “ISP Ejemplo.Compañía”, el cual presta servicios a distintos clientes como corporativos y pymes, se evidencia que existen fallas en su diseño de red, particularmente en la red WAN del ISP. Adicionalmente el uso equivocado de equipos de red como el Firewall Mikrotic, la falta de redundancia en la topología de red, y la vulnerabilidad a fallas ponen en riesgo el servicio que presta a los clientes. Por otra parte el ISP da mal uso de los recursos con los que cuenta y utiliza diversos protocolos de enrutamiento tales como los protocolos Open Shortest Path First (OSPF) Y Enhanced Interior Gateway Routing Protocol (EIGRP propiedad de CISCO), causando mayor procesamiento y generando mayor gasto de tiempo en el momento de transportar un paquete de un origen a su destino.

El diseño de red del ISP que se analiza cuenta con enlaces Backup de conexión hacia Internet que se encuentran deshabilitados, si alguno de los enlaces principales llegase a tener problemas, se perdería la conexión del ISP hacia internet, presentando un incidente el cual podría afectar la disponibilidad del servicio en su totalidad, afectando así al cliente final.

En la **Figura 1** se aprecia la topología de red del ISP Ejemplo.Compañia, en la que se evidencia los inconvenientes más significativos que contiene la topología red:

A Hay, enlaces hacia Internet que se encuentran deshabilitados por el administrador, haciendo manual su redundancia y vulnerable a fallas que se pueden generar en la red del ISP.

B La disponibilidad de servicio está atada a cambios manuales en la red por parte del administrador.

C Existen puntos únicos de falla que afectarían el servicio en un cien por ciento (100%).

D Utiliza diversos protocolos de enrutamiento donde sería ideal utilizar uno solo.

Por la variedad de inconvenientes y problemas encontrados en el diseño de red del ISP se plantea la siguiente pregunta problema a resolver:

¿Cómo implementar un sistema redundante que a su vez contemple la forma de que mitigue fallos en la red del ISP Ejemplo.Compañía?

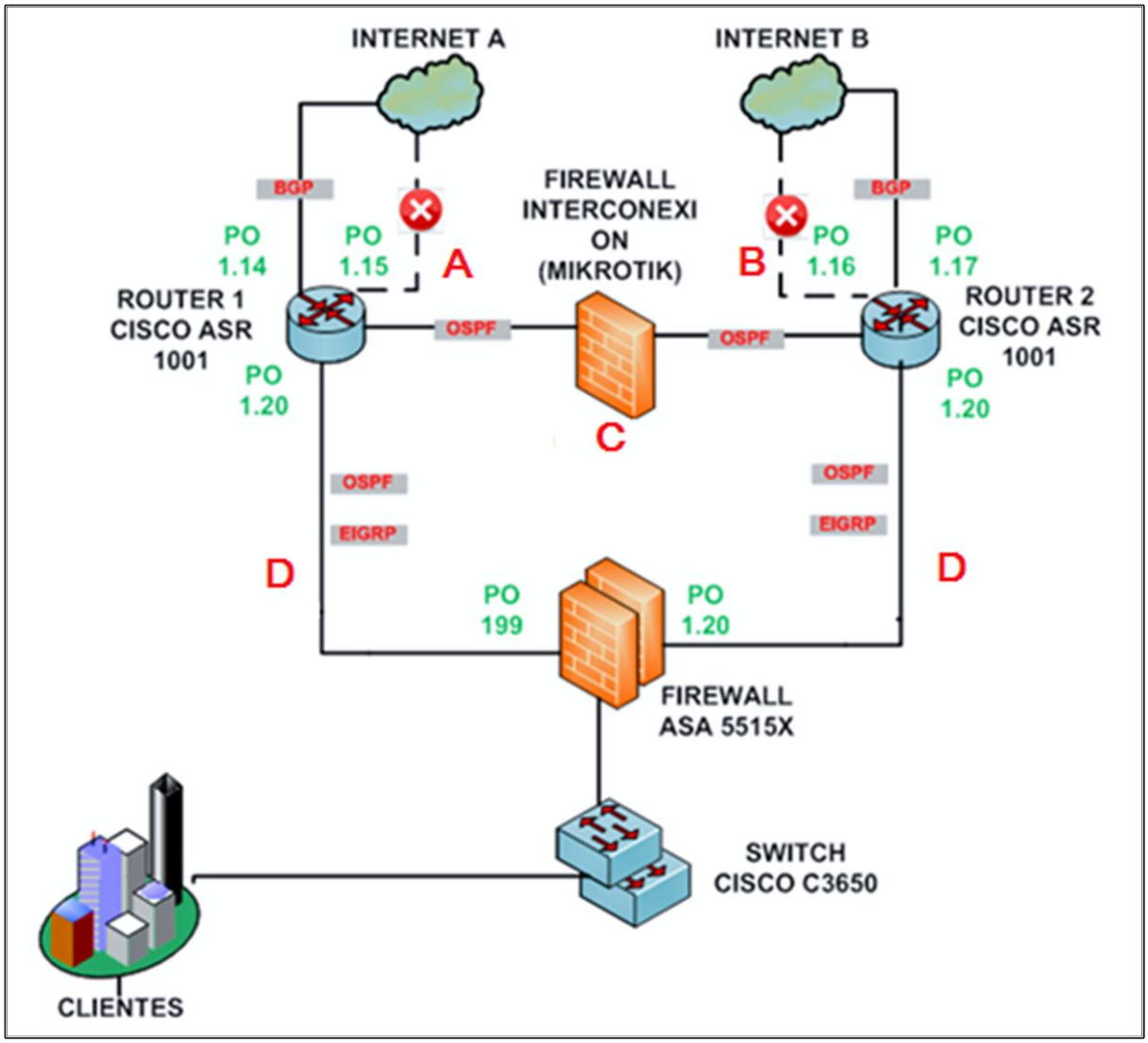


Figura 1: Diseño de red antiguo del ISP

2. JUSTIFICACIÓN

Con este proyecto se pretende dar solución a los problemas de diseño de red del ISP Ejemplo.Compañía, mejorando su desempeño, disponibilidad y convergencia ante fallas de la red. En el desarrollo de este proyecto se aplican conocimientos importantes de Telemática y Troubleshooting, adquiridos durante la carrera y fortalecidos durante los cursos de Routing y Switching de CISCO CCNP.

Por lo anterior este proyecto tiene el objetivo de realizar un nuevo diseño de red, solucionando los principales problemas que tiene la topología de red del ISP como son: el enrutamiento dinámico y la optimización de los recursos de red, utilizar y habilitar los enlaces Backup para que en dado caso de llegar a ocurrir un problema en el enlace principal que tiene conexión a internet el enlace Backup pueda mitigar el problema y así evitar una caída total del servicio que se presta a los diferentes clientes del ISP Ejemplo.Compañía, en otras palabras hacer que la red tenga una redundancia solida utilizando los enlaces principales y Backups con los que cuenta la red.

Esta solución va encaminada a realizar un correcto diseño que pueda enviar en todo momento la cantidad de paquetes de datos que el cliente necesite y el dispositivo de red permita, además de tener una red tolerante a fallas en los enlaces principales y Backups que se conectan con internet. Es de aclarar que el nuevo diseño de red que se va a realizar no es el único capaz de solucionar los inconvenientes de la red del ISP Ejemplo.Compañía, debido a que existen diferentes formas de interpretar e implementar un diseño de red nuevo; este diseño se realiza con bases teóricas y prácticas que se adquirieron durante las asignaturas cursadas en la carrera y los módulos cursados de CCNP.

4. OBJETIVOS

3.1 OBJETIVOS GENERALES

Diseñar la red que solucione la problemática del **ISP Ejemplo.Compañía**, mediante la utilización de un protocolo de redundancia en la red LAN y un protocolo de enrutamiento dinámico que optimice los recursos de red, para generar estabilidad y alta disponibilidad en el momento de conectarse a la red de Internet.

3.2 OBJETIVOS ESPECÍFICOS

- Identificar los errores más significativos que tiene la red del ISP Ejemplo.Compañia.
- Utilizar adecuadamente los recursos de los dispositivos con los que cuenta la red del **ISP Ejemplo.Compañía**.
- Reducir la cantidad de protocolos de enrutamiento en la red del ISP, para hacer que la red del ISP optimice recursos de procesamiento.
- Utilizar protocolos como HSRP para permitir que la red del ISP tenga redundancia de forma automática.
- Realizar pruebas que demuestren que en caso de una caída o falla de un enlace principal, el enlace Backup mitigara y permitirá que siga la conectividad con el enlace vecino.

5. MARCO REFERENCIAL

4.1 PROVEEDOR DE SERVICIOS DE INTERNET (ISP)

Los ISP son empresas que se enfocan en brindan el servicio de conexión a Internet, son los intermediarios entre el usuario y la conexión a Internet. Se identifican porque estas empresas no interactúan en las peticiones de sus usuarios, simplemente se encargan de transportar e interconectar el tráfico de sus clientes a Internet, no se involucran en la selección de origen o destino de sus clientes. (David Álvarez, 2009)
Existen diferentes tipos de proveedores de servicios de Internet como:

- **ISP de Acceso:** Este tipo de ISP como su nombre lo indica ofrece acceso a la red, utiliza diversas tecnologías para facilitar el acceso de sus clientes a Internet, alguna de estas tecnologías contienen líneas de cobre, servicios de fibra óptica, Digital Subscriber Line (DSL) y conexión inalámbricas como satelital, Wi-Fi y acceso a celular, estas tecnologías se prestan dependiendo a la necesidad de los clientes. (Gazmuri, 2008)

- **ISP de Buzón de correo:** Esta clase de ISP se encarga de alojar dominios de correo electrónico con acceso a almacenamiento de los buzones de correo. Facilita a los clientes servidores de correo electrónico para recibir, enviar, aceptar y almacenar correos electrónicos. Algunos proveedores de buzón de correo son empresas como: Yahoo! Mail, Outlook.com, Gmail, AOL Mail entre otras empresas prestadoras de buzón de correo.(Kucherawy, 2012)

  El RFC 6650 cubre los servicios de alojamiento de correo electrónico, servicios competentes de empresas, universidades, organizaciones, grupos e individuos que administran sus propios servidores de correo. Esta tarea se realiza gracias al Protocolo Simple de Transferencia de Correo (SMTP) y también gracias a Internet Message Access Protocol (IMAP). (Kucherawy, 2012)

- **ISP de Transito:** Este tipo de ISP es el encargado de interconectar a los ISP de acceso, los ISP de tránsito o también llamados Tier 1 o ISP de nivel 1, generalmente tiene una red de mayor tamaño y una gran capacidad de ancho de banda. Un ISP de

acceso puede tener diversas conexiones hacia el ISP de tránsito para poder brindar un mejor servicio a usuarios finales. (Kucherawy, 2012)

En la **Figura 2** se contempla la distribución de conectividad de internet entre los ISP.

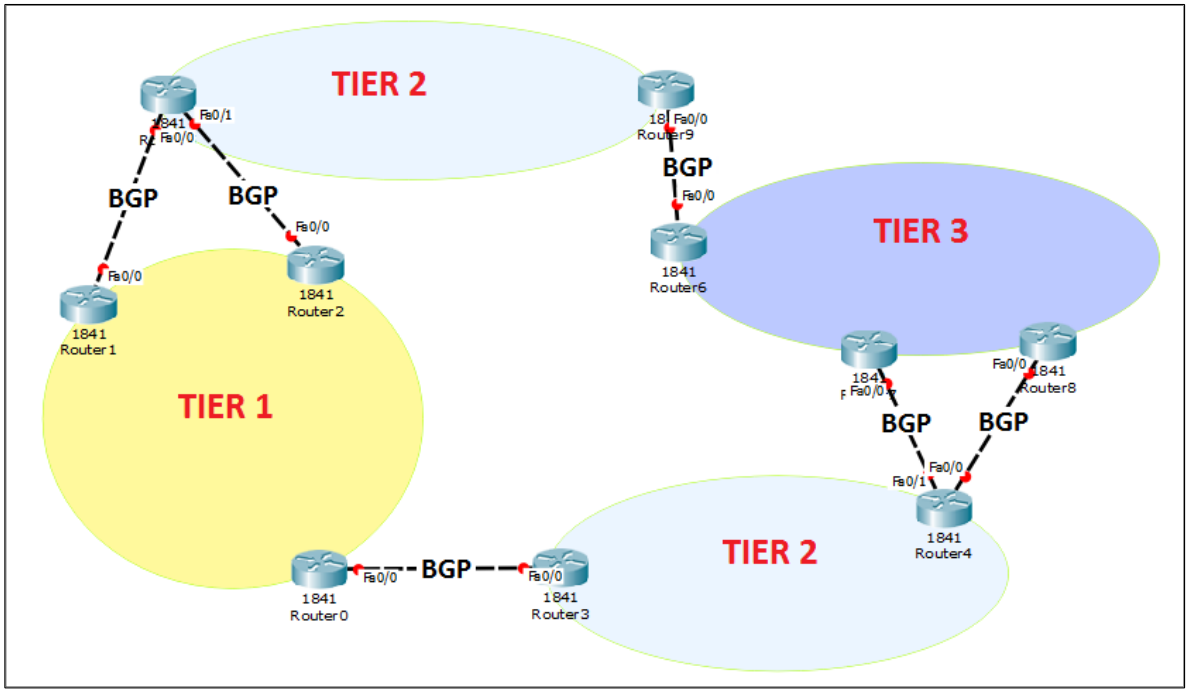


Figura 2: Distribución de conectividad de internet.

- **ISP Virtuales (VISP):** Este tipo de ISP compra o renta el acceso a Internet a otro ISP y luego revende el servicio a los usuarios finales. La función principal de este tipo de ISP no es solo proveer servicios de conectividad a internet sino también provee servicios como: correo electrónico, soporte técnico y alojamiento web o técnicamente conocido como Hosting (Gazmuri, 2008).
- **ISP Gratuitos (Freenets):** Esta clase de ISP proporciona servicios de Internet de forma gratuita, algunos de ellos para financiar la tecnología e infraestructura utilizada muestran anuncios publicitarios y comerciales de televisión. (Gazmuri, 2008).

4.2 IPv4 (Internet Protocol Versión 4)

El protocolo IPv4 tiene unas direcciones de longitud de 32 bits. Estos 32 bits son divididos en 4 octetos, cada octeto con una longitud de 8 bits.

Una forma básica de entender la numeración en binario es tener claro que esta numeración está representada por el número (0 o 1), si tomamos un octeto como ejemplo, en cada posición del octeto multiplicado por el número 2 a la potencia de la posición, comenzando por 0 y aumentando hasta 7, de derecha a izquierda. (Rafael Moreno, 2010)

Se aprecia en la **Figura 3** un ejemplo de un número binario de 8 dígitos.

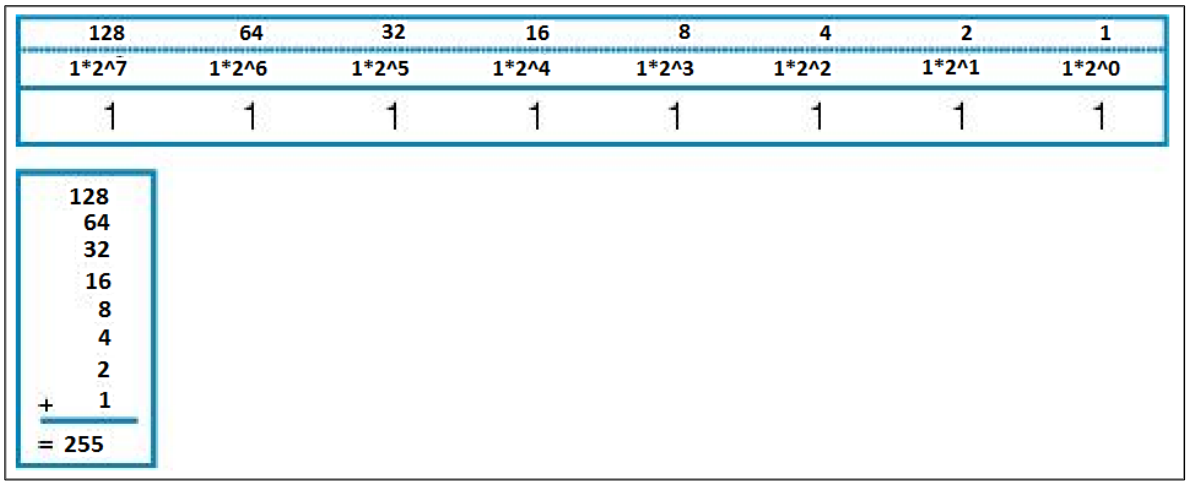


Figura 3: Ejemplo de un número binario de 8 dígitos. (CISCO, IP Addressing: IPv4 Addressing, 2011)

Una dirección de host IP se encarga de identificar un dispositivo en el que se pueden enviar paquetes IP. Las direcciones IP identifican redes de segmento de la red a la que uno o más hosts se pueden conectar. Algunas de las características de IPv4 son las siguientes(Oviedo, 2006):

- Las direcciones IP son de 32 bits de longitud.
- Las direcciones IP se dividen en cuatro secciones de un byte (8 bits o un octeto).
- Las direcciones IP son típicamente escritos en un formato conocido como decimal con puntos.

En la **Tabla 1** se muestra algunos ejemplos de direcciones IP en decimal y respectivamente en binario.

Dirección IP en decimal	Dirección IP en binario
10.34.216.75	00001010.00100010.11011000.01001011
172.16.89.34	10101100.00010000.01011001.00100010
192.168.100.4	11000000.10101000.01100100.00000100

Tabla 1: Ejemplo de direcciones IP. (CISCO, IP Addressing: IPv4 Addressing, 2011)

4.2.1 CLASE DEDIRECCIONES IPV4

Con el fin de proporcionar una estructura a la forma de direcciones IP, se agrupan en diferentes clases que van desde la clase A hasta la clase E. cada clase tiene un rango de direcciones IP determinado por el número de bits asignado a la sección de red de la dirección IP de 32 bits. El número de bits de la sección de esta red está representado por una máscara de red, está es escrita en decimal y se identifica en la mayoría de casos de la siguiente manera ***/n*** donde n es el número en decimal de la máscara. (Nava, 2008)

En la **Tabla 2** se aprecia los rangos de las clases de direcciones IP con sus respectivas mascaras de red asociadas a cada clase:

CLASE	RANGO	MASCARA
A	1.0.0.0 – 126.255.255.255	255.0.0.0
B	128.0.0.0 – 191.255.255.255	255.255.0.0
C	192.0.0.0 – 223.255.255.255	255.255.255.0
D	224.0.0.0 – 239.255.255.255 (Multicast)	Reservado multicast no tiene mascara
E	240.0.0.0 – 254.255.255.255 (Experimental)	Reservado para fines experimentales no tiene mascara

Tabla 2: Clases de direcciones IPv4.

Clase A: Esta clase establece un número máximo de redes de 128, cada una de estas redes con 16 millones de hosts. Los primeros 8 bits se asignan a red y los siguientes 24 son asignados a los host. (Ahuatzin, 2009)

Las direcciones de red de clase A 127.0.0.0 son utilizadas con funciones de bucle de prueba para el propio host estas direcciones también son llamadas direcciones del propio host. (Oviedo, 2006)

Clase B: Establece un máximo de 26382 redes con 64000 host cada una. Los primeros 16 bits establecen la red y los siguientes 16 bits son asignados a host. (Ahuatzin, 2009)

Clase C: Registra hasta 2 millones de redes cada una con 256 host. Los primeros 24 bits establecen las redes y los 8 bits restantes son utilizados para los hosts.

Las direcciones Clase D y E no pueden ser utilizadas como direcciones de origen, estas direcciones se usan de forma especial

Clase D: reservadas para redes multicast, desde 224.0.0.0 hasta 239.255.255.255 (RFC3171).

Clase E: esta clase es de uso experimental, desde 240.0.0.0 hasta 254.255.255.255 (RFC1700).

El RFC 1918 define las direcciones privadas o no ruteables. Ninguna dirección contenida en estos rangos que se observan en la **Tabla 3** no podrá ser utilizada en una dirección IP pública o de acceso a internet.

CLASE	RANGO	MASCARA
A	10.0.0.0 – 10.255.255.255	8 bits red – 24 bits host
B	172.16.0.0 – 172.31.255.255	12 bits red – 20 bits host
C	192.168.0.0 – 192.168.255.255	16 bits red – 16 bits host

Tabla 3: Rango direcciones privadas.

Estas direcciones privadas no se utilizan como direcciones globales en Internet. Son exclusivamente reservadas para redes no conectadas a internet y por tanto se pueden

utilizar dentro de las redes internas de compañías o intranets. Para que estas redes se conecten a Internet es necesario utilizar Network Address Translation (NAT) que su función es transformar o convertir estas direcciones privadas en direcciones públicas para así ser validas en Internet. (Mayán, 2010)

4.3 PROTOCOLOS DE ENRUTAMIENTO

Un protocolo de enrutamiento es un conjunto de reglas que son usadas por elementos de red como los routers cuando estos se comunican con otros routers con el objetivo de intercambiar información de enrutamiento. Los protocolos de enrutamiento se dividen en enrutamiento estático y enrutamiento dinámico.(Alcalá, 2011)

4.3.1 ENRUTAMIENTO ESTÁTICO

Son rutas que se configuran manualmente se usan para el enrutamiento desde una red hasta una red de conexión única en la **Figura 4** se observa un ejemplo del funcionamiento de una conexión por rutas estáticas.(CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007)

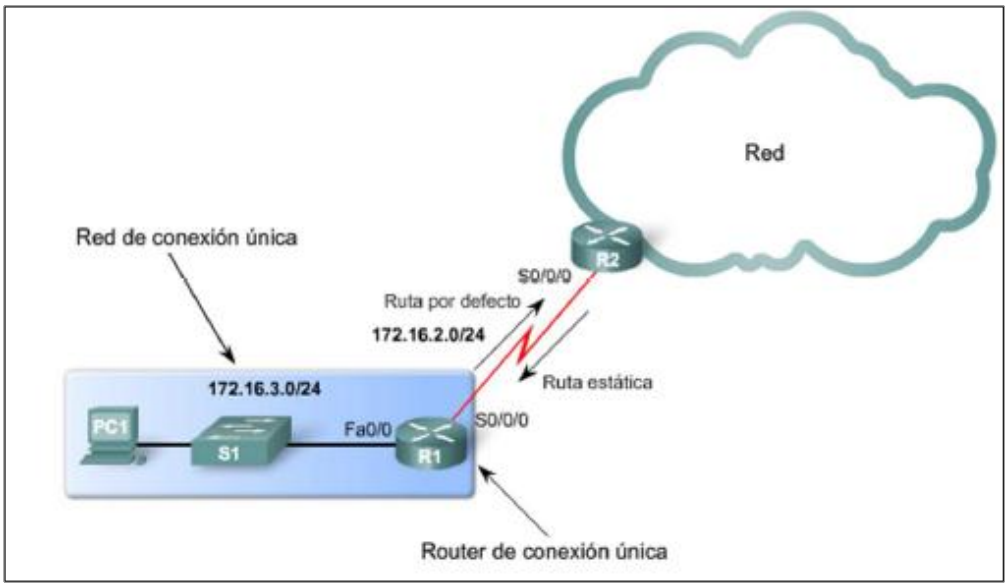


Figura 4: Función de una ruta estática. (CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007)

El comando utilizado para la configuración de rutas estáticas es el siguiente:

Router (config) # iproute {dirección_red} {mascara_ subred} {dirección ip* | *interfaz de salida}

En ***dirección de red*** se utiliza la dirección IP que se quiere ser enrutada, seguido de su respectiva mascara de red. La ***dirección IP* | *interfaz de salida*** se utiliza la dirección IP de la interfaz por la que se quiere enrutar a la siguiente red del router vecino.(Veracruzana, 2014)

Para una buena configuración de rutas estáticas se recomienda los tres principios de enrutamiento de Zinin (CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007):

Principio 1: "Cada router toma decisiones de forma independiente, sobre la base de la información que contiene en la tabla de enrutamiento". (CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007)

Principio 2: "el hecho de que un router tenga cierta información en su tabla de enrutamiento no significa que los demás routers contengan la misma información". (CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007)

Principio 3: la información de enrutamiento acerca de una ruta que va desde una red hasta otra no proporciona información de enrutamiento acerca de la ruta en sentido contrario o ruta de regreso". (CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007)

Para la verificación de la configuración de las rutas estáticas se deben utilizar los siguientes comandos.

Show running-config: este comando muestra toda la configuración que tiene el dispositivo.

Show ip route: este comando muestra la tabla de enrutamiento del router.

Ping: comando utilizado para verificar que los paquetes lleguen al destino y que la ruta de regreso funcione.

4.3.2 ENRUTAMIENTO DINÁMICO

Los protocolos de enrutamiento dinámico mantienen tablas de información de forma dinámica entre routers, además de actualizar las tablas de enrutamiento de forma automática cada vez que la topología de la red cambia, el enrutamiento dinámico determina cual es la mejor ruta que debe tomar un paquete para llegar a su destino.

Los protocolos de enrutamiento dinámico tienen el objetivo de descubrir redes remotas, mantener la información de enrutamiento actualizada además de seleccionar la mejor ruta a redes de destino. Ofrece la funcionalidad necesaria para encontrar una nueva mejor ruta si la ruta actual deja de estar disponible. (UPM, 2013)

El enrutamiento dinámico se clasifica en dos tipos de protocolo de enrutamiento, como son el Interior Gateway Protocol (IGP) y Exterior Gateway Protocol (EGP).

- **IGP** se utiliza dentro de un Sistema Autónomo (SA) y dentro de redes individuales. Los protocolos que se agrupan en IGP son: Routing Information Protocol (RIP), Interior Gateway Routing Protocol (IGRP), Enhanced Interior Gateway Routing Protocol (EIGRP propiedad de CISCO), Intermediate System to Intermediate System (IS-IS), Open Shortest Path First (OSPF).

  Existen algoritmos de enrutamiento que son utilizados para facilitar información de enrutamiento y determinar la mejor ruta, estos algoritmos son los siguientes(Gonzalez, 2010)

  Vector Distancia: este algoritmo determina la dirección y la distancia hacia cualquier enlace de la red. La métrica del vector distancia se basa en el número de saltos, es decir la cantidad de routers por los que tiene que atravesar el paquete para llegar a la red de destino, la ruta que tenga el menor número de saltos es la elegida y la que se publicara en la tabla de enrutamiento. (CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007)

  Estado de Enlace: este algoritmo se basa en retardo, ancho de banda, carga y confiabilidad, de los diferentes enlaces posibles para llegar a la red de destino, en base a los conceptos nombrados el protocolo escogerá la mejor ruta por la que los paquetes se transportaran.

  El algoritmo de estado de enlace usa Link State Advertisement (LSA), que intercambian entre los routers y gracias a esta información los routers crean una base

de datos de la topología de red completa; las actualizaciones de estado de enlace no son periódicas a comparación de el algoritmo vector distancia que realiza actualizaciones periódicas. (CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007)

Los protocolos de enrutamiento utilizan **métricas** para determinar que rutas son mejores que otras. La métrica es el análisis y en lo que se basa el algoritmo de protocolo de enrutamiento dinámico para seleccionar una ruta sobre otra, basándose en eso el protocolo crea la tabla de enrutamiento en el router publicando solo las mejores rutas. (Goita, 2003)

Las métricas utilizadas por los protocolos de enrutamiento IP son:

- Ancho de banda: capacidad de datos de un enlace.
- Costo: el costo se basa en el ancho de banda (BW).
- Retraso: cantidad de tiempo que tarda un paquete en atravesar una ruta.
- Conteo de saltos: número de routers por los que pasa un paquete.
- Carga: considera la utilización de tráfico de un enlace determinado.
- Confiabilidad: valor de errores de bits de cada enlace.

Las cifras de estas métricas se almacenan en la tabla de enrutamiento de cada router. Cada protocolo de enrutamiento utiliza una métrica distinta, en la **Tabla 4** se aprecia que métrica utiliza cada protocolo de enrutamiento IGP.

PROTOCOLO	**MÉTRICA**
RIP	Conteo de Saltos
IGRP – EIGRP	Ancho de banda (usado por defecto), Retraso (usado por defecto), carga, confiabilidad
IS-IS – OSPF	Costo, Ancho de banda

Tabla 4: Métricas que se usan para cada protocolo de enrutamiento.

Si dos o más rutas tienen el mismo valor de métrica el router realiza un **balanceo de carga** entre estas dos rutas del mismo costo. El router distribuye la carga de paquetes entre las rutas que tienen el mismo costo(CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007).

En la **Figura 5** se observa un ejemplo de cómo se realiza el balanceo de carga entre dos rutas que tienen el mismo costo.

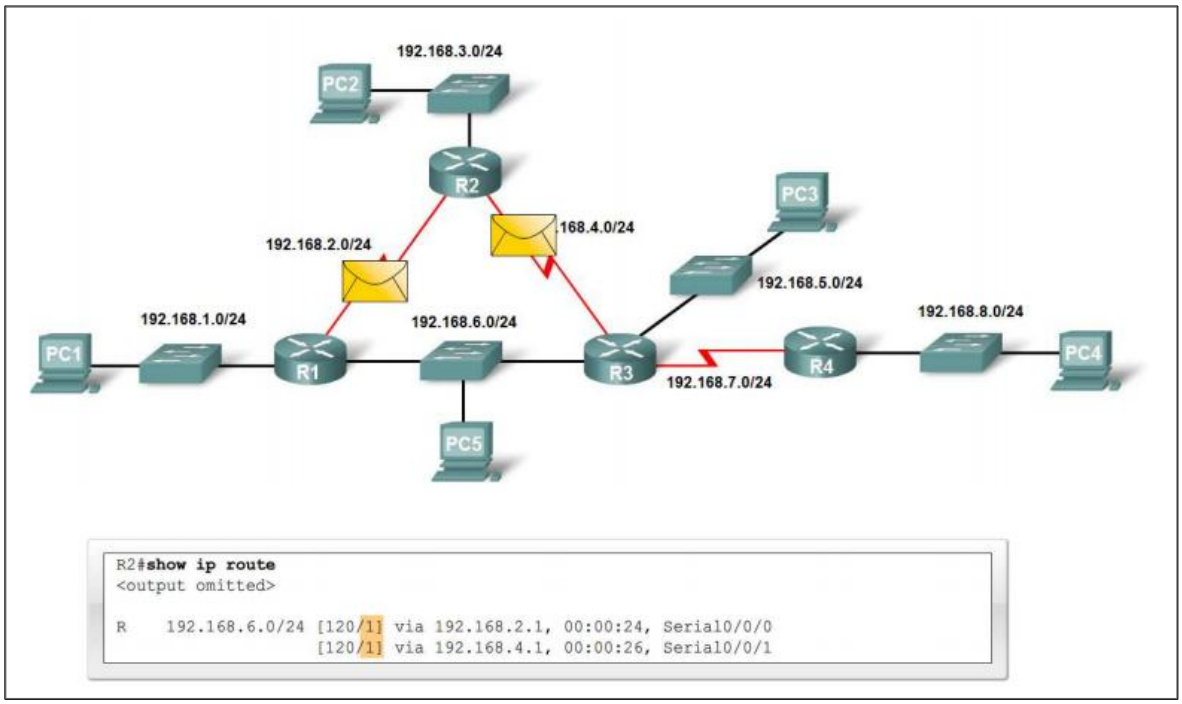


Figura 5: Ejemplo de balanceo de carga. (CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007)

DISTANCIA ADMINISTRATIVA (AD): es un valor que especifica la preferencia por una ruta determinada, cada protocolo de enrutamiento lleva asociada una distancia administrativa. Entre más bajo sea el valor de la distancia administrativa significa una mayor fiabilidad; un router puede implementar varios protocolos de enrutamiento a la vez.

En la **Tabla 5** se contempla cada una de las distancias administrativas que tiene cada protocolo de enrutamiento. (CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007)

Origen de la ruta	Distancia administrativa
Conectado	0
Estática	1
Ruta Sumarizada EIGRP	5
BGP externo	20
EIGRP interno	90
IGRP	100
OSPF	110
IS-IS	115
RIP	120
EIGRP externo	170
BGP interno	200

Tabla 5: Distancia administrativa predeterminadas.(CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007)

- **EGP** se usa para el enrutamiento entre Sistemas Autónomos (SA), el protocolo que se utiliza en EGP es Border Gateway Protocol (BGP), en la **Figura 6** se observa cómo se clasifica los protocolos de enrutamiento dinámico.

  BGP funciona de manera diferente a los IGP por que no toma decisiones de enrutamiento basadas en métricas de mejor ruta. Los routers que hablan BGP o BGP speaker intercambian atributos de red incluyendo una lista de rutas completa de números de sistemas autónomos que un router debe tener en cuenta para llegar a una red de destino. (Overview, 2011)

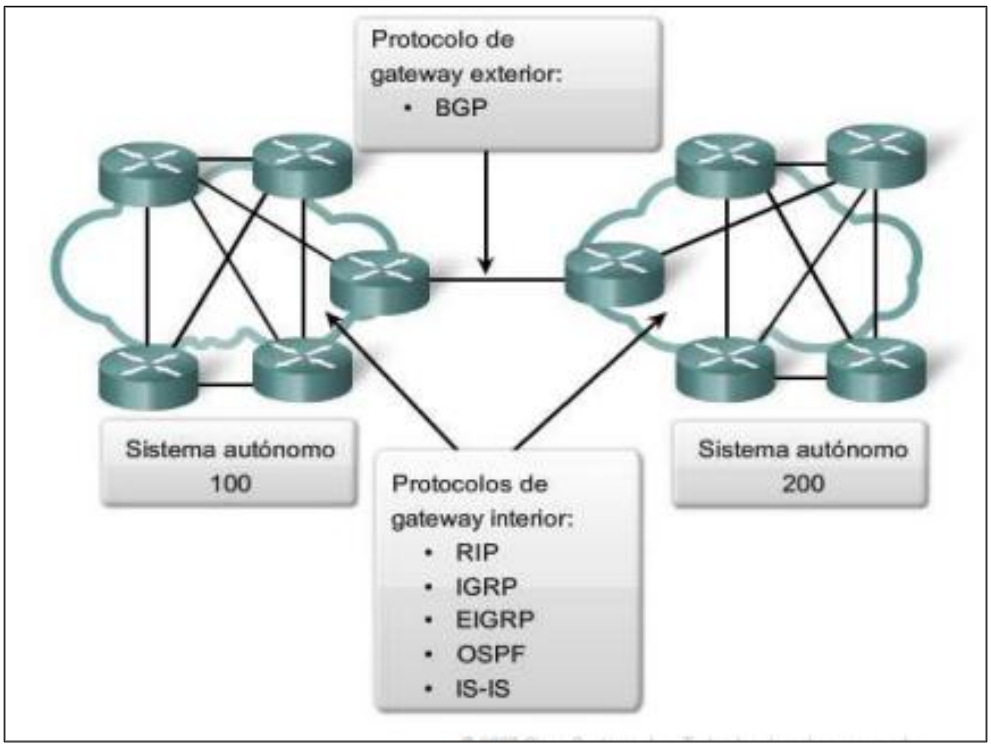


Figura 6: Clasificación de los protocolos de enrutamiento dinámico.(CISCO, Conceptos y Protocolos de Enrutamiento Capítulo 2, 2007)

Sistema Autónomo (SA): un SA es un grupo de routers que comparten políticas de enrutamiento similares y operan dentro de un único dominio administrativo; los números SA son administrados por la Internet Assigned Numbers Authority (IANA), si un SA se conecta al internet público utilizando un protocolo EGP como Border Gateway Protocol (BGP) entonces se le asigna un numero de SA único que es administrado por la IANA.

La IANA es responsable de asignar números de SA a través de cinco Registros Regionales de Internet (RIRs). Los RIR son corporaciones sin fines de lucro establecidas con el propósito de administrar y registrar el espacio de direcciones IP y números de SA en ubicaciones geográficas claves. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Como se aprecia en la **Figura 7** la RIR se divide en cinco regiones en el mundo que se dividen en las siguientes:

- **AfricNIC:** se encarga de administrar la región del continente de África,
- **APNIC:** su función es la administración de números de SA en la región de Asia,

- **ARIN:** se encarga de la administración de números de SA de Canadá y Estados Unidos,
- **LACNIC:** se encarga de administrar los números de SA de la región de Suramérica y cetro América,
- **RIPE:** se encarga de la administración de Europa, Medio Oriente y el centro de Asia; de esta manera se divide la RIRs.

Figura 7: Registros regionales de internet.(CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Los números de SA pueden estar entre 1 y 65.535, los RIR administran los números entre el 1 y el 64512, los números restantes son usados para uso privado similar a las direcciones IP privadas. Se prevé que el actual grupo de direcciones de SA se agote pronto, por esta razón, la IETF publica los RFC 4893 y RFC 5398 que describen la extensión del número de SA de 16 bits a un campo de 32 bits, aumentando el tamaño de la agrupación de 65.536 a 4.294.467.296 valores. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

4.3.3 BORDER GATEWAY PROTOCOL (BGP)

El protocolo Border Gateway Protocol (BGP) se define en el RFC 1771. La función principal de un sistema que utiliza BGP es intercambiar información con otros sistemas BGP, ya sea que tengan diferente o el mismo Sistema Autónomo (SA). La red de comunicación que se crea entre protocolos BGP, transmite información sobre los respectivos SA, esta información es suficiente para construir un gráfico de la conectividad entre SA, reduciendo Loops de interdominio y algunas políticas a nivel de SA. BGP utiliza Transmission Control Protocol (TCP) como su protocolo de transporte, utiliza el puerto TCP 179 para establecer sus conexiones. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Internet es un grupo de diversos SA que se encuentran interconectados para permitir la comunicación entre ellos, proporcionando el camino entre estos SA. BGP es un protocolo Path Vector y es el único protocolo de enrutamiento dinámico que utiliza el protocolo TCP.

Existen diversas versiones de BGP la versión más reciente es la versión 4 (BGP – 4), esta es la última versión de BGP y se define en el RFC 4271 de junio del 2006, la diferencia de esta nueva versión respecto a las anteriores es que BGP – 4 soporta supernetting, CIDR y VLSM, además esta nueva versión de BGP impide que la tabla de enrutamiento de Internet sea demasiado grande. (Balchunas, 2007)

Cuando se utiliza CIDR en un router para un ISP, la tabla de enrutamiento IP, que está compuesta principalmente por rutas BGP, tiene más de 300.000 bloques CIDR. No utilizar CIDR en el nivel de Internet haría que la tabla de enrutamiento IP tenga más de 2.000.000 de entradas. El uso de CIDR y por lo tanto de BGP-4 evita que la tabla de enrutamiento de Internet sea demasiado grande para interconectar a millones de usuarios. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

BGP peer o BGP neighbor: estos dos términos se utilizan cuando el protocolo BGP ha establecido una comunicación con un vecino. Los dos routers que han formado una conexión TCP para intercambiar información de rutas BGP se denominan BGP peers o BGP neighbor, gracias a la comunicación establecida entre los vecinos BGP estos aprenden los caminos que cada uno de los vecinos tienen en su respectiva tabla de enrutamiento. En la **Figura 8** se aprecia un ejemplo de cómo se establecen los BGP neighbor. (Navarra, 2012)

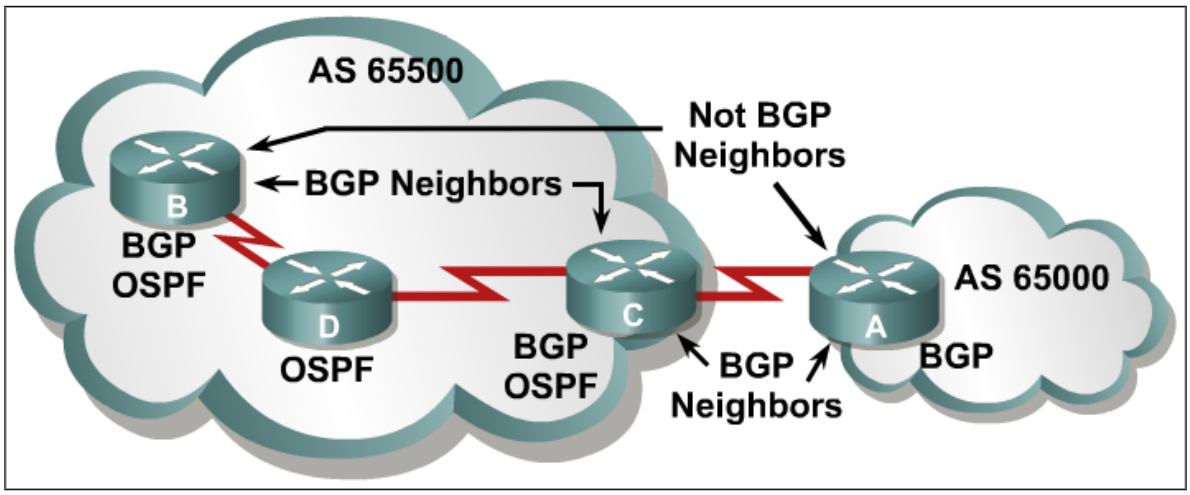


Figura 8: Funcionamiento de BGP neighbor o peers.(CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Conexión Redundante: Una conexión redundante es cuando se tienen diversos enlaces de un cliente hacia un Proveedor de Servicios de Internet (ISP), cuando una conexión de un cliente hacia un ISP no utiliza redundancia, esta se conoce como single Homed, pero tiene un problema, si la red del ISP falla, la conectividad que tiene el cliente hacia el ISP se verá interrumpida por tanto esta conexión no es redundante (Litoral, 2010).

Si un cliente está conectado a múltiples ISPs, la conexión es redundante y se conoce como conexión Multi-Homed. Existe otro tipo de conexión que se denomina dual Multi-Homed este método de conexión a ISPs aumenta la redundancia, debido a que el cliente puede tener dos enlaces hacia cada ISP. En la **Figura 9** se contempla los cuatro distintos tipos de conexión hacia un ISP como son el Single Homed, Dual Homed, Multi-Homed y Dual Multi-Homed.(CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

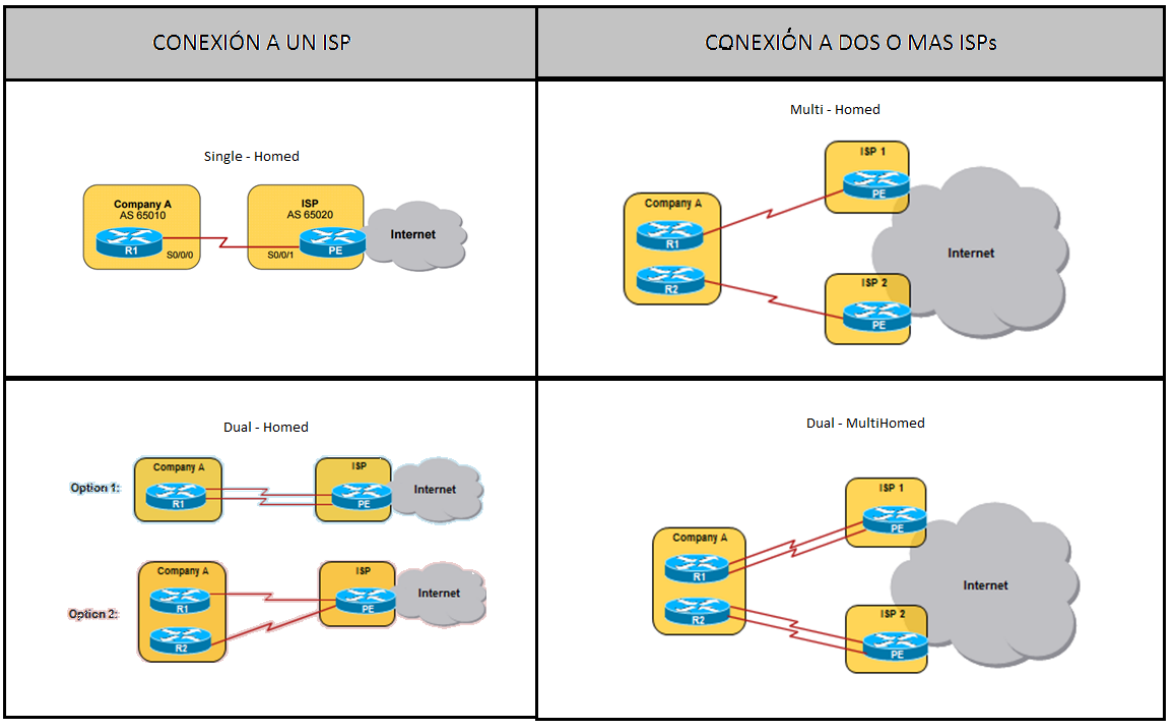


Figura 9: Tipos de conexión hacia un ISP. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Single Homed: el tipo de conexión hacia un ISP depende de la oferta que el cliente tenga con el ISP. En la **Figura 10** se observa una conexión single Homed con dos opciones de configuración:

Opción 1*:* se usa una ruta estática predeterminada del cliente al ISP y rutas estáticas del ISP hacia las redes del cliente.

Opción 2*:* cuando se utiliza BGP el cliente anuncia dinámicamente sus redes públicas y el ISP propaga una ruta predeterminada al cliente.

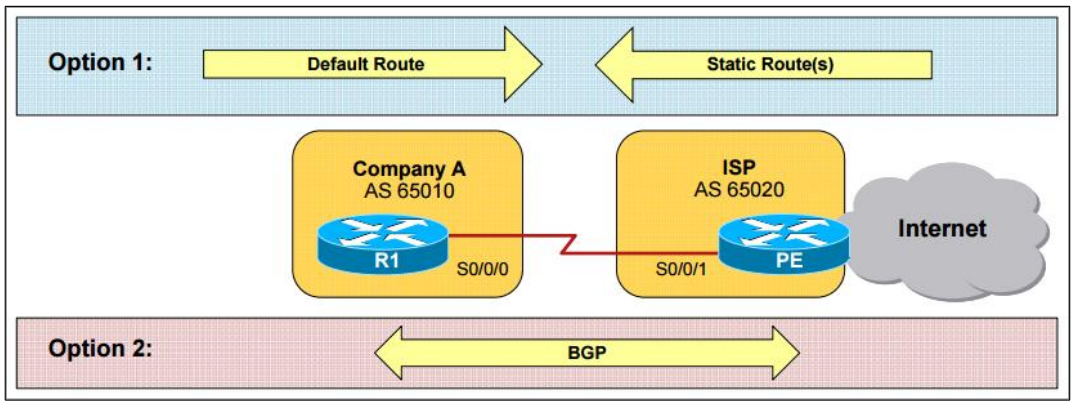


Figura10: Conexión Single Homed. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Dual Homed: Consta de la existencia de dos enlaces del cliente hacia el ISP, permitiendo más flujo de tráfico hacia el ISP. Como se puede ver en la **Figura 11** dos métodos u opciones para el uso de la conexión Dual Homed:

Opción 1*:* ambos enlaces pueden conectarse a un router de cliente.

Opción 2*:* para mejorar la resiliencia, los dos enlaces pueden terminar en routers separados en la red del cliente.

Estas opciones de despliegue de enrutamiento incluyen funcionalidad de enlace primario y de respaldo en caso de fallo del enlace principal, además de cargar el uso compartido mediante Cisco Express Forwarding (CEF). Independientemente el enrutamiento puede ser estático o dinámico (BGP). (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

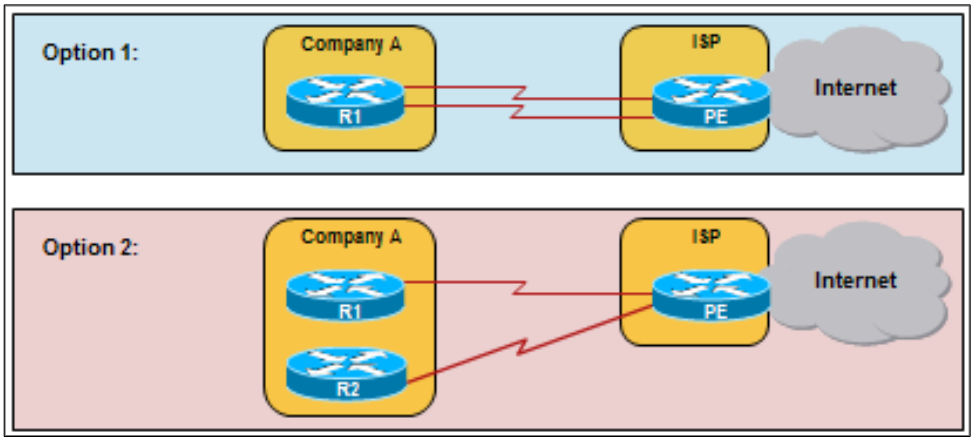


Figura 11: Conexión Dual Homed. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Multi-Homed: las conexiones de un cliente a diferentes ISP pueden terminar en un único router del cliente o en routers diferentes para mejorar aún más la resiliencia. En este tipo de conexiones los routers deben ser capaces de reaccionar a los cambios dinámicos por lo tanto se utiliza el protocolo dinámico BGP. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Esta conexión Multi-Homed incluyen beneficios como:

- Carga compartida para diferentes redes de destino entre los ISP.
- Resistencia a un fallo de un solo ISP.
- Escalabilidad de la solución, más allá de dos ISP.
- Conseguir una solución independiente del ISP.

En la **Figura 12** se muestra un ejemplo de la conexión Multi-Homed.

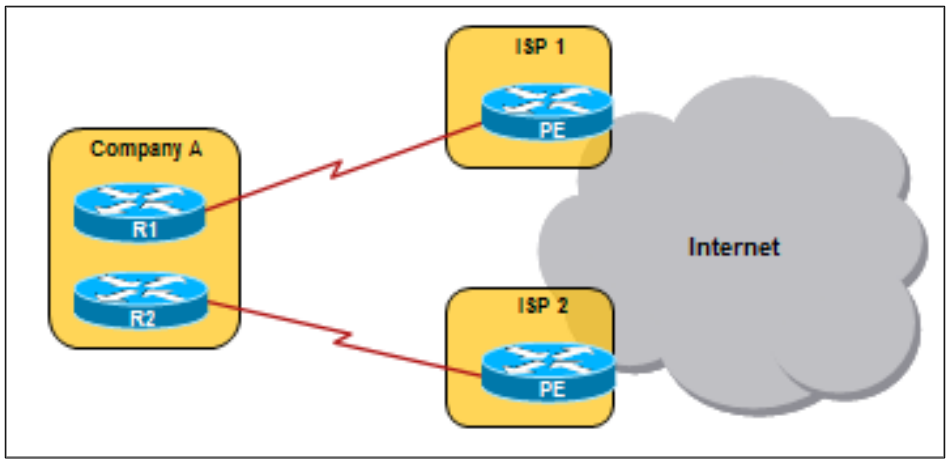


Figura 12: Conexión Multi-Homed.(CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Dual Multi-Homed: esta conexión incluye todos los beneficios de la conectividad Multi-Homed, con resiliencia mejorada. La configuración normalmente tiene múltiples routers de borde, uno por ISP, y utiliza BGP. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

En la **Figura 13** se observa un ejemplo de una conexión Dual Multi-Homed, se evidencia la conexión de una compañía que contiene enlaces hacia dos ISP.

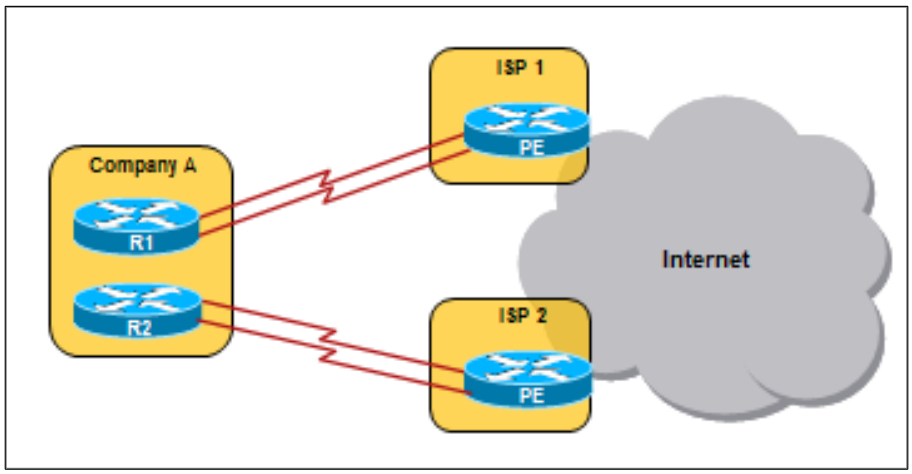


Figura 13: Conexión Dual Multi-Homed.(CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Existen dos clases de el protocolo BGP, cuando se ejecuta entre routers de diferentes SA se denomina Exterior BGP (EBGP) y cuando se ejecuta entre routers en el mismo SA se denomina Interior BGP (IBGP). En la **Figura 14**se observa un ejemplo en el que se puede identificar estas dos clases (EBGP e IBGP).(CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

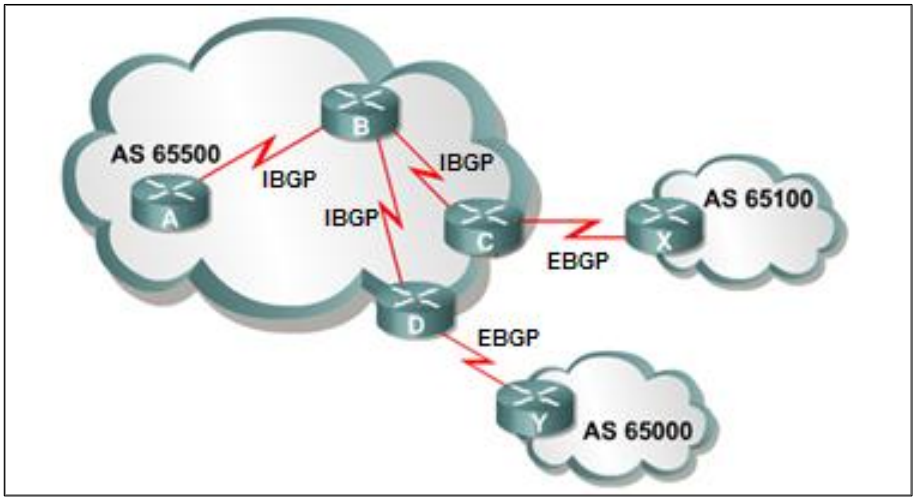


Figura 14: Ejemplo del uso de EBGP e IBGP. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Exterior BGP (EBGP): cuando el protocolo BGP se ejecuta entre routers de diferentes SA, se denomina EBGP. Los routers que ejecutan EBGP se encuentran conectados

directamente entre sí creando vecindades; para que estos neighbor o vecinos se comuniquen o intercambien información de actualizaciones de enrutamiento BGP, la capa de transporte TCP se encarga de permitir la comunicación confiable entre estos dos vecinos que corren el protocolo BGP, una vez establezca la comunicación se podrá intercambiar actualizaciones de enrutamiento BGP. Cabe aclarar que los vecinos EBGP deben tener números de SA diferentes. (BGP, 2012)

Interior BGP (IBGP): cuando el protocolo BGP se ejecuta entre routers del mismo SA, se denomina IBGP. IBGP funciona dentro de un SA para intercambiar información BGP, así todos los routers que ejecutan BGP o también llamados BGP Speakers tengan la misma información de enrutamiento BGP sobre SA externos.

Los routers que ejecutan IBGP no tienen que estar directamente conectados entre sí, siempre y cuando se puedan alcanzar unos a otros, generalmente se utiliza protocolos IGP para que sean alcanzables y se pueda establecer la vecindad BGP. Al igual que EBGP antes de establecer la vecindad, TCP establece una sesión de comunicación entre los vecinos, así cuando la sesión de TCP se establezca se procederá al intercambio de actualización de enrutamiento BGP. Cabe aclarar que los vecinos IBGP deben tener el mismo número de SA. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Los protocolos de enrutamiento interno (IGP) anuncian una lista de redes y métricas para poder llegar a la red de destino, en cambio los routers EGP que hablan BGP intercambian la información de accesibilidad de red utilizando **Path Vector** o **vector de trayectoria** que son formados por **Path Attributes** o **atributos de ruta.**(CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

La información de un Path Vector incluye una lista de la ruta completa de números de SA BGP necesaria para para llegar a una red de destino.

Otros atributos incluyen la dirección IP para llegar al próximo SA (el atributo de siguiente salto) y como las redes al final de la ruta se introdujeron en BGP (el atributo de código de origen)

En la **Figura 15** se observa que información transporta el Vector de Trayectoria o Path Vector.

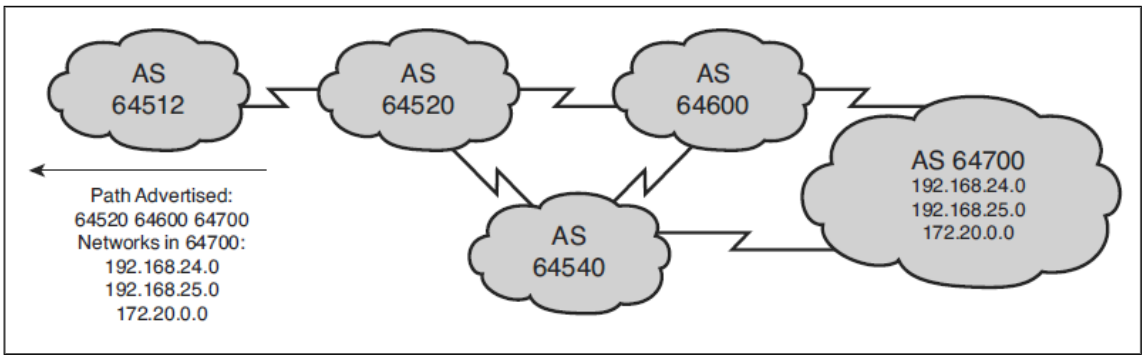


Figura 15: Información de un vector distancia o Path vector. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

BGP mantiene su propia tabla para almacenar información que envía y recibe de los vecinos BGP, esta tabla es conocida como la tabla BGP, la base de datos de la topología BGP, la tabla de enrutamiento BGP y la base de datos de reenvió de BGP. Gracias a esta tabla que proporciona BGP el router ofrece las mejores rutas desde la tabla BGP a la tabla de enrutamiento IP. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Para que BGP establezca una adyacencia, debe configurarla explícitamente para cada vecino. BGP forma una relación TCP con cada uno de los vecinos configurados y realiza un seguimiento del estado de estas relaciones mediante el envío periódico de un mensaje BGP / TCP keepalive. Este keepalive o tiempo de vida que envía BGP / TCP dura por defecto 60 segundos. (Dominguez, 2004)

Después de establecer la adyacencia, los vecinos intercambian las rutas BGP que se encuentran en su tabla de enrutamiento IP, cada router recopila estas rutas de cada vecino con el que establece con éxito una adyacencia y luego las ubica en la tabla BGP o Forwarding Database. Cada router compara las rutas BGP ofrecidas con otras rutas posibles a esas redes. Y la mejor ruta, basada en la distancia administrativa se instala en la tabla de enrutamiento IP. (Sandra, 2010)

Las rutas EBGP tienen por defecto una distancia administrativa de 20. Las rutas IBGP tienen una distancia administrativa de 200.

Tablas BGP:

- **Tabla de vecinos:** en esta tabla como su nombre lo indica muestra los vecinos BGP que contiene el router que habla el protocolo BGP.
- **Tabla BGP (Forwarding database):** en esta tabla se almacena todas las redes aprendidas de cada vecino, puede contener varias rutas de acceso a las redes de destino además contiene atributos BGP para cada ruta de la tabla de enrutamiento IP.
- **Tabla enrutamiento IP:** esta tabla se encarga de mostrar la lista de los mejores caminos a las rutas de destino.

Los **tipos de mensajes** que utiliza BGP son 4 (Open Message, Update Message, Notification Message y Keepalive Message) en la **Figura 16** se aprecia los distintos campos y los mensajes que utiliza el protocolo BGP.

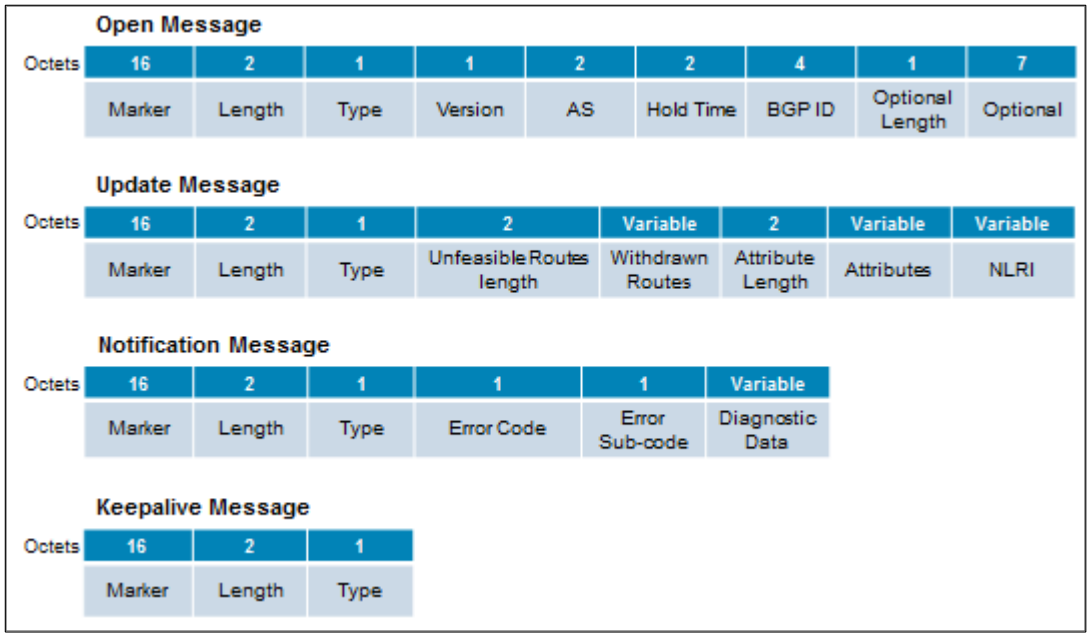


Figura 16: Tipos de mensajes de BGP. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Todos los mensajes de BGP inician con los mismos tres campos de cabecera; los mensajes pueden tener entre 19 y 4096 bytes.

- El primer campo se llama campo de marcador o marker, ocupa 16 bytes del mensaje, se utiliza para la autenticación de mensajes BGP o para detectar las pérdidas de sincronización entre dos vecinos BGP

- El segundo campo con una longitud de 2 bytes es el campo de longitud, indica la longitud total del mensaje BGP, incluido el encabezado.
- El tercer campo corresponde a uno de los cuatro tipos de mensajes de BGP (Open Message, Update Message, Notification Message y Keepalive Message), ocupa una longitud de 1 byte del mensaje.

A continuación se explicara cada uno de los mensajes que utiliza el protocolo de enrutamiento dinámico BGP:

- **Open Message:** cada vez que se establezca una conexión TCP con un vecino BGP, se envía el mensaje Open e incluye un conjunto de parámetros que se deben acordar antes de que se pueda establecer una completa adyacencia BGP. Una vez que ambos vecinos BGP han acordado una mutua comunicación, pueden comenzar a intercambiar información de enrutamiento por medio de mensajes de actualización de BGP, en la **Figura 17** se aprecia los distintos capos del Mensaje Open con sus respectiva longitud en bytes que puede utilizar cada uno de estos campos del mensaje. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

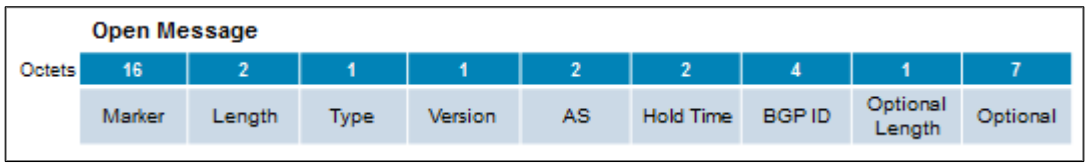


Figura17: Open Message. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

- **Update Message:** los mensajes de actualización contienen toda la información que utiliza BGP para construir una imagen libre de bucle o loops de la red interna. Un mensaje de actualización de BGP tiene información sobre una sola ruta; varias rutas requieren múltiples mensajes de actualización. Como se aprecia en la **Figura 18** los campos del mensaje de actualización o Update. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

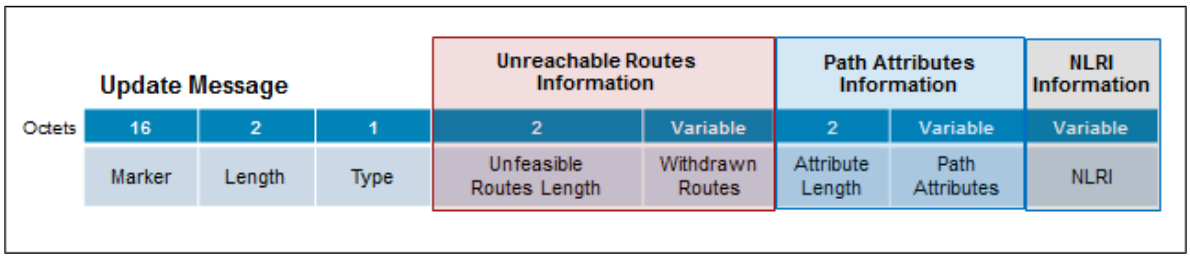


Figura18: Update Message. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Un mensaje de actualización incluye tres tipos de información, estos tipos de información son los siguientes:

- Unreachable Routes information o información de rutas inaccesibles, es una lista de actualizaciones de enrutamiento que ya no son accesibles y que se deben eliminar de una tabla de enrutamiento BGP. Las rutas retiradas tienen el mismo formato que NLRI. (Sandra, 2010)
- Path Attributes Information o información de atributos de ruta, esta información de atributos incluye las rutas SA, rutas de origen, rutas de preferencias locales, etc. Cada atributo de ruta incluye el tipo de atributo, la longitud del atributo y el valor del atributo (TLV). (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)
- Network layer reachability information (NLRI), es una lista de redes (Prefijos de direcciones IP y longitudes de prefijo) a las que puede acceder esta ruta. En la **Tabla 6** se evidencia como NLRI construye la lista de redes. (Sandra, 2010)

Dirección IP y Mascara	NLRI
10.1.1.0 255.255.255.0	24,10.1.1.0
192.24.160.0 255.255.224.0	19, 192.24.160.0

Tabla6: Lista Network layer reachability information (NLRI).(CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

- **Notification Message:** este mensaje BGP se envía cuando se detecta una condición de error, al detectar el error la conexión BGP se cierra inmediatamente después de enviarse el mensaje de notificación. Los mensajes de notificación incluyen un código de error, un sub código de error y datos relacionados con el error. En la **Figura 19** se contempla el mensaje de notificación con los respectivos campos que este tiene.(CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

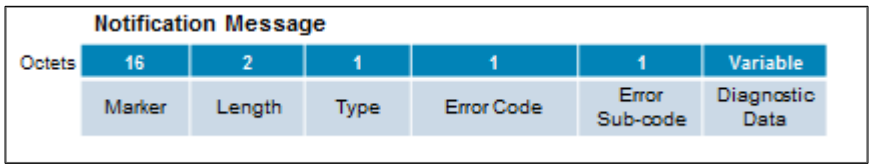


Figura19: Notification Message. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

- **Keepalive Message:** estos mensajes se envían a los vecinos BGP cada 60 segundos (por defecto) para mantener las conexiones. Este mensaje tiene las siguientes características:
  - El mensaje consta de un encabezado de mensaje de 19 bytes.
  - El tiempo de retención es tres veces el temporizador KEEPALIVE de 60 segundos. Si el temporizador periódico es igual a cero, no se envía mensajes keepalive.

Como se puede ver en la **Figura 20** los campos del mensaje keepalive.

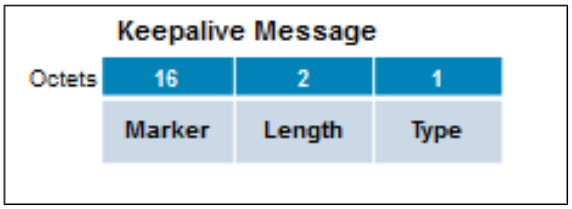


Figura20: Keepalive Message. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Path Attributes o Atributos de Ruta son un conjunto de métricas BGP que describen la ruta hacia una red. BGP, utiliza los atributos de ruta para determinar la mejor ruta hacia las redes de destino, algunos atributos son obligatorios y se incluyen automáticamente en los mensajes de actualización, mientras que otros son configurables manualmente. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Los atributos BGP se pueden utilizar para aplicar una orientación de enrutamiento además de filtrar información de enrutamiento, preferir ciertas rutas, personalizar el comportamiento de BGP. Cabe aclarar que un atributo de ruta consta de tres campos importantes que son: Tipo de atributo, Longitud de atributo y Valor de atributo (TLV).

En la **Figura 21** se aprecian los cuatro distintos tipos de atributos que son: obligatorios bien conocidos, discrecionales bien conocidos, opcionales transitivos y opcional no transitivo.

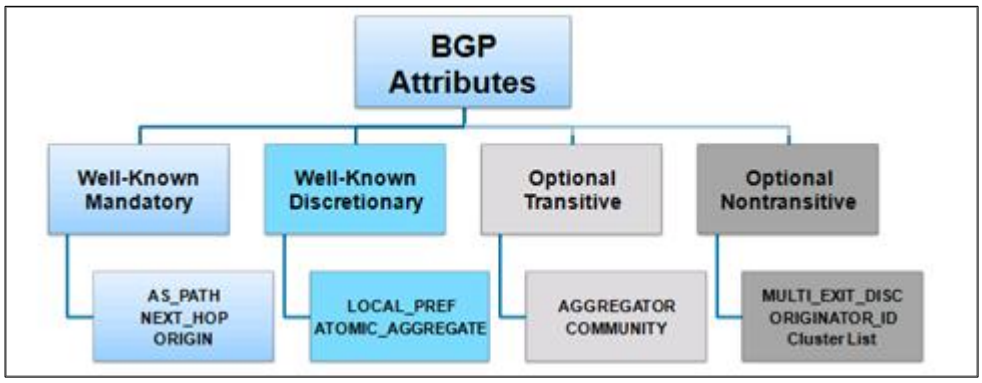


Figura 21: Tipos de atributos. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

- Los **atributos obligatorios bien conocidos** garantizan que todas las implementaciones BGP coincidan en un conjunto estándar de atributos. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

  Este conjunto de atributos obligatorios bien conocidos agrupa atributos como AS_Path, Next_Hop y el atributo Origin.

  - **AS_PATH:** este atributo contiene una lista de números SA para llegar a una ruta. Cada vez que una actualización de ruta pasa por un SA, el nuero de SA se agrega al principio del atributo AS_PATH antes de que se anuncie al siguiente vecino BGP. BGP siempre incluye este atributo en sus actualizaciones. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

    Además de tener una lista de SA, este atributo también sirve para la detección de bucles (un SA ignora un anuncio de ruta si este ya contiene su propio número de SA) y para el filtrado de rutas dependiendo de las políticas de enrutamiento. (España, 2006)

    En la **Figura 22** se observa un ejemplo de como el atributo AS_PATH añade los números de SA y crea la lista de SA.

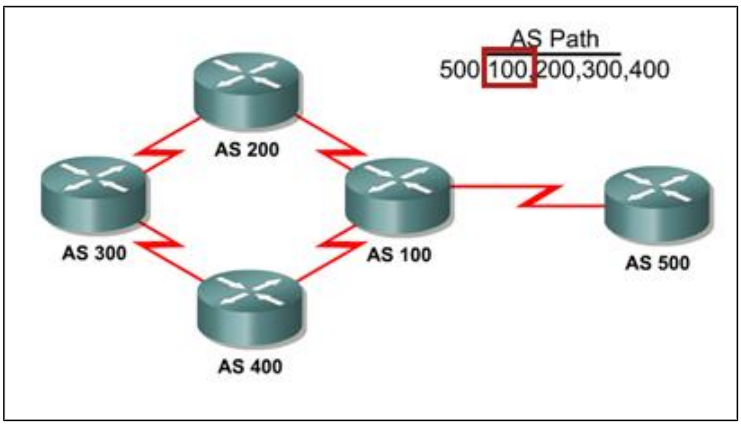


Figura 22: Ejemplo atributo AS_PATH. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

- **NEXT_HOP:** este atributo indica la dirección IP que se va a utilizar para llegar al destino, la dirección IP es el punto de entrada del siguiente SA a lo largo de la ruta a esa red de destino. Por lo tanto para EBGP la siguiente dirección de salto será la dirección IP del vecino que envió la actualización. (Mesa, 2007)
- **ORIGIN:** este atributo indica la forma por la que se ha aprendido la ruta, además este atributo puede seleccionar la ruta, dando prioridad a los valores en el siguiente orden: IGP (I) < EGP (E) < INCOMPLETE (?).

  IGP (I): esta sigla significa que la ruta ha sido aprendida por un protocolo IGP o es aprendida por el interior de un SA, normalmente ocurre cuando se utiliza un comando de red para anunciar una ruta a través de BGP. (Mesa, 2007)

  EGP (E): la ruta se aprende a través de EGP o es aprendida ruta externa del SA. (Mesa, 2007)

  INCOMPLETE (?): el origen de la ruta es desconocido o es prendida por otros medios y generalmente ocurre cuando una ruta se redistribuye en BGP. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

- Los atributos **discrecionales bien conocidos** son reconocidos por todas las implementaciones de BGP pero no puede ser enviado en el mensaje de actualización BGP. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

  Este conjunto de atributos discrecionales bien conocidos agrupa atributos como LOCAL_PREF y ATOMIC_AGGREGATE.

- **LOCAL_PREF:** este atributo es un parámetro local a un SA, solo es anunciado en IBGP y sirve para dar prioridad de las rutas que se anuncian internamente en el SA mediante IBGP. De este modo, se configura la preferencia de las rutas anunciadas hacia el interior desde el exterior del SA. este atributo se tiene en cuenta antes que el atributo AS_PATH a la hora de seleccionar la mejor ruta hacia un destino. (Mesa, 2007)

  Se prefiere un camino con mayor preferencia local, el valor predeterminado para el LOCAL_PREF en un router Cisco es de 100. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

  Con el comando ***bgp local-preference*** se puede modificar la preferencia local por defecto que tiene el router.

- **ATOMIC_AGGREGATE:** este atributo es utilizado para indicar que las rutas se han resumido. El atributo indica que la información recibida puede no ser la completa información de ruta disponible. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

- Los atributos **Opcionales transitivos** pueden o no pueden ser reconocidos por todas las ejecuciones de BGP. Debido a que el atributo es transitivo, BGP acepta y anuncia el atributo, incluso si no se reconoce.

- **COMMUNITY:** este atributo opcional se puede utilizar para filtrar rutas con una etiqueta y permitir que otros routers tomen decisiones basadas en esa etiqueta. Si un router no reconoce el atributo de comunidad, este los direcciona al siguiente router, sin embargo si el router entiende el concepto, debe configurarse para propagar la comunidad. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

- Los atributos **Opcionales no transitivos** al igual que los opcionales transitivos pueden o no ser reconocidos por todas las ejecuciones de BGP. Si el router BGP receptor reconoce o no el atributo, no es transitivo y no se transmite a otros vecinos BGP. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

- **MULTIPLE EXIT DISCRIMINATOR (MED):** a este atributo también se le conoce como métrica. Se utiliza en el caso que se tenga dos SA multiconectados, su función es ayudar a seleccionar una ruta cuando se reciben por EBGP varias rutas iguales anunciadas desde el mismo SA por diferentes enlaces. (Mesa, 2007)
  El MED se envía a los vecinos de EBGP y esos routers se encargan de propagar el MED dentro de su SA. Mediante el uso del atributo MED, BGP es el único protocolo que puede afectar la forma en que las rutas se envían a un SA. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

  Como se observa en la **Figura 23** un ejemplo del funcionamiento del atributo MED. Los routers B y C tienen configurado un atributo MED en las actualizaciones del router. El router B se establece un atributo MED de 150 y en el router C se establece un atributo MED de 200. Cuando A recibe actualizaciones de B y C, selecciona el router B como el siguiente mejor salto debido al MED inferior.

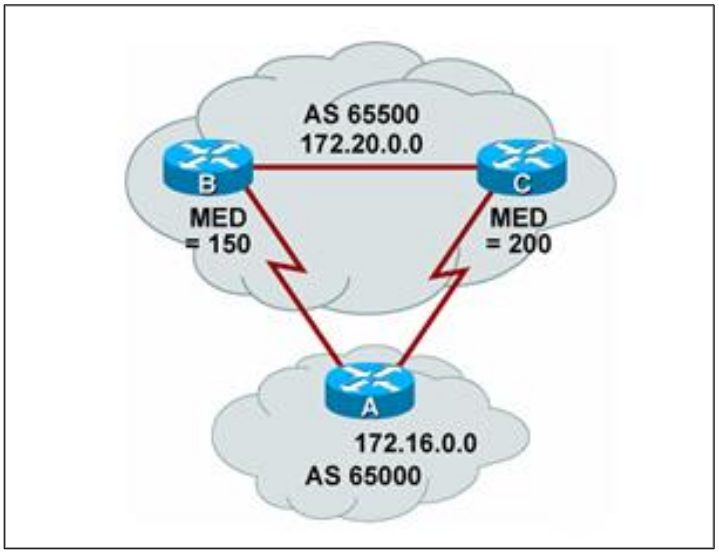
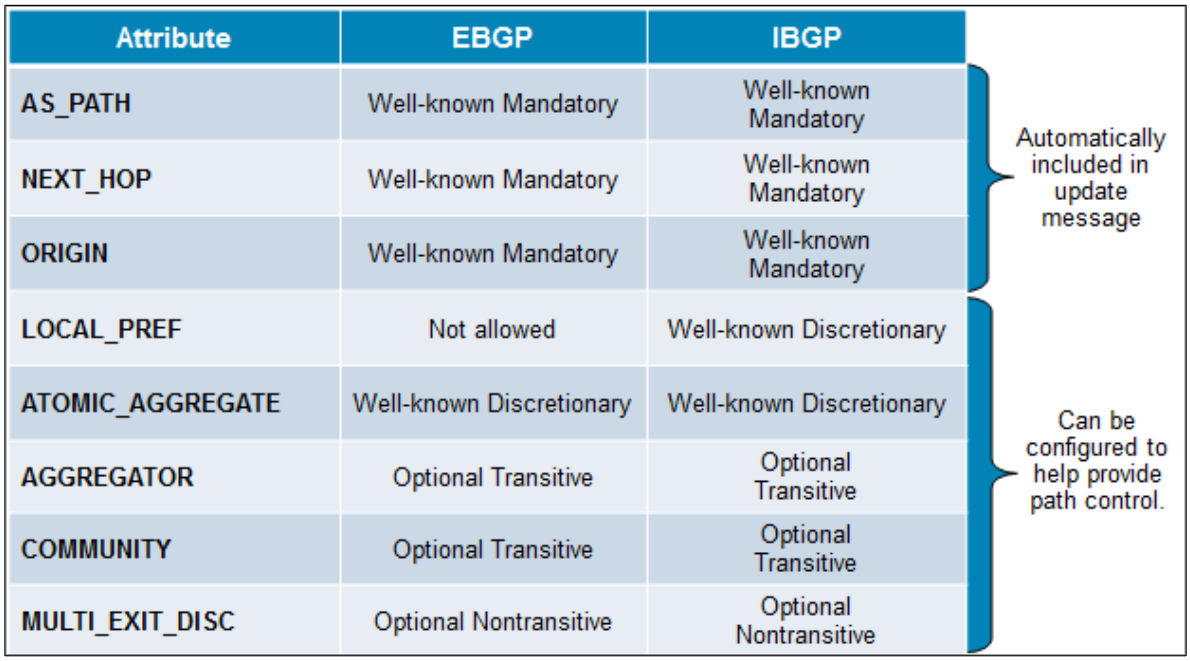


Figura 23: Ejemplo atributo MED. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

En la **Figura 24** se aprecia un cuadro resumen de los atributos de BGP.



Attribute	EBGP	IBGP	
AS_PATH	Well-known Mandatory	Well-known Mandatory	Automatically included in update message
NEXT_HOP	Well-known Mandatory	Well-known Mandatory	
ORIGIN	Well-known Mandatory	Well-known Mandatory	
LOCAL_PREF	Not allowed	Well-known Discretionary	Can be configured to help provide path control.
ATOMIC_AGGREGATE	Well-known Discretionary	Well-known Discretionary	
AGGREGATOR	Optional Transitive	Optional Transitive	
COMMUNITY	Optional Transitive	Optional Transitive	
MULTI_EXIT_DISC	Optional Nontransitive	Optional Nontransitive	

Figura 24: Cuadro resumen de atributos de BGP. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Existe un atributo que es propietario de cisco y utilizado únicamente en los dispositivos Cisco, este atributo se le conoce con el nombre de WEIGHT o Peso.

- **WEIGHT:** este atributo es utilizado como primer criterio de selección para obtener la mejor ruta cuando se tienen diferentes rutas hacia un mismo destino. Similar al atributo LOCAL_PREF el atributo de peso o weight es asignado localmente en el router, de modo que no es necesario anunciarlo a otros routers. El valor del atributo weight puede variar entre 0 y 65535, teniendo un valor por defecto de 32768 para las rutas cuyo origen es el mismo router de origen y con 0 para el resto de rutas. (Mesa, 2007).

  El atributo weight prefiere las rutas con un peso mayor cuando existen múltiples rutas al mismo destino.

  Un ejemplo para entender mejor el funcionamiento del atributo weight se indica en la **Figura 25**.

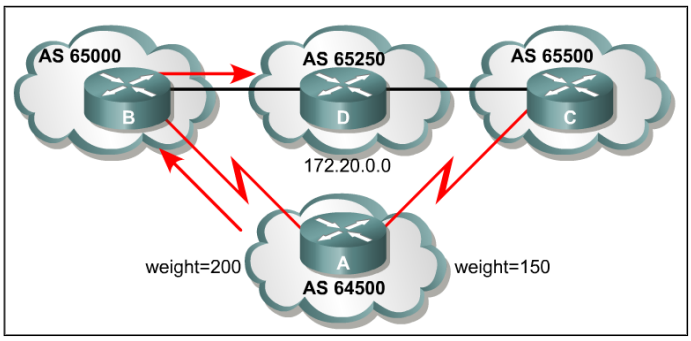


Figura25: Ejemplo atributo Weight.(CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

Los routers B y C aprenden sobre la red 172.20.0.0 desde AS 65250 y propagan la actualización al router A. Por lo tanto, el router A tiene dos formas de llegar a la red 172.20.0.0. El router A establece el peso de las actualizaciones de la siguiente manera:

Las actualizaciones procedentes del router B se establecen en 200 y las actualizaciones procedentes del router C se establecen en 150. El router A utiliza el router B debido al mayor peso configurado en el atributo. (Teldat, 2008)

En la Ilustración 26 se observa el atributo de Peso o Weight es el primer parámetro en el que un router cisco toma la decisión para elegir la mejor ruta, el siguiente parámetro para la elección de la mejor ruta, es el atributo LOCAL_PREF, después se prefiere la ruta que fue originada localmente, seguido del atributo AS_PATH, luego el atributo ORIGIN, luego decidiendo la mejor ruta por el MED o métrica más baja, si todos los escenarios son idénticos se prefiere las rutas EBGP sobre IBGP, además de preferir las rutas que se pueden alcanzar a través del vecino IGP más cercano. Si la ruta interna es la misma el ID del router BGP será el desempate, eligiendo la ruta con el ID del router más baja. (Teldat, 2008)

En este orden que se muestra en la **Figura 26** el router tiene la capacidad de elegir la mejor ruta para alcanzar el destino del paquete.

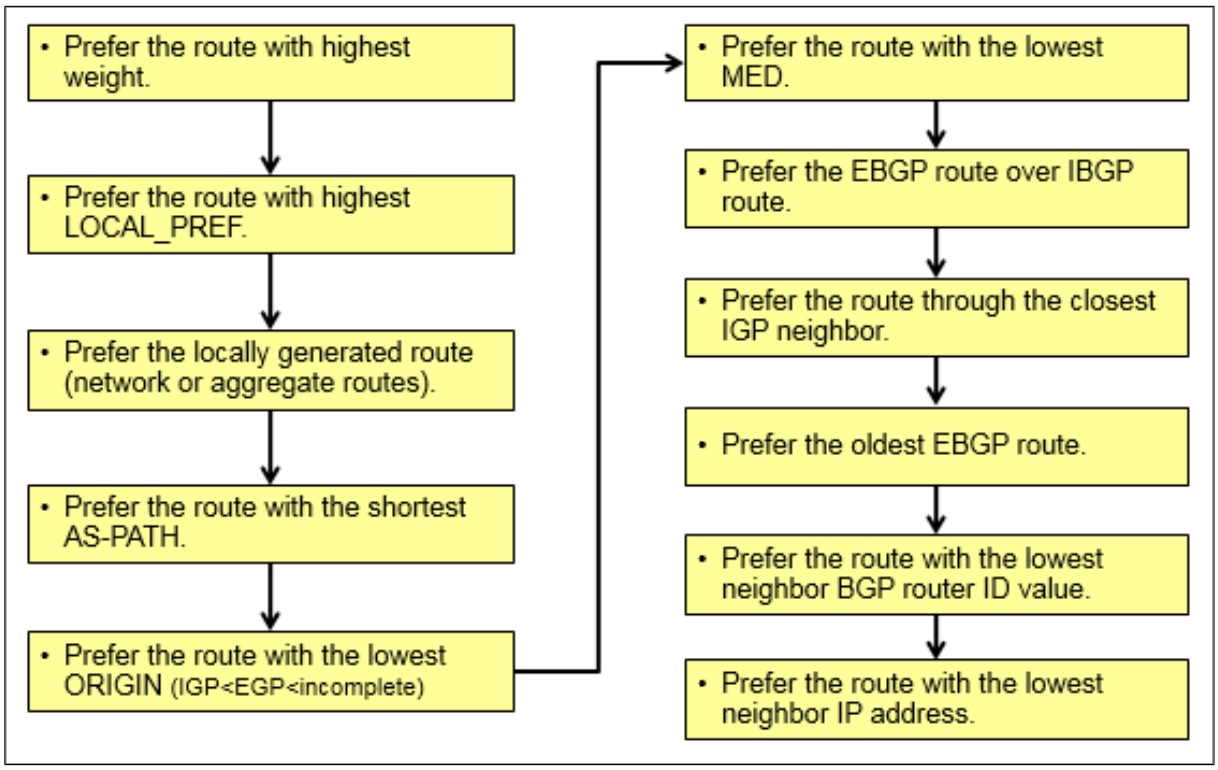


Figura 26: Proceso de selección de rutas BGP. (CISCO, CCNP ROUTE: Implementing IP Routing, 2010)

4.4 HOT STANDBY ROUTER PROTOCOL (HSRP)

Hot Standby Router Protocol (HSRP), es un protocolo que se encarga de solucionar problemas causados por fallos de primer salto que generalmente tienen direcciones estáticas en los host. Al no implementarse HSRP y en dado caso que se llegara a presentar un error en la puerta de enlace del host lo dejaría incapaz de comunicarse fuera de su propia red. Con el protocolo HSRP la puerta de enlace predeterminada es una dirección de un router virtual. (Hucaby, 2001)

HSRP es un protocolo propietario de Cisco, todos los routers Cisco utilizan HSRP, lo que permite a las estaciones finales continuar comunicándose en toda la red incluso cuando la puerta de enlace predeterminada no está disponible. Con HSRP, un grupo de routers trabajan en conjunto para representar un único router en Standby. El grupo de routers en Standby funcionan como un único router configurado con una dirección IP virtual y una MAC, distinto de los routers físicos de la red.(Hucaby, 2001)

Si el router primario o principal falla, un router en estado Standby remplaza automáticamente este router principal que presenta falla. La prioridad que se asigna a cada router determina si el router está en estado activo o en Standby.(Hucaby, 2001)
La prioridad de HSRP es un valor entre 0 y 255. El valor por defecto asignado es una prioridad de 100. El equipo que tenga la prioridad más alta se convertirá en el router activo, si un grupo de prioridades tienen un valor igual, el dispositivo elegirá al router activo comparando las direcciones IP, El dispositivo con la dirección IP más alta se convertirá en el router activo. (CISCO, CCNP Swithing Module 6: First Hop Redundancy Protocol Implementation, 2010)

4.4.1 MENSAJES DE HSRP

Todos los routers de un grupo en Standby envían y reciben mensajes HSRP. Estos mensajes se utilizan para determinar y mantener las funciones del router dentro del grupo. Los mansajes HSRP se encapsulan en la porción de datos de paquetes de UDP (User Datagram Protocol) y usan el número de puerto 1985. Estos paquetes están dirigidos a una dirección de multidifusión con un tiempo de vida (TTL) de un segundo (1s). La **Figura 27** muestra el formato general de un mensaje HSRP. (Hucaby, 2001)

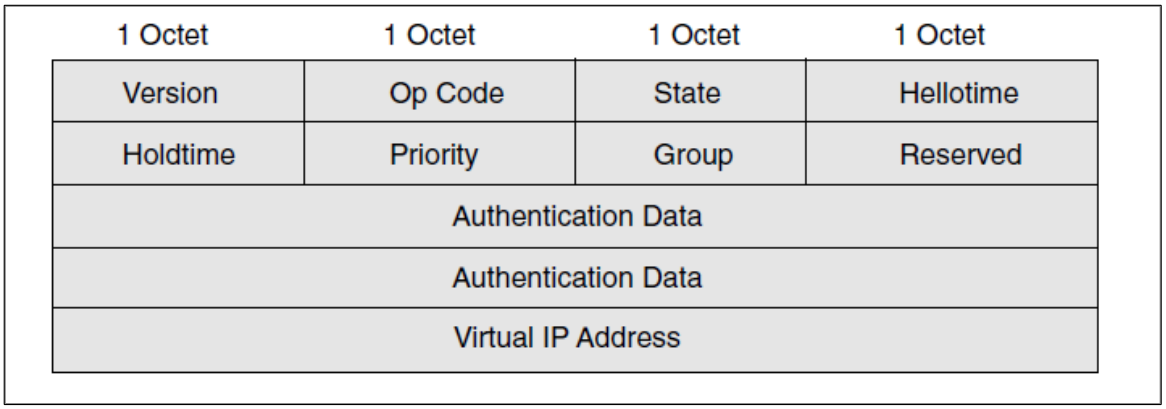


Figura 27: Formato de un mensaje HSRP. (Hucaby, 2001)

El mensaje HSRP contiene la siguiente información:

- El campo versión del mensaje indica que versión está utilizando HSRP.
- OP Code describe el tipo de mensaje contenido en este paquete.
- El mensaje Hello se envía para indicar que un router está en ejecución y es capaz de convertirse en el router activo o Standby.

- Los mensajes de group o grupo son enviados cuando un router desea convertirse en el router activo.
- Los mensajes reserved o reservados se envían cuando el router ya no desea ser el enrutador activo.
- Internamente cada router del grupo de Standby implementa una máquina de estado. El campo de estado describe el estado actual del router que envía el mensaje.
- El campo Hello Time solo se utiliza en los mensajes de bienvenida. Este campo contiene el periodo aproximado entre los mensajes de saludo que el enrutador envía. El tiempo se da en segundos.
- Al igual que el campo Hello Time El campo tiempo de espera se utiliza en los mensajes de bienvenida. Este campo contiene la cantidad de tiempo que el mensaje Hello necesita para que sea válido. El tiempo se da en segundos.
- El campo prioridad se utiliza para elegir los routers activos y en Standby. Al comparar las prioridades de dos routers diferentes, el router con la prioridad más alta gana. En caso de que los routers tengan la misma prioridad, el router con la dirección IP más alta será el ganador.

Solo los enrutadores activos y en Standby envían los mensajes HSRP periódicos después de que el protocolo haya completado el proceso de elección. (Hucaby, 2001)

4.4.2 ESTADOS DE HSRP

HSRP define seis estados en los que un router con configuración HSRP puede existir. Cuando un estado se encuentra en algún router, el router realiza acciones específicas del estado en el que se encuentra. (CISCO, CCNP Swithing Module 6: First Hop Redundancy Protocol Implementation, 2010)

Los estados de HSRP son los siguientes:

- **Estado Inicial:** todos los routers empiezan en el estado inicial. Este estado indica que HSRP no se encuentra funcionando, este estado se introduce mediante un cambio de configuración o cuando aparece una interfaz por primera vez. (Hucaby, 2001)

- **Estado de Aprendizaje:** en este estado el router todavía está esperando escuchar el router activo. El router aún no ha recibido un mensaje de saludo del router activo, ni ha aprendido la dirección IP del router virtual. (Hucaby, 2001)
- **Estado de Escucha:** en este estado el router conoce la dirección IP del router virtual, pero no es ni el router activo ni el router en Standby. (Hucaby, 2001)
- **Estado de Voz:** en el estado de voz el router envía mensajes de saludo periódicos y está participando activamente en la elección del router activo y del router en Standby. (Hucaby, 2001)
- **Estado Standby o Espera:** en este estado el router es un candidato para convertirse en el siguiente router activo y envía mensajes de avisos periódicos. Debe haber al menos un router de espera en el grupo HSRP. (Hucaby, 2001)
- **Estado Active o Activo:** en el estado activo, el router está reenviando paquetes que se envían a la dirección MAC virtual del grupo. El router activo envía mensajes de saludos periódicos a los demás routers del grupo HSRP. (Hucaby, 2001)

4.5 SIMULADOR DE RED

Un simulador de red es una aplicación que permite a usuarios como administradores de red, diseñar una topología de red que puede constar de dispositivos como: computadores, routers, switches, servidores, etc. Estos diseños de red en las aplicaciones de red o simuladores permiten probar la red antes de realizarlo en un entorno real. Estas pruebas realizadas en los simuladores sirven para descartar posibles errores, optimizar configuraciones y tener la certeza de que la red que se diseña funciona correctamente y sin problemas, garantizando a los usuarios un entorno libre de errores y de alta disponibilidad de la red.(Velasco, 2014)

Existen diversos simuladores de redes para hacer pruebas con ellas. Alguno de estos simuladores son: Cisco Packet Tracer y Graphical Network Simulator (GNS3).

4.5.1 CISCO PACKET TRACER

Packet Tracer es uno de los simuladores de red más completos que existe. Este simulador es directamente desarrollado por Cisco, es el recomendado para realizar las

pruebas de red con sus propios routers, switches, hubs, servidores y demás dispositivos de red de Cisco. (Velasco, 2014)

Esta aplicación permite a los usuarios diseñar y crear topologías de red además de configurar dispositivos. Su funcionamiento es sencillo y una vez se tenga la configuración física y lógica de la red se podrá realizar una simulación de conectividad con comandos como PING o Tracer. (Maldonado, 2012)

4.5.2 Graphical Network Simulator (GNS3)

GNS3 es un simulador de redes, diseñado para realizar topologías de red complejas de tal forma que sean lo más similar a un entorno real. Es una herramienta de trabajo gratuita excelente para ingenieros o administradores de red que desean probar su red antes de implementarlo en un entorno real. (Velasco, 2014)

Este software soporta configuración y emulación de dispositivos de red como routers, con sistema operativo IOS CISCO, también permite introducir hosts (maquinas Linux o Windows) a través de **VirtualBox** a la topología de red diseñada. Este software tiene la posibilidad de permitir la captura del tráfico generado en la simulación, esta captura se realiza mediante el software de monitorización de paquetes **Wireshark**. (computadores, 2005)

	Cisco Packet Tracer	Graphical Network Simulator (GSN3)
Ventajas	• Soporte para todos los sistemas operativos. • Permite configuraciones en tiempo real. • Soporta protocolos como: HTTP, TCP/IP, Telnet, SSH, TFTP, DHCP, DNS, HTTP, TCP/IP, Telnet, SSH, TFTP, DHCP y DNS, TCP/UDP, IPv4, IPv6, ICMPv4 e ICMPv6, RIP, EIGRP, OSPF Multitarea, enrutamiento	• Soporte para todos los sistemas operativos. • Permite incorporar máquinas virtuales. • Realiza simulaciones complejas y muy similares a un entorno real. • Permite captura del tráfico que recorre la red. • Simula el protocolo BGP. • Es de uso gratuito. • Simula dispositivos de red de distintos fabricantes.

	estático y redistribución de rutas, Ethernet 802.3 y 802.11, HDLC, Frame Relay y PPP, ARP, CDP, STP, RSTP, 802.1q, VTP, DTP. • Utiliza pocos recursos del dispositivo en el que se utiliza la aplicación. • Entorno grafico amigable con el usuario y fácil de utilizar. • Es de uso gratuito.	• Entorno grafico amigable con el usuario facilitando el uso de la aplicación.
Desventaja	• No soporta BGP. • Únicamente utiliza y simula dispositivos fabricados por Cisco.	• Consume grandes cantidades de recursos de memoria y rendimiento del dispositivo en el que se utiliza la aplicación.

Tabla 7: Comparativa entre simuladores de red GNS3 y Packet Tracer. (computadores, 2005)

5. DESARROLLO DEL PROYECTO

Teniendo en cuenta la topología de diseño de red que se estudia del ISP Ejemplo.Compañia, se realiza un procedimiento paso a paso para dar solución a los problemas que afectan a los clientes, problemas como los extensos tiempos sin acceso a internet cuando se presenta un incidente en la red del ISP. Estos extensos tiempos sin servicio al cliente se debe a la escasa redundancia con la que cuenta la red del ISP.

La configuración de un protocolo redundante ayuda a disminuir los tiempos de respuesta a fallas o incidentes en la red, de manera que el servicio que se presta al cliente se verá afectado mientras se realiza la convergencia del protocolo redundante, que tarda menos de 10 segundos en converger.

En cuanto al cambio de diseño que se realiza a la topología de red, es necesario reconfigurar los protocolos de enrutamiento, pues en el caso de BGP deberá aprender quienes serán sus nuevos vecinos BGP para que así establezca sesión y comunicación con los demás ISP que prestan la salida hacia internet.

Los siguientes pasos son los que se siguieron para el desarrollo y solución de este proyecto.

PASO 0: Recrear la topología de red del ISP Ejemplo.Compañia que presenta las fallas.

- Teniendo la configuración de los equipos que presentan inconvenientes como son el ASR01, ASR02 y el Firewall, se recrea la topología de red del ISP. El resultado de esta topología de red es la que se aprecia en la **Figura 28**.

PASO 1: Identificar errores en el diseño de red y errores en la configuración de los dispositivos de red.

- En el diseño se implementa un equipo que es innecesario utilizar el cual genera conflicto de enrutamiento, por tal razón afecta en el tiempo de tráfico de paquetes que cruzan por el equipo y en ocasiones no deja cruzar ningún paquete, afectando la conectividad del cliente hacia la red de internet, este equipo es el Firewall Mikrotic cuya función es comunicar y conectar los routers ASR-01 y ASR-02. En la **Figura 28** se aprecia este dispositivo con una letra (A) de identificación.

- Existe conexión física con respaldo entre los dos proveedores de internet hacia los routers del ISP, ASR-01 y ASR-02, el problema recae en la sesión que crea el protocolo de enrutamiento BGP en el Router ASR-01 interface Port-Channel 1.15 hacia internet y en el Router ASR-02 interface Port-Channel 1.16 hacia internet, el cual estas sesiones de los routers no se establecen, por tal motivo no se puede transportar tráfico por el enlace sin sesión hacia internet. En la **Figura 28** se observa el diseño lógico de la red en donde se muestra el enlace con el error establecimiento de una sesión BGP hacia Internet.

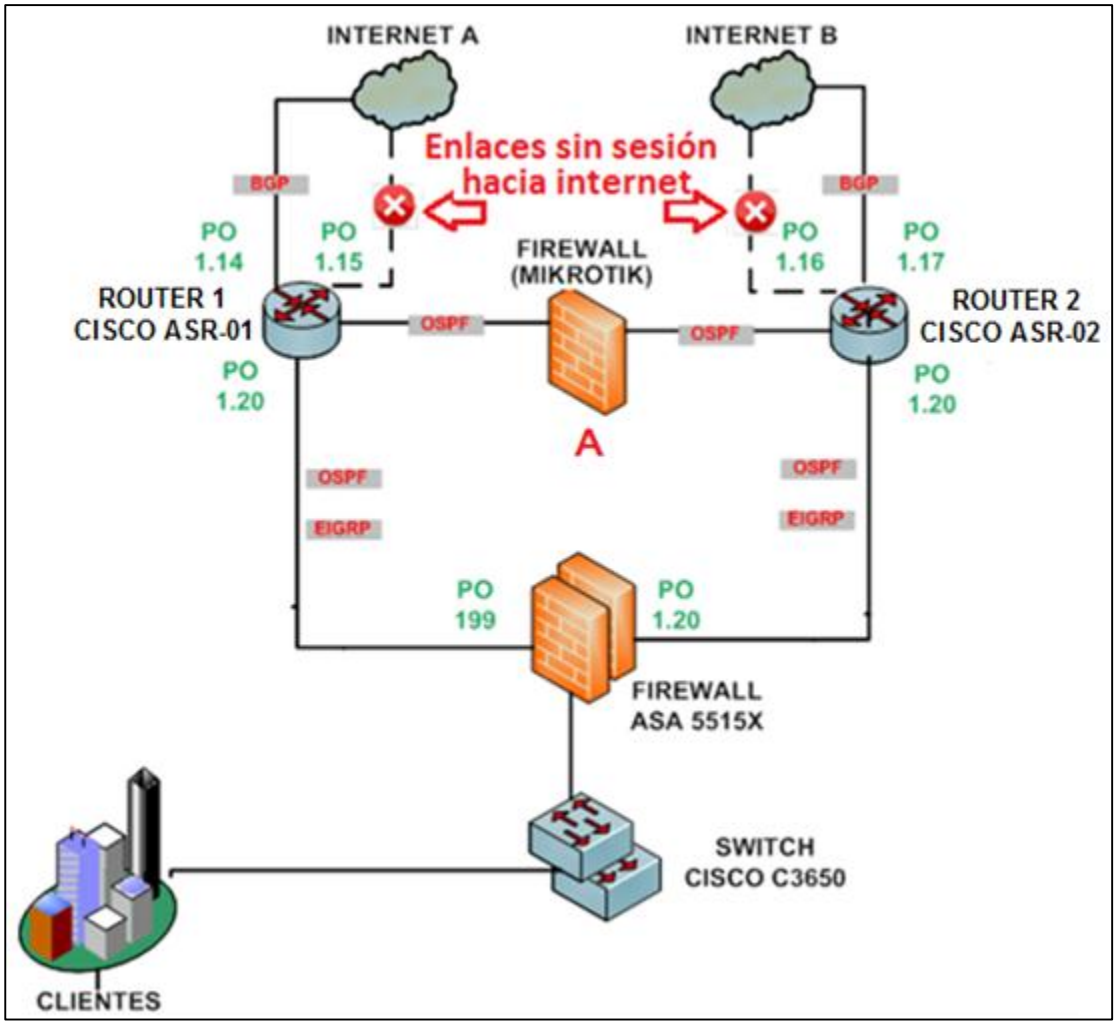


Figura 28: diseño antiguo del ISP Ejemplo.Compañia.

En las siguientes tablas se muestra el direccionamiento utilizado para el diseño de red de los dispositivos que se encuentran en el diseño de red del ISP Ejemplo.Compañia.

En la **Tabla 8** se encuentra el direccionamiento realizado para el equipo router ASR-01

Direccionamiento IP Equipo: ASR1001-1			
INTERFACE	IP	Mascara	Función
Port-channel1.14	80.80.90.26	255.255.255.252	BGP
Port-channel1.15	75.85.95.242	255.255.255.252	BGP (SHUTDOWN)
Port-channel1.19	114.117.207.13	255.255.255.252	ospf
Port-channel1.20	114.117.207.177	255.255.255.248	eigrp
Port-channel1.23	114.117.207.21	255.255.255.252	ospf

Tabla 8: Direccionamiento antiguo de router ASR-01

En la **Tabla 9** se encuentra el direccionamiento realizado para el equipo router ASR-02

Direccionamiento IP Equipo: ASR1001-2			
INTERFACE	IP	Mascara	Función
Port-channel1.16	75.85.95.234	255.255.255.252	BGP (SHUTDOWN)
Port-channel1.17	75.85.95.230	255.255.255.252	BGP
Port-channel1.18	114.117.207.9	255.255.255.252	ospf
Port-channel1.20	114.117.207.179	255.255.255.248	eigrp
Port-channel1.22	114.117.207.17	255.255.255.252	ospf

Tabla 9: Direccionamiento antiguo de router ASR-02

En la **Figura 29** se observa la configuración de los dispositivos ASR-01 y ASR-02 en el cual se detecta y se resalta en un recuadro rojo que efectivamente el enlace Backup se encuentra deshabilitado tanto en la configuración del router ASR-01 como en la configuración del router ASR-02.

ASR-01

```
router bgp 26322
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 bgp default local-preference 500
 neighbor 172.16.1.130 remote-as 26322
 neighbor 172.16.1.130 description iBGPejemplo.compania
 neighbor 172.16.1.130 update-source Loopback0
 neighbor 172.16.1.131 remote-as 26322
 neighbor 172.16.1.131 description iBGPejemplo.compania
 neighbor 172.16.1.131 update-source Loopback0
 neighbor 172.16.1.132 remote-as 26322
 neighbor 172.16.1.132 description iBGPejemplo.compania
 neighbor 172.16.1.132 update-source Loopback0
 neighbor 172.16.1.132 version 4
 neighbor 75.85.95.241 remote-as 26219
 neighbor 75.85.95.241 description Columbus Networks Backup
 neighbor 75.85.95.241 shutdown
 neighbor 80.80.90.25 remote-as 26219
 neighbor 80.80.90.25 description Columbus Networks
```

ASR-02

```
router bgp 26322
 bgp log-neighbor-changes
 neighbor 172.16.1.129 remote-as 26322
 neighbor 172.16.1.129 description iBGPejemplo.compania
 neighbor 172.16.1.129 update-source Loopback0
 neighbor 172.16.1.131 remote-as 26322
 neighbor 172.16.1.131 description iBGPejemplo.compania
 neighbor 172.16.1.131 update-source Loopback0
 neighbor 172.16.1.132 remote-as 26322
 neighbor 172.16.1.132 description iBGPejemplo.compania
 neighbor 172.16.1.132 update-source Loopback0
 neighbor 172.16.1.132 version 4
 neighbor 75.85.95.229 remote-as 3549
 neighbor 75.85.95.229 description Level3 Principal
 neighbor 75.85.95.233 remote-as 3549
 neighbor 75.85.95.233 description Level3 Backup
 neighbor 75.85.95.233 shutdown
```

Figura 29: configuración de enlace Backup hacia Internet deshabilitado en los equipos ASR-01 y ASR-02.

- En el diseño del ISP Ejemplo.Compañia se utilizan diversos protocolos de enrutamiento para realizar un mismo proceso. Al utilizar diversos protocolos de enrutamiento en un router aumenta el procesamiento del equipo generando más tiempo en el momento de transportar paquetes de un origen a un destino. En la **Figura 30** se aprecia la configuración de los protocolos que utiliza el router ASR-01.

ASR-01

```
router eigrp 90
 default-metric 90000 1 255 1 1500
 network  114.117.207.176 0.0.0.7
 redistribute ospf 100 metric 90000 1 255 1 1500
 redistribute bgp 263227 metric 9000000 1 255 1 1500 route-map Internal_1
!
router ospf 100
 router-id 172.16.1.129
 area 1 filter-list prefix OSPF-Internal out
 area 2 filter-list prefix OSPF-Internal out
 network 172.16.0.0 0.0.0.3 area 1
 network 172.16.0.4 0.0.0.3 area 2
 network 172.16.1.0 0.0.0.255 area 0
 network  114.117.207.12 0.0.0.3 area 1
 network  114.117.207.20 0.0.0.3 area 2
 network  114.117.207.128 0.0.0.63 area 0
 default-information originate always
!
router bgp 26322
 bgp log-neighbor-changes
 bgp graceful-restart restart-time 120
 bgp graceful-restart stalepath-time 360
 bgp graceful-restart
 bgp default local-preference 500
 neighbor 172.16.1.130 remote-as 26322
 neighbor 172.16.1.130 description iBGPejemplo.compania
 neighbor 172.16.1.130 update-source Loopback0
 neighbor 172.16.1.131 remote-as 26322
 neighbor 172.16.1.131 description iBGPejemplo.compania
 neighbor 172.16.1.131 update-source Loopback0
 neighbor 172.16.1.132 remote-as 26322
 neighbor 172.16.1.132 description iBGPejemplo.compania
 neighbor 172.16.1.132 update-source Loopback0
 neighbor 172.16.1.132 version 4
 neighbor 75.85.95.241 remote-as 26219
 neighbor 75.85.95.241 description Columbus Networks Backup
 neighbor 75.85.95.241 shutdown
 neighbor 80.80.90.25 remote-as 26219
 neighbor 80.80.90.25 description Columbus Networks
```

Figura 30: protocolos de enrutamiento que utiliza el router ASR-01.

El router ASR-02 utiliza los mismos protocolos de enrutamiento que usa el router ASR-01 estos protocolos de enrutamiento son los siguientes:

- OSPF.
- EIGRP.
- BGP.

Se observa en la **Figura 31** los protocolos utilizados por el router ASR-02.

ASR-02

```
router eigrp 90
 default-metric 80000 1 255 1 1500
 network 114.117.207.176 0.0.0.7
 redistribute ospf 100 metric 80000 1 255 1 1500
 redistribute bgp 263227 metric 8000000 1 255 1 1500 route-map Internal_1
!
router ospf 100
 router-id 172.16.1.130
 area 1 filter-list prefix OSPF-Internal out
 area 2 filter-list prefix OSPF-Internal out
 network 172.16.0.8 0.0.0.3 area 1
 network 172.16.0.12 0.0.0.3 area 2
 network 172.16.1.0 0.0.0.255 area 0
 network 114.117.207.8 0.0.0.3 area 2
 network 114.117.207.16 0.0.0.3 area 1
 network 114.117.207.128 0.0.0.63 area 0
 default-information originate always
!
router bgp 263227
 bgp log-neighbor-changes
 neighbor 172.16.1.129 remote-as 263227
 neighbor 172.16.1.129 description iBGPejemplo.compania
 neighbor 172.16.1.129 update-source Loopback0
 neighbor 172.16.1.131 remote-as 263227
 neighbor 172.16.1.131 description iBGPejemplo.compania
 neighbor 172.16.1.131 update-source Loopback0
 neighbor 172.16.1.132 remote-as 263227
 neighbor 172.16.1.132 description iBGPejemplo.compania
 neighbor 172.16.1.132 update-source Loopback0
 neighbor 172.16.1.132 version 4
 neighbor 75.85.95.229 remote-as 3549
 neighbor 75.85.95.229 description Level3 Principal
 neighbor 75.85.95.233 remote-as 3549
 neighbor 75.85.95.233 description Level3 Backup
 neighbor 75.85.95.233 shutdown
 !
```

Figura 31: protocolos de enrutamiento que utiliza el router ASR-02.

- El diseño de red no tiene un protocolo de redundancia, es importante tener protocolos de redundancia para poder mitigar errores que pueden causar inconvenientes e irregularidades en la red y de este modo afectar al servicio que se presta a los clientes.

PASO 2: se realiza un nuevo direccionamiento de red para cada uno de los dispositivos que se encuentran en la topología de red del ISP Ejemplo.Compañia.

Se aprecia en la **Tabla 10** las direcciones IP de cada una de las interfaces de los dispositivos que se encuentran en el diseño de red del ISP Ejemplo.Compañia:

Direccionamiento IP Equipo: ASR-01 --> SA: 26322			
INTERFACE	IP	Mascara	Función
Fast Ethernet 2/0	190.135.236.26	255.255.255.252	BGP PPAL
FastEthernet3/0	190.216.222.234	255.255.255.252	BGP BKP
FastEthernet1/0	100.211.207.177	255.255.255.248	IBGP - HSRP
Loopback 0	172.16.1.129	255.255.255.255	IBGP

Direccionamiento IP Equipo: ASR-02 --> SA: 26322			
INTERFACE	IP	Mascara	Función
FastEthernet 0/0	190.226.132.230	255.255.255.252	BGP PPAL
FastEthernet3/0	190.132.200.242	255.255.255.252	BGP BKP
FastEthernet1/0	100.211.207.179	255.255.255.248	IBGP - HSRP
Loopback 0	172.16.1.130	255.255.255.255	IBGP

Direccionamiento IP Equipo: INTERNET 1 --> SA: 26219			
INTERFACE	IP	Mascara	Función
FastEthernet 2/0	190.135.236.25	255.255.255.252	ASR-1 PPAL
FastEthernet 3/0	190.132.200.241	255.255.255.252	ASR-2 BKP
FastEthernet 1/0	190.116.236.238	255.255.255.252	INTERNET

Direccionamiento IP Equipo: INTERNET 2 --> SA: 3549			
INTERFACE	IP	Mascara	Función
FastEthernet 0/0	190.226.132.229	255.255.255.252	ASR-2 PPAL
FastEthernet3/0	190.216.222.232	255.255.255.252	ASR-1 BKP
FastEthernet1/0	190.116.236.242	255.255.255.252	INTERNET

Direccionamiento IP Equipo: INTERNET --> SA: 1111			
INTERFACE	IP	Mascara	Función
FastEthernet 0/0	190.116.236.237	255.255.255.252	INTERNET 1
FastEthernet1/0	190.116.236.241	255.255.255.252	INTERNET 2
Loopback0	1.1.1.1	255.255.255.255	Simula Servidores
Loopback1	4.4.4.4	255.255.255.255	Simula Servidores

Direccionamiento IP Equipo: FIREWALL --> SA: 1111			
INTERFACE	IP	Mascara	Función
FastEthernet 0/0	100.211.207.178	255.255.255.248	IBGP
Loopback0	100.211.192.0	255.255.254.0	INTERNET 2
Loopback1	100.211.194.0	255.255.254.0	Simula Host

Loopback2	100.211.196.0	255.255.254.0	Simula Host
Loopback3	100.211.198.0	255.255.254.0	Simula Host
Loopback4	100.211.200.0	255.255.254.0	Simula Host
Loopback5	100.211.202.0	255.255.254.0	Simula Host
Loopback6	100.211.204.0	255.255.254.0	Simula Host

Tabla 10: Direccionamiento de nuevo diseño de topología de red.

PASO 3: Se realiza el nuevo diseño de red, teniendo en cuenta todas las recomendaciones y buenas prácticas para realizar un diseño de red utilizando el protocolo BGP.

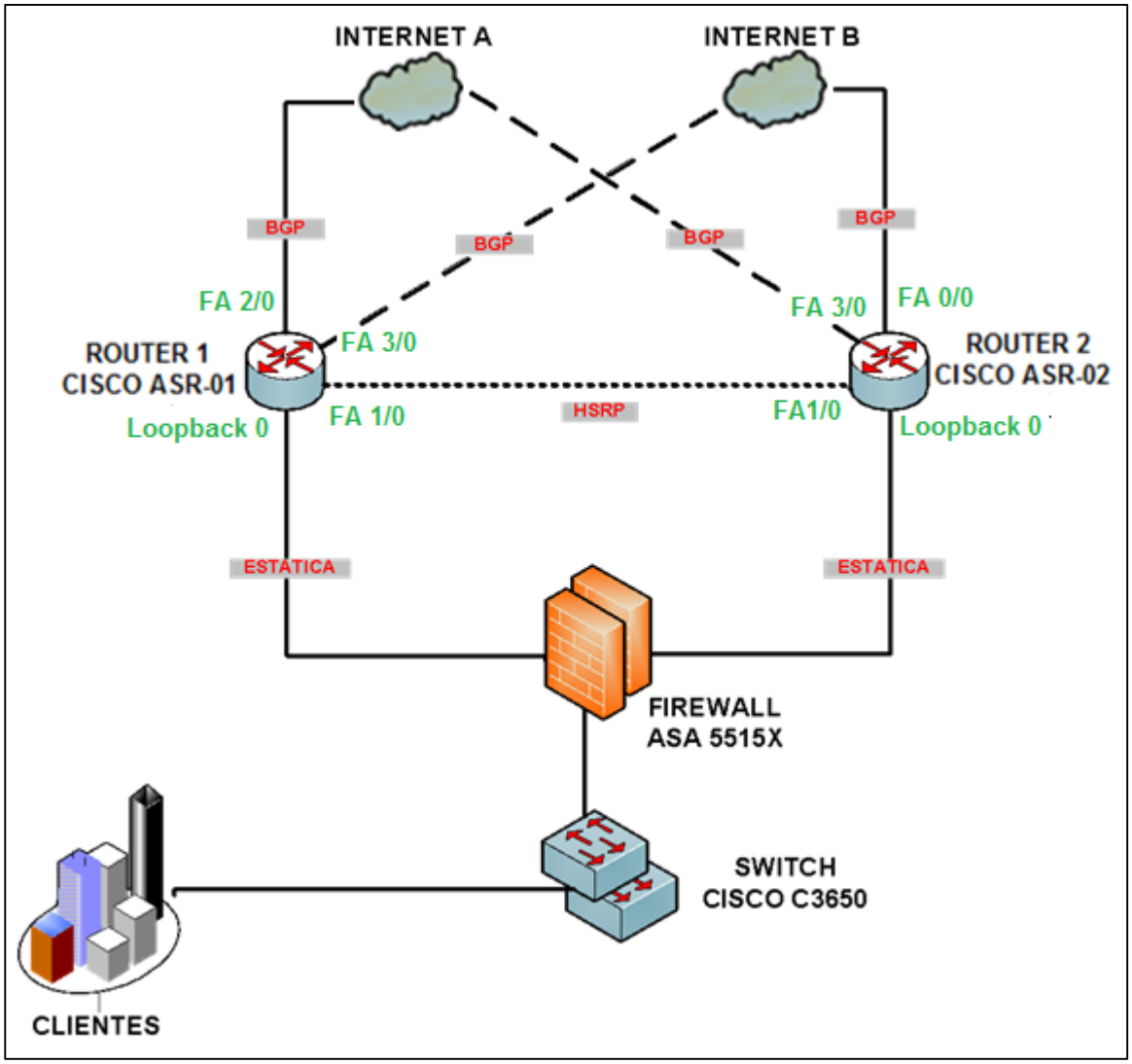


Figura 32: Nuevo diseño lógico de la topología de red del ISP Ejemplo.Compañia.

En la **Figura 32** se observa el nuevo diseño lógico de la topología de red del ISP. En este diseño a diferencia del anterior se modificó lo siguiente:

- Se descartó el equipo Firewall Mikrotic en este diseño, debido a que no está realizando ningún proceso importante para tener la red funcionando correctamente, a diferencia de esto, el dispositivo estaba generando inconvenientes en la comunicación de los routers ASR-01 y ASR-02.

- En la conexión de los routers ASR-01 y ASR-02 hacia las salidas de INTERNET se realiza un cambio en la conexión, se sigue utilizando la misma conexión recomendada para dos o más ISP (Dual-Multihomed) pero con un leve cambio, la conexión hacia Internet se realiza cruzada, esto con el fin de aumentar la redundancia de la red y poder mitigar errores con menor impacto a los clientes y prevenir que el servicio se pierda por completo.

- Se reduce la utilización de diversos protocolos (OSPF y EIGRP), debido a que el Core de esta topología necesita realizar procesos con mayor fluidez y en menor tiempo, estos protocolos que se utilizaban en el anterior diseño fueron remplazados por enrutamientos estático debido a que presta una distancia administrativa menor.

- En el nuevo diseño de red específicamente en los routers de salida hacia INTERNET se implementa el protocolo de redundancia HSRP, permitiendo decidir automáticamente el camino en dado caso que alguno de los routers ASR-01 y ASR-02 falle.

En la **Figura 33** se logra apreciar el diseño físico nuevo de red del ISP Ejemplo.Compañia ya plasmado en el simulador de red GNS3.

Para la simulación de la red del ISP Ejemplo.Compañia se remplaza el dispositivo Firewall ASA 5515X, debido a que el simulador de red no cuenta con una imagen para simular este equipo, por tal razón se remplaza por un router que si se puede simular y lleva el nombre de FIREWALL.

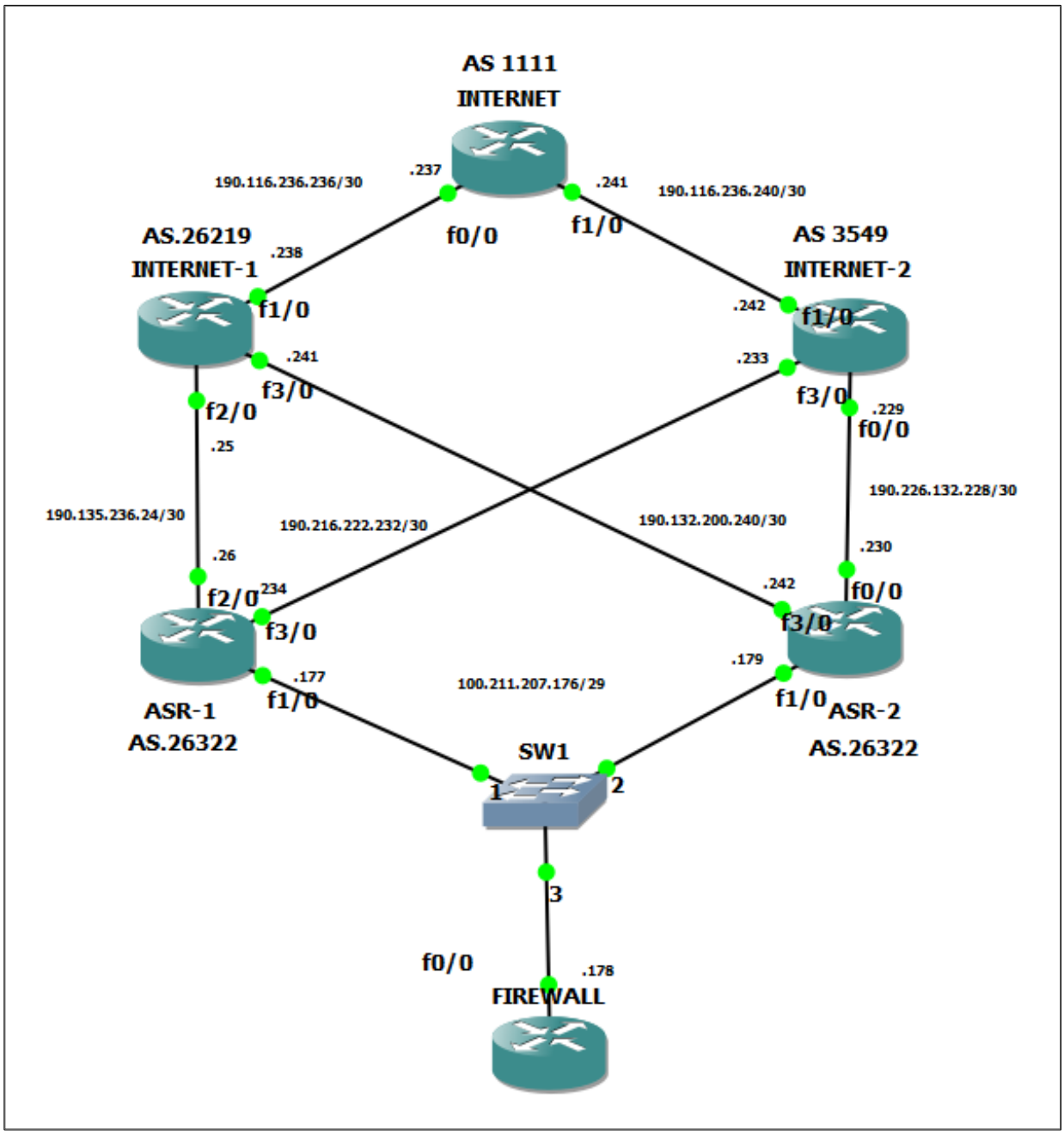


Figura 33: Diseño de la topología de red plasmado en el simulador GNS3.

PASO 4: configuración en cada uno de los dispositivos que conforman la topología de red en el simulador de red GNS3**.**

Configuración ASR_1

- Configurar protocolo de enrutamiento BGP con número de Sistema Autónomo (SA) de: 26322.

  Con el comando ***router bgp "# SA"*** se define el proceso BGP y el respectivo número de SA al que el router pertenece, este router pertenece a el SA con número 26322. Para verificar si efectivamente se creó el proceso BGP se digita el siguiente comando en el modo global ***show running-config.***

- Aprender y asociar los vecinos BGP.

  Definir los neighbor o vecinos es el siguiente paso en el proceso de configuración. Los vecinos son los routers con los que se establecerá una sesión BGP (peering) a través de TCP.

  El comando utilizado para establecer la conexión TCP con los vecinos es el siguiente: ***neighbor "ip address" remote-as "#SA"*** este número de SA pertenece al SA remoto del vecino o del router con el que se quiere establecer la sesión BGP. La dirección IP corresponde a la dirección de la interfaz del router directamente conectado (next hop). En la **Figura 34** se observa la configuración de vecinos BGP en el router ASR-01.

```
neighbor 190.135.236.25 remote-as 26219
neighbor 190.135.236.25 description Conexion Columbus Principal
neighbor 190.216.222.233 remote-as 3549
neighbor 190.216.222.233 description Conexion Level3 Backup
```

Figura 34: Configuración de vecinos BGP para router ASR-01.

Con el comando ***description*** se puede utilizar para saber que función está realizando el vecino o para agregar algún comentario.

NOTA: para la configuración de las sesiones I-BGP generalmente se usan interfaces Loopback, de tal forma que permiten asegurar las sesiones I-BGP indicando una dirección IP virtual, de manera que esta dirección virtual sea independiente de las interfaces físicas del router vecino y se pueda establecer la sesión I-BGP por cualquier interfaz física. En router vecino se debe indicar al proceso BGP que se está usando una interfaz Loopback en lugar de una interfaz física para poder establecer la

conexión TCP con el vecino. El comando utilizado para anunciar una interfaz Loopback es el siguiente:

neighbor "ip address" update-source "interfaz loopback vecino"

En la **Figura 35** se ve la configuración para anunciar una interfaz Loopback.

```
neighbor 172.16.1.130 remote-as 26322
neighbor 172.16.1.130 description iBGP
neighbor 172.16.1.130 update-source Loopback0
```

Figura 35: Configuración vecino I-BGP mediante Loopback.

- Enseñarle a BGP las redes que se van a transportar. Una vez se inicia el proceso BGP se procede a configurar las redes o información que se van a transportar mediante el protocolo BGP. El comando utilizado para enseñar redes es el siguiente: ***network "IP network" mask "mascara de la red"***

  El comando para enseñar rutas indica al proceso BGP las rutas que debe anunciar, estas rutas se expresan mediante una dirección IP y una máscara de red. Para que estas rutas puedan ser anunciadas el router debe conocerlas, bien sea mediante enrutamiento estático o enrutamiento dinámico o porque las redes de destino estén conectadas directamente al router. Se puede ver en la **Figura 36** la configuración para enseñar redes al protocolo BGP.

```
network 100.211.192.0 mask 255.255.254.0
network 100.211.194.0 mask 255.255.254.0
network 100.211.196.0 mask 255.255.254.0
network 100.211.198.0 mask 255.255.254.0
network 100.211.200.0 mask 255.255.254.0
network 100.211.202.0 mask 255.255.254.0
network 100.211.204.0 mask 255.255.254.0
network 100.211.206.0 mask 255.255.254.0
network 100.211.207.176 mask 255.255.255.248
```

Figura 36: Configuracion de redes en BGP para el router ASR-01.

En la **Figura 37** se muestra el uso del comando ***show running-config,*** el cual nos permite ver toda la configuración realizada en un dispositivo, en este caso el router ASR-01. Se observa la configuración completa del proceso BGP con sus respectivos vecinos y redes aprendidas.

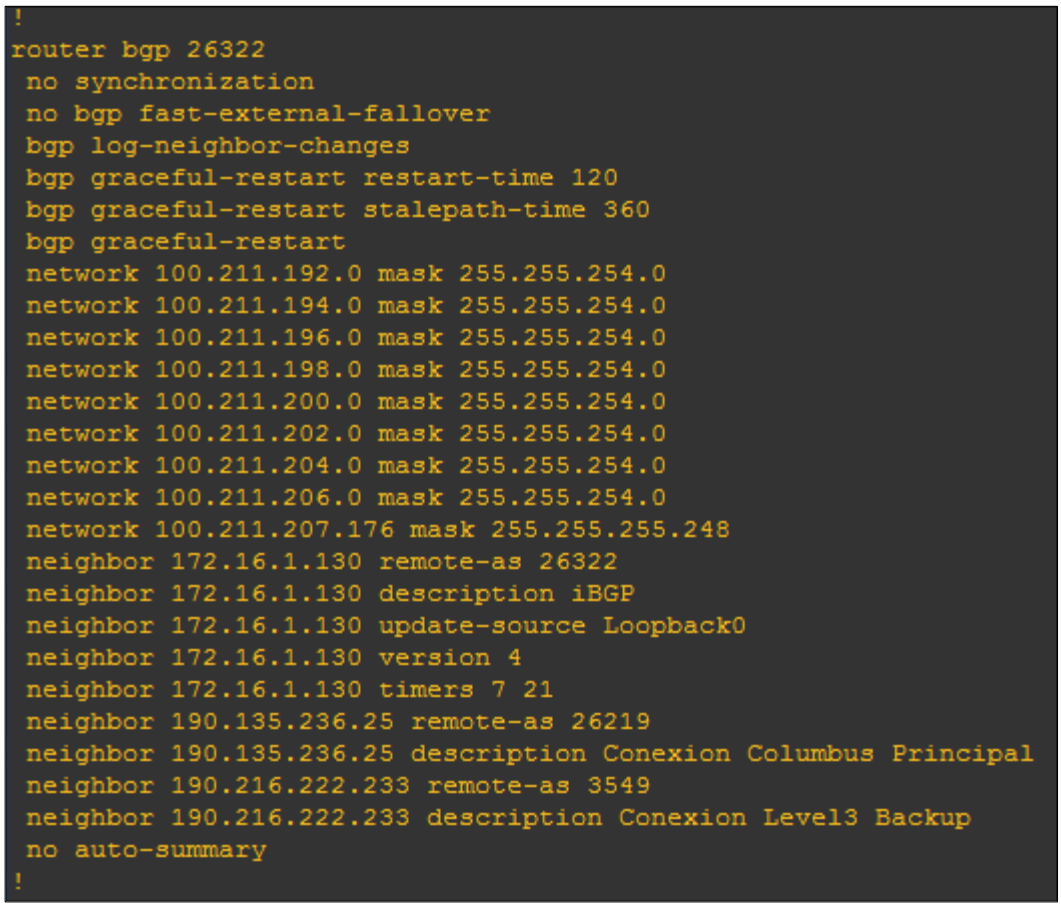


Figura 37: Configuración protocolo BGP en router ASR-01.

Configuración ASR_2

- Configurar protocolo de enrutamiento BGP con número de Sistema Autónomo (SA) de: 26322.

  Con el comando ***router bgp "# SA"*** se define el proceso BGP y el respectivo número de SA al que el router pertenece, este router pertenece a el SA con número 26322. Para verificar si efectivamente se creó el proceso BGP se digita el siguiente comando en el modo global ***show running-config.***

- Aprender y asociar los vecinos BGP.

  Al igual que en la configuración del router ASR-01 se realiza la misma configuración para el router ASR-02.

El comando utilizado para establecer la conexión TCP con los vecinos es el siguiente: ***neighbor "ip address" remote-as "#SA"*** este número de SA pertenece al SA remoto del vecino o del router con el que se quiere establecer la sesión BGP. La dirección IP corresponde a la dirección de la interfaz del router directamente conectado (next hop). En la **Figura 38** se observa la configuración de vecinos BGP en el router ASR-02.

```
neighbor 190.132.200.241 remote-as 26219
neighbor 190.132.200.241 description Conexion Columbus Backup
neighbor 190.226.132.229 remote-as 3549
neighbor 190.226.132.229 description Conexion Level3 Principal
```

Figura 38: Configuración de vecinos BGP para router ASR-02.

- Para enseñarle a BGP las redes que se van a transportar se utiliza la misma configuración utilizada para el router ASR-01, el comando utilizado es el siguiente: ***network "IP network" mask "mascara de la red"***. En la **Figura 39** se aprecia la configuración para enseñar redes al router ASR-02 que configura el protocolo BGP.

```
network 100.211.192.0 mask 255.255.254.0
network 100.211.194.0 mask 255.255.254.0
network 100.211.196.0 mask 255.255.254.0
network 100.211.198.0 mask 255.255.254.0
network 100.211.200.0 mask 255.255.254.0
network 100.211.202.0 mask 255.255.254.0
network 100.211.204.0 mask 255.255.254.0
network 100.211.206.0 mask 255.255.254.0
network 100.211.207.176 mask 255.255.255.248
```

Figura 39: Configuracion de redes en BGP para el router ASR-01.

En la **Figura 40** muestra el uso del comando ***show running-config,*** el cual nos permite ver toda la configuración realizada en un dispositivo, en este caso el router ASR-02. Se observa la configuración completa del proceso BGP con sus respectivos vecinos y redes aprendidas.

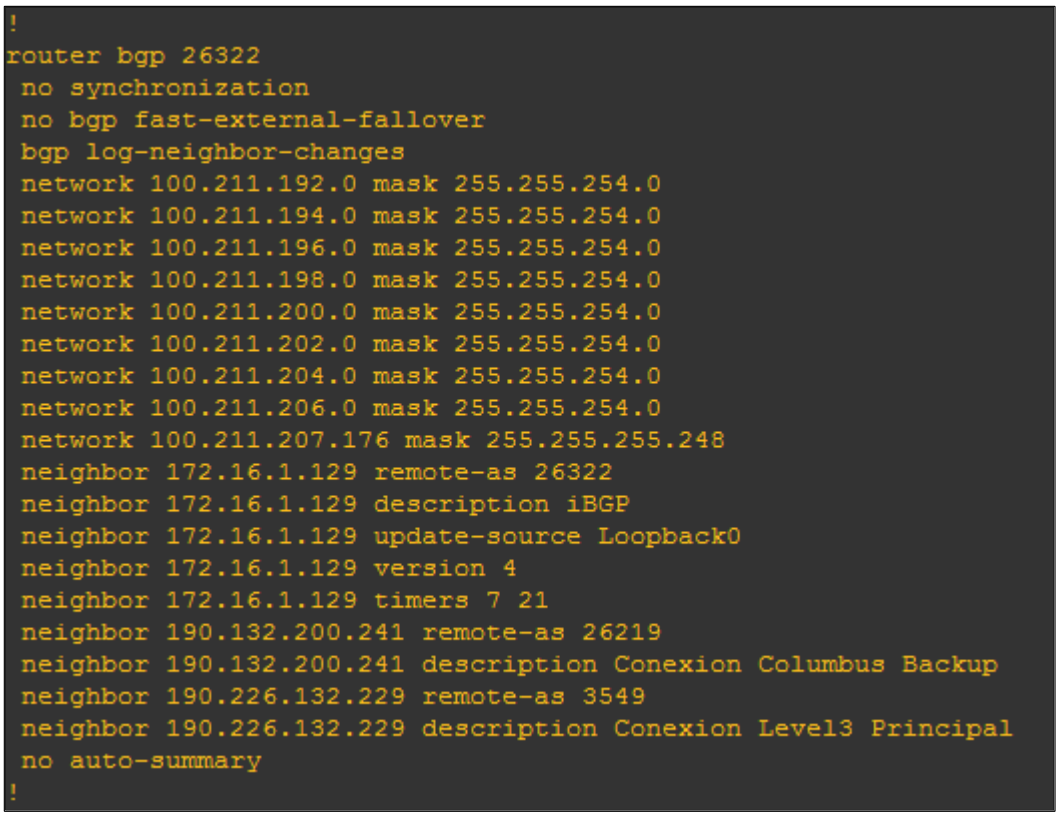


Figura 40: Configuración protocolo BGP en router ASR-02.

Configuración de routers INTERNET, INTERNET-1 y INTERNET-2

- configurar BGP con el Sistema Autónomo (SA) asignado a cada uno de los routers.
  Con el comando ***router bgp "# SA"*** se define el proceso BGP y el respectivo número de SA al que el router pertenece, **INTERNET** con un SA de 1111**, INTERNET-1** con un SA de 26219 y **INTERNET-2** con un SA de 3549
  Para verificar si efectivamente se creó el proceso BGP en cada uno de los routers configurados se digita el siguiente comando en el modo global del dispositivo ***show running-config.***

- Aprender y asociar los vecinos BGP con el comando ***neighbor "ip address" remote-as "#SA"*** este número de SA pertenece al SA remoto del vecino o del router con el

que se quiere establecer la sesión BGP. La dirección IP corresponde a la dirección de la interfaz del router directamente conectado (next hop).

En la **Figura 41** se aprecia la configuración del proceso BGP en el router INTERNET. En este dispositivo se crean dos interfaces virtuales Loopback para simular dispositivos que se encuentran en internet, las direcciones de estas interfaces virtuales son las que se observan en la **Tabla 11:**

```
router bgp 1111
 no synchronization
 bgp log-neighbor-changes
 neighbor 190.116.236.238 remote-as 26219
 neighbor 190.116.236.242 remote-as 3549
 no auto-summary
```

Figura 41: Configuración equipo INTERNET.

Direccionamiento IP Loopback que Simulan Dispositivos en Internet			
INTERFACE	IP	Mascara	Función
Loopback 0	4.4.4.4	255.255.255.255	Dispositivo Internet
Loopback 1	8.8.8.8	255.255.255.255	Dispositivo Internet

Tabla 11: Direcciones Loopback simulando dispositivos en internet.

En la **Figura 42** se observa la configuración del proceso BGP en el router INTERNET-1, se observa que aprende dos redes que son las correspondientes a las interfaces Loopbacks que simulan estar en internet.

```
router bgp 26219
 no synchronization
 bgp log-neighbor-changes
 network 4.4.4.4 mask 255.255.255.255
 network 8.8.8.8 mask 255.255.255.255
 neighbor 190.116.236.237 remote-as 1111
 neighbor 190.132.200.242 remote-as 26322
 neighbor 190.135.236.26 remote-as 26322
 no auto-summary
```

Figura 42: Configuración equipo INTERNET-1.

Se observa en la **Figura 43** la configuración del proceso BGP en el router INTERNET-1, se observa que asocia los vecinos y aprende dos redes que son las correspondientes a las interfaces Loopbacks que simulan estar en internet.

```
router bgp 3549
 no synchronization
 bgp log-neighbor-changes
 network 4.4.4.4 mask 255.255.255.255
 network 8.8.8.8 mask 255.255.255.255
 neighbor 190.116.236.241 remote-as 1111
 neighbor 190.216.222.234 remote-as 26322
 neighbor 190.226.132.230 remote-as 26322
 no auto-summary
```

Figura 43: Configuración equipo INTERNET-2.

NOTA: en INTERNET se crea Loopbacks para simular direcciones que se encuentran en internet.

Configuración del FIREWALL

- Se configuran las direcciones de las redes que se van a anunciar a través de BGP. Cabe aclarar que en la simulación de este trabajo se utiliza un router en vez de un firewall porque en los dispositivos que maneja el simulador GNS3 no se encontró el dispositivo que la topología de red usa, por esta razón es remplazado por un router.

  Al igual que en el router INTERNET se crea interfaces virtuales simulando direcciones de internet, en el router FIREWALL se crean direcciones virtuales para simular hosts que se encuentran en la red del ISP.

  Este dispositivo no habla BGP. La forma de enseñarlas redes a los dispositivos ASR-01 y ASR-02 es mediante enrutamiento estático. En la **Figura 44** se aprecia la configuración de este dispositivo.

```
!
ip route 0.0.0.0 0.0.0.0 100.211.207.180
!
```

Figura 44: Configuración de enrutamiento estático de router FIREWALL.

La dirección 0.0.0.0 con mascara 0.0.0.0 y siguiente salto 100.211.207.180 se utiliza para designar el Gateway de último recurso. Este Gateway es la dirección del protocolo de alta redundancia HSRP.

NOTA: Otro aspecto a tener en cuenta es cada vez que se realizan cambios en la configuración de BGP, es necesario aplicar un ***reset*** a la conexión con el vecino para que los cambios que se realizaron tengan efecto. El comando utilizado es el siguiente: ***clear ip bgp "ip address"*** (donde ip address es la dirección IP del vecino) también se utiliza el comando ***clear ip bgp ** (este comando resetea todas las conexiones con los vecinos).

PASO 4: Configurar el protocolo de redundancia HSRP en los routers ASR-01 y ASR-02 para obtener alta disponibilidad en la red.

NOTA: Teniendo una red de un ISP donde en toda su infraestructura utiliza equipos de manufactura CISCO, se implementa el protocolo de redundancia creado por CISCO el protocolo HSRP debido a que este protocolo utiliza un comando como el track que le dan un plus con respecto al protocolo Virtual Router Redundancy Protocol (VRRP) definido con el RFC 3768, este último protocolo es utilizado cuando se usan dispositivos de red de distintos fabricantes por ejemplo Cisco - Juniper, Cisco – HP o HP - Juniper.

En la **Tabla 12** se observa las direcciones IP que se utilizaran para la configuración del protocolo de redundancia HSRP.

Direccionamiento IP Protocolo HSRP			
INTERFACE	IP	Mascara	Función
FastEthernet 1/0	100.211.207.177	255.255.255.248	HSRP - ASR-01
FastEthernet1/0	100.211.207.179	255.255.255.248	HSRP – ASR-02
Virtual	100.211.207.180	255.255.255.248	Puerta de enlace del protocolo

Tabla 12: Direccionamiento utilizado para configuración del protocolo HSRP.

En las interfaces FastEthernet 1/0 de los routers ASR-01 y ASR-02 se configura el protocolo de redundancia HSRP.

En la **Figura 45** se ve las interfaces en donde se configura el protocolo HSRP.

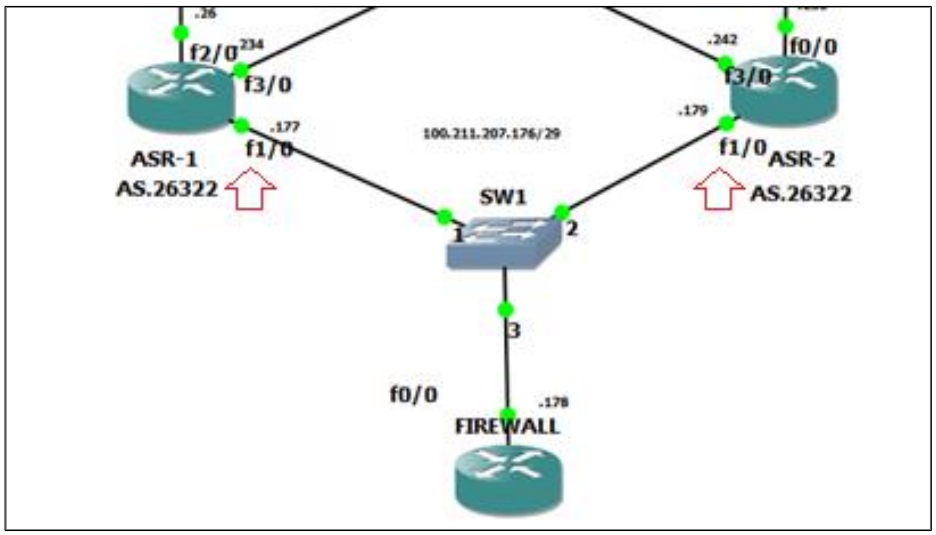


Figura 45: interfaces donde se configura el protocolo HSRP.

En la **Figura 46** se aprecia la configuración utilizada para activar el protocolo HSRP. El protocolo HSRP escoge como router principal al que tenga la prioridad más alta, en este caso la prioridad de 150 es la del router ASR-01 por ende es el router activo para el protocolo HSRP.

```
ASR-01(config)# interface ethernet 0/1
ASR-01(config-if)# ip address 100.211.207.177 255.255.255.248
ASR-01(config-if)# stanby 20 ip 100.211.207.180
ASR-01(config-if)# stanby 20 priority 150
ASR-01(config-if)# stanby 20 preempt
```

Figura 46: Configuración HSRP en el router ASR-01.

Se puede observar en la **Figura 47** la configuración utilizada para activar el protocolo HSRP en el router ASR-02. La prioridad de 120 es la del router ASR-02 y es más baja que la del router ASR-01 por ende este el router se encuentra en espera o en Standby para el protocolo HSRP.

```
ASR-02(config)# interface ethernet 0/1
ASR-02(config-if)# ip address 100.211.207.179 255.255.255.248
ASR-02(config-if)# stanby 20 ip 100.211.207.180
ASR-02(config-if)# stanby 20 priority 120
ASR-02(config-if)# stanby 20 preempt
```

Figura 47: Configuración HSRP en el router ASR-02.

El comando ***preempt*** se utiliza para que el tráfico cambie automáticamente de un router Standby a un router activo.

6. RESULTADOS

Los análisis realizados en el desarrollo del proyecto muestran el funcionamiento de la topología de red que se diseñó para el ISP Ejemplo.Compañia, en primer lugar se realizaron pruebas para garantizar que hay comunicación y establecimiento de sesión entre los vecinos BGP, en segundo lugar se realizan pruebas de conectividad de extremo a extremo (desde un host hacia una dirección en internet), y la tercera prueba es el funcionamiento del protocolo de redundancia HSRP, una vez realizadas estas pruebas se obtiene como resultado lo siguiente:

- Prueba de establecimiento de sesión entre vecinos BGP.

  Como resultado de que las conexiones y los procesos BGP se encuentran correctamente configurados, se procede a verificar que cada uno de los routers que hablan el protocolo de enrutamiento dinámico BGP tengan establecido una sesión BGP con cada uno de sus vecinos, esta verificación de sesión de vecinos se realiza con el siguiente comando: ***show ip bgp sumary***.

  En la **Figura 48** se aprecian las 3 sesiones del router ASR-01, establecidas con los SA 26322, 26219 y 3549.Además se observa que 2 de ellas están activas hace 51 segundos y una sesión activa hace 45 segundos.

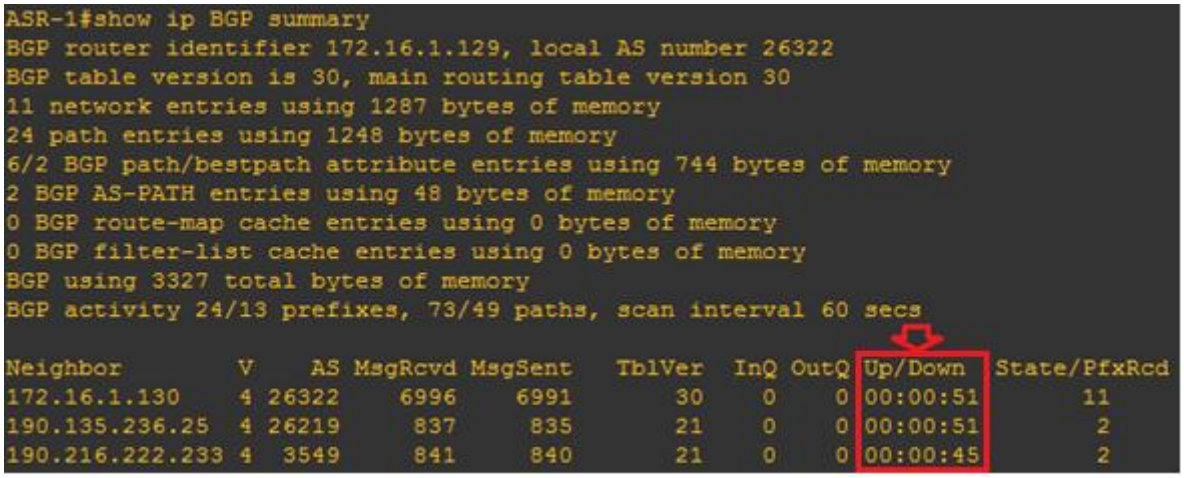


Figura 48: Sesiones establecidas del router ASR-01.

En la **Figura 49**se aprecian las 3 sesiones del router ASR-02, establecidas con los SA 26322, 26219 y 3549 además se observa que todas están activas hace 9 segundos.

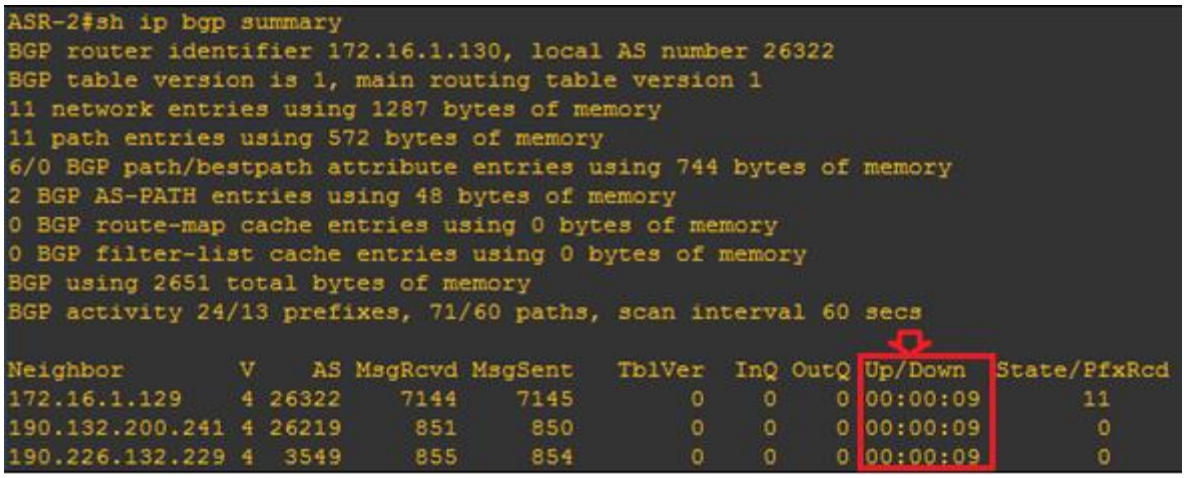


Figura 49: Sesiones establecidas del router ASR-02.

En la **Figura 50** se observa las 3 sesiones del router INTERNET-1, establecidas dos con los SA 26322 y una sesión con el SA 1111, además también se aprecia que 2 de ellas se encuentran activas hace 21 segundos y una sesión activa hace 16 segundos.

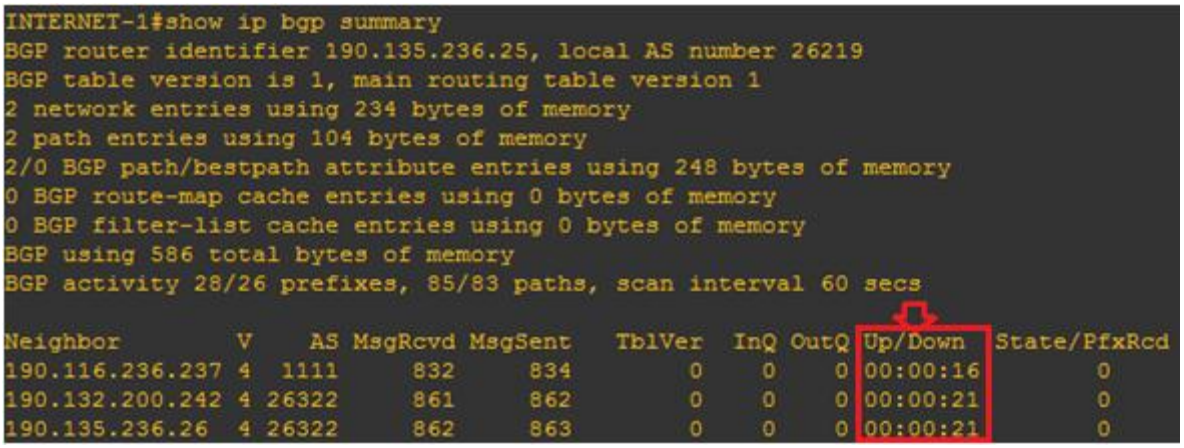


Figura 50: Sesiones establecidas del router INTERNET-1.

Se logra ver en la **Figura 51** las 3 sesiones del router INTERNET-2,2 de ellas establecidas con los SA 26322 y una sesión con el SA 1111, también se aprecia que se encuentran activas hace 40 segundos.

```
INTERNET-2#sh ip bgp summary
BGP router identifier 190.226.132.229, local AS number 3549
BGP table version is 16, main routing table version 16
11 network entries using 1287 bytes of memory
35 path entries using 1820 bytes of memory
6/2 BGP path/bestpath attribute entries using 744 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3947 total bytes of memory
BGP activity 44/33 prefixes, 141/106 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
190.116.236.241 4  1111     887     892       14    0    0 00:00:40        11
190.216.222.234 4 26322     880     880       14    0    0 00:00:40        11
190.226.132.230 4 26322     878     878       14    0    0 00:00:40        11
```

Figura 51: Sesiones establecidas del router INTERNET-2.

En la **Figura 52** se observan las 2 sesiones del router INTERNET, establecidas con los SA 26219 y 3549, además se observa que se encuentran activas hace 1 minuto y 18 segundos.

```
INTERNET#show ip bgp summary
BGP router identifier 8.8.8.8, local AS number 1111
BGP table version is 14, main routing table version 14
11 network entries using 1287 bytes of memory
22 path entries using 1144 bytes of memory
5/2 BGP path/bestpath attribute entries using 620 bytes of memory
4 BGP AS-PATH entries using 96 bytes of memory
0 BGP route-map cache entries using 0 bytes of memory
0 BGP filter-list cache entries using 0 bytes of memory
BGP using 3147 total bytes of memory
BGP activity 55/44 prefixes, 139/117 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
190.116.236.238 4 26219     862     865       14    0    0 00:01:18        11
190.116.236.242 4  3549     907     903       14    0    0 00:01:20        11
```

Figura 52: Sesiones establecidas del router INTERNET.

- Prueba de conectividad de extremo a extremo.

  En esta prueba de conectividad se verifica la comunicación que existe entre las Loopback que simulan los host hacia las Loopbacks que se encuentran en internet. Para realizar esta prueba se utiliza el comando ***ping*** y ***traceroute***, en la **Figura 53** se aprecia las pruebas realizadas a la topología de red.

```
FIREWALL#ping 4.4.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 80/110/192 ms
FIREWALL#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/122/156 ms
```

Figura 53: Prueba de PING.

Se observa que las pruebas de ping realizadas desde el router FIREWALL al router INTERNET se realizaron correctamente. Se aprecia en la Figura 54 las pruebas realizadas con el comando ***traceroute.***

```
FIREWALL#traceroute 4.4.4.4

Type escape sequence to abort.
Tracing the route to 4.4.4.4

  1 100.211.207.177 96 msec 68 msec 96 msec
  2 190.135.236.25 192 msec 148 msec 96 msec
  3 190.116.236.237 216 msec 96 msec 152 msec
FIREWALL#traceroute 8.8.8.8

Type escape sequence to abort.
Tracing the route to 8.8.8.8

  1 100.211.207.177 72 msec 64 msec 64 msec
  2 190.135.236.25 64 msec 92 msec 64 msec
  3 190.116.236.237 128 msec 164 msec 96 msec
```

Figura 54: Prueba traceroute.

Se observa que efectivamente los mensajes enviados de prueba al router de INTERNET llegan correctamente.

- Prueba de funcionamiento protocolo HSRP.

  Para probar el funcionamiento del protocolo de redundancia HSRP se procede a verificar la función de cada uno de los routers. Con el comando ***show Standby brief*** se verifica en qué estado se encuentra el router ya sea en activo o en pasivo.
  En la **Figura 55** se ve que función tiene el router ASR-01 en el funcionamiento del protocolo HSRP.

```
ASR-1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Fa1/0       20  150  P Active   local           100.211.207.179 100.211.207.180
```

Figura 55: verificación de estado de HSRP en el router ASR-01.

Se observa que el router local se encuentra activo y el router con dirección IP de 100.211.207.179 se encuentra en Standby. También se observa la prioridad que tiene el router ASR-01 que es de 150.

En la **Figura 56** se aprecia que función tiene el router ASR-02 en el funcionamiento del protocolo HSRP.

```
ASR-2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Fa1/0       20  120  P Standby  100.211.207.177 local           100.211.207.180
```

Figura 56: verificación de estado de HSRP en el router ASR-02.

Se observa que el router local se encuentra en Standby y el router con dirección IP de 100.211.207.177 se encuentra en activo. También se observa la prioridad que tiene el router ASR-02 que es de 120.

Conociendo que router tiene estado activo y que router tiene el estado Standby se procede a realizar la prueba de funcionamiento del protocolo HSRP.
Se deshabilita la interfaz FastEthernet 1/0 del router ASR-01 y se verifica si el router que se encontraba en estado Standby cambia su estado a activo, si realiza el cambio automáticamente el protocolo de redundancia HSRP se configuro

correctamente. En la **Figura 57** se observa la interfaz que se deshabilitara en la topología de red.

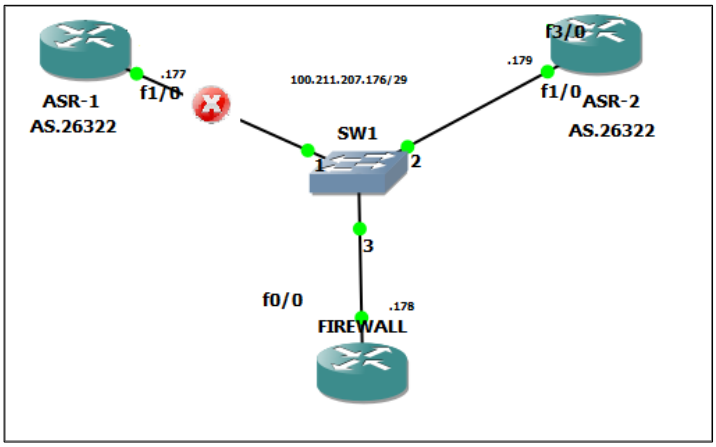


Figura 57: Interfaz deshabilitada para prueba de protocolo HSRP.

Una vez deshabilitada la interfaz se procede a realizar prueba de conectividad para verificar que los mensajes siguen llegando a su destino. Esta prueba se realiza con el comando PING.

Se aprecia en la **Figura 58** la prueba de conectividad de extremo a extremo.

```
FIREWALL#ping 4.4.4.4

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 4.4.4.4, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/132/176 ms
FIREWALL#ping 8.8.8.8

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 96/114/188 ms
```

Figura 58: Prueba de conectividad con comando PING.

Se observa que existe comunicación desde el router FIREWALL al router INTERNET. En la **Figura 59** se observa la verificación de estado HSRP en el router ASR-01.

```
ASR-1#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Fa1/0       20  150  P Init     unknown         unknown         100.211.207.180
```

Figura 59: Verificación de estado HSRP en router ASR-01 con interfaz deshabilitada.

Se observa que el estado se encuentra desconocido debido a que se encuentra deshabilitada la interfaz en donde se configura el protocolo de redundancia HSRP. En la **Figura 60** se verificara en qué estado se encuentra el router ASR-02.

```
ASR-2#show standby brief
                     P indicates configured to preempt.
                     |
Interface   Grp Prio P State    Active          Standby         Virtual IP
Fa1/0       20  120  P Active   local           unknown         100.211.207.180
```

Figura 60: Verificación de estado HSRP en router ASR-02.

Se observa que el router ha cambiado de estado, antes se encontraba en estado Standby y ahora se encuentra en estado activo, esto quiere decir que la configuración del protocolo de redundancia HSRP se realizó correctamente y el router en estado Standby remplaza las funciones del router en estado activo correctamente.

7. CONCLUSIONES

- Antes de implementar el protocolo BGP en un dispositivo de red, es importante saber que el dispositivo sea capaz de ejecutar todos los procesos BGP sin que afecte el procesamiento, es decir que el dispositivo soporte el protocolo BGP sin ninguna sobrecarga de procesamiento. Con respecto a la configuración e implementación del protocolo BGP se observó que es importante en el momento de crear las sesiones BGP, introducir las direcciones IP correctas de los vecinos BGP, esto para evitar inconvenientes en el momento de establecer sesión BGP con los routers que hablan este protocolo.

- Según las pruebas y resultados obtenidos al desconectar manualmente un punto en la interface de los routers que prestan la salida hacia internet se puede concluir que es importante tener una redundancia en la red, haciendo notar beneficios que tienen en la red del ISP, vale la pena destacar que teniendo una redundancia debidamente configurada se reduce el porcentaje de fallos en la red de forma significativa, así pues la redundancia de red permite mitigar errores o fallos de una manera dinámica y eficaz posible en la red del ISP.

- Este trabajo permite visualizar de una manera más amplia el impacto que tiene mantener una red de un ISP en buena calidad para que así preste un servicio óptimo a la sociedad y se reduzca el número de llamadas del cliente informando la pérdida del servicio prestado, además que se observa de una manera técnica las consecuencias que tiene tener una red que presenta inconvenientes.

- Utilizando una conexión BGP Dual Multi-Homed el diseño de red mitiga las fallas de envío de datos que se presenten en el ISP, de esta manera si se detecta una falla que afecta el funcionamiento del ISP, el diseño de topología

de red del ISP es capaz de transportar el tráfico a través de otro camino que no se vea afectado por la falla generada.

- Al trabajar con este tipo de problemas se contempla la capacidad y las buenas bases teóricas y prácticas que tiene un ingeniero de Telecomunicaciones de la Universidad Santo Tomas para el desarrollo, implementación y solución de problemas frecuentes y reales con los que cuentan diferentes empresas en el sector de las telecomunicaciones.

- Se aprecia que en algunas empresas que prestan servicios de Telecomunicaciones tienen problemas para solucionar sus propios problemas de red, esto incita a las empresas a buscar personal capacitado para el desarrollo de soluciones a los problemas de la empresa.

BIBLIOGRAFÍA

Ahuatzin, G. (2009). *Desarrollo de un esquema de traduccion de direcciones IPv6-IPv4-IPv6.* Obtenido de http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/ahuatzin_s_gl/capitulo2.pdf

Alcalá, U. d. (2011). *Protocolos de enrutamiento dinamico.* Obtenido de http://atc2.aut.uah.es/~jmruiz/Descarga_LE/Prac_3.ProtocolosEnrutamientoDinamico_RIP_y_OSPF.pdf

Balchunas, A. (2007). *Routeralley.* Obtenido de http://www.routeralley.com/guides/bgp.pdf

BGP, F. (2012). Obtenido de http://bibing.us.es/proyectos/abreproy/11359/fichero/BGP%252F5.+Fundamentos+de+BGP.pdf

CISCO. (2007). *Conceptos y Protocolos de Enrutamiento Capitulo 2.*

CISCO. (2010). CCNP ROUTE: Implementing IP Routing. *Chapter 6: Implementing a Border Gateway Protocol Solution for ISP Connectivity*.

CISCO. (2010). CCNP Swithing Module 6: First Hop Redundancy Protocol Implementation.

CISCO. (2011). IP Addressing: IPv4 Addressing. San Jose, California, USA.

computadores, R. d. (2005). *Simuladores ´Open-Free´*. Obtenido de http://blogs.ua.es/redesitis/recursos-didacticos/simuladores-open-free/

David Alvarez, J. P. (02 de Junio de 2009). *Proveedores de Servicios de Internet y de contenidos, responsabilidad civil y derechos de autor.* Obtenido de file:///C:/Users/Perez/Downloads/Dialnet-ProveedoresDeServiciosDeInternetYDeContenidosRespo-3658940.pdf

Dominguez, J. A. (2004). *University of Oregon.* Obtenido de http://ws.edu.isoc.org/data/2004/101532717144826b46d9c9e/bgp.pdf

España, U. d. (2006). *Redes de nueva generacion.* Obtenido de Area de Ingeneria Telematica: https://www.tlm.unavarra.es/~daniel/docencia/rng/rng14_15/slides/Tema2-01-BGP.pdf

Gazmuri, I. d. (2008). *fundacionfueyo.udp.cl.* Obtenido de Responsabilidad de los proveedores de servicios de internet por infraccion de los derechos de autor: http://fundacionfueyo.udp.cl/articulos/inigo_de_la_maza/responsabilidad%20isp.pdf

Goita, M. J. (2003). *Universidad Nacional del Nordeste.* Obtenido de Facultad de Ciencias Exactas: http://exa.unne.edu.ar/informatica/SO/tfjuly.PDF

Gonzalez, L. (2010). *IES Los Viveros Sevilla.* Obtenido de DPTO Electronica: http://www.ieslosviveros.es/alumnos/asig8/carpeta812/PROTOCOLOS_DE_ENRUTAMIENTO.pdf

Hucaby, T. B. (2001). Cisco CCNP Switching Exam Certification Guide. Indianapolis.

Kucherawy, M. (Junio de 2012). *Creation and use of email feedback reports: An applicability statement for the abuse reporting format (ARF)*.

Litoral, E. S. (2010). *Diseño e Implementación de Experiencias Docentes para un Sitio de Proveedor de Servicios de Internet.* Ecuador.

Maldonado, J. (15 de 07 de 2012). *Simuladores de red*. Obtenido de http://simuladoresredes.blogspot.com.co/

Mayán, I. D. (2010). *Direcciones IP y clases de redes.* Obtenido de https://unalm-construcion2010.wikispaces.com/file/view/p)+Redes+y+subredes.pdf

Mesa, M. L. (2007). *e-REdING.* Obtenido de Trabajos y proyectos fin de estudios de la E.T.S.I.: http://bibing.us.es/proyectos/abreproy/11359/direccion/BGP%252F

Nava, J. (2008). *Direccionamiento IPv4.* Obtenido de https://juannava64.files.wordpress.com/2012/02/redes-direccionamiento-ipv4.pdf

Navarra, U. d. (2012). *Tecnologias Azanzadas de Red.* Obtenido de https://www.tlm.unavarra.es/~daniel/docencia/tar/tar13_14/practicas/practica6-BGP.pdf

Overview, I. T. (2011). Obtenido de ftp://ftp.ccc.de/docs/vortraege/Felix%20-%20IP%20Routing/support/EGP.pdf

Oviedo, U. d. (2006). *Tema 6: El Protocolo TCP/IP.* Obtenido de http://www.isa.uniovi.es/docencia/redes/Apuntes/tema6.pdf

Rafael Moreno, R. M. (2010). *Grados Ing Informatica/Ing Computadores/ Ing Software.* Obtenido de Universidad Complutense de Madrid: https://www.fdi.ucm.es/profesor/rubensm/ASOR/Trasparencias/Tema%200-%20Revision%20del%20Protocolo%20IPv4.pdf

Sandra, J. R. (http://bibdigital.epn.edu.ec/bitstream/15000/2693/1/CD-3378.pdf de 12 de 2010). *Escuela Politecnica Nacional.*

Teldat, R. (Marzo de 2008). *Protocolo BGP.* Obtenido de ftp://ftp.storm.hr/Upload/Teldat_privremeno/Teldat_dokumentacija/documentacion/Manuales%2010.6/Dm763/Dm763v10-61_Protocolo_BGP.pdf

UPM. (2013). *Universidad politecnica de Madrid.* Obtenido de http://www.elai.upm.es/webantigua/spain/Asignaturas/redes/laboratorio/Practica5.pdf

Velasco, R. (20 de 03 de 2014). *REDESZONE*. Obtenido de http://www.redeszone.net/2014/03/20/lista-de-simuladores-de-redes-para-virtualizar-nuestra-propia-red/

Veracruzana, U. (2014). *enrutamiento estatico.* Obtenido de http://www.uv.mx/personal/ocruz/files/2014/01/Enrutamiento-estatico.pdf