PROPUESTA TÉCNICA PARA AUMENTAR EL ANCHO DE BANDA DEL SERVICIO DE INTERNET EN TELNOVA S.A.S. POR MEDIO DE BALANCEÓ DE CARGA

David Julián Barón Pastrana

Trabajo de grado presentado para optar al título de:

Ingeniero De Telecomunicaciones

Director:

Ing. Rafael Cubillos Sánchez (Msc)

Universidad Santo Tomás

Facultad De Ingeniería De Telecomunicaciones

Bogotá D.C. Colombia

2021

TABLA DE CONTENIDO

GLOSARIO

- BGP (Border Gateway Protocol)
- IP (Internet Protocol)
- IPSLA (Internet Protocol Service Level Agreement)
- GLBP (Gateway Load Balancing Protocol)
- AVG (Active Virtual Gateway)
- HSRP (Hot Standby Router Protocol)
- VRRP (Virtual Router Redundancy Protocol)
- IETF (Internet Engineering Task Force)
- RFC (Request for Comments)
- MAC (Media Access Control)
- ISP (Internet Service Provider)
- xDSL (Digital Subscriber Line)
- HFC (Hybrid Fiber Coaxial)
- SDH (Synchronous Digital Hierarchy)
- 3G (Third Generation of Wireless Mobile)
- 4G (Fourth Generation of Wireless Mobile)
- GPON (Gigabit Passive Optical Network)
- FO (Optical Fiber)
- Throughput (Effective Transfer Rate)
- CPE (Customer Premises Equipment)
- IOS (Internetwork Operating System)

RESUMEN

Se desarrolla un proceso de investigación documental en el cual se tiene como objetivo realizar una propuesta técnica para aumentar el ancho de banda del servicio de internet en la empresa Telnova S.A.S. Utilizando la infraestructura disponible en el municipio de paz de Ariporo, por medio de la recopilación de resultados de artículos científicos se decide realizar la propuesta técnica utilizando el protocolo VRRP en configuración de balanceo de carga y topología redundante de dos canales, con el fin de sumar el ancho de banda para aumentar la capacidad total. La propuesta es simulada en el software GNS3 comprobando que la solución planteada es viable de aplicar en un entorno real. Como resultado del análisis de las rutas de los paquetes IP se obtiene ampliación de ancho de banda con tráfico asimétrico.

Palabras clave: VRRP;GNS3;Topologia;Redundante;Balanceo.

ABSTRACT

A documentary research process is developed in which the objective is to make a technical proposal to increase the bandwidth of the internet service in the company Telnova S.A.S. Using the infrastructure available in the municipality of Paz de Ariporo, through the collection of results from scientific articles, it was decided to carry out the technical proposal using the VRRP protocol in load balancing configuration and redundant two-channel topology, in order to add bandwidth to increase total capacity. The proposal is simulated in the GNS3 software, checking that the proposed solution is feasible to apply in a real environment. As a result of the analysis of the IP packet routes, bandwidth expansion is obtained with asymmetric traffic.

Keywords: VRRP;GNS3;Topology;Redundant;Balancing.

1 INTRODUCCIÓN

1.1 PLANTEAMIENTO DEL PROBLEMA

La empresa Telnova S.A.S se proyecta como un micro operador de telecomunicaciones para brindar servicios de internet en hogares ubicados en el municipio de Paz De Ariporo en el departamento de Casanare. tiene un problema técnico relacionado con la capacidad de ancho de banda del servicio de internet que puede contratar con los proveedores de telecomunicaciones locales, dicha capacidad está limitada a 1Gbps debido a que esta es la máxima capacidad ofrecida por los proveedores locales ya que estos operadores no cuentan con la infraestructura adecuada para ofrecer servicios de mayor ancho de banda. Para que estos proveedores puedan ofrecer canales de internet de una capacidad superior se requiere que ellos adquieran equipos de transmisión con puertos que soporten estándares de 10Gbps. Los principales operadores de telecomunicaciones del país no penetran el mercado local con equipos de vanguardia que puedan brindar conexiones de 10Gbps debido a que Paz De Ariporo, es un municipio de baja densidad poblacional el cual cuenta con aproximadamente 26.104 habitantes.[1] Esta condición influye directamente en la demanda de servicios, razón por la cual los operadores no contemplan la modernización y ampliación de capacidad sobre la infraestructura actualmente instalada en el casco urbano, a un corto o mediano plazo. Por tal motivo se sugiere la adquisición de un nuevo canal de internet.

Se plantea el interrogante, ¿qué solución técnica se le puede brindar a la empresa Telnova S.A.S. para lograr aumentar el ancho de banda del servicio de internet a un corto plazo con la infraestructura que ofrecen los operadores actualmente en el municipio de Paz de Ariporo?

1.2 JUSTIFICACIÓN

El mundo empresarial se encuentra en constante competencia, por lo tanto, ninguna empresa puede arriesgar su cuota de mercado por prestar un mal servicio debido a que la experiencia que le brinde a sus clientes sea afectada por problemas de lentitud y pérdida de datos relacionado con anchos de banda insuficientes, adicionalmente las solicitudes de ampliación de servicio deben ser realizadas en el menor tiempo posible. Por tal motivo se hace necesaria la búsqueda de alternativas a corto plazo para ampliar el canal de internet de la empresa Telnova S.A.S.

1.3 OBJETIVOS

1.3.1 Objetivo General:

Realizar una propuesta técnica para aumentar el ancho de banda del servicio de internet en Telnova S.A.S. por medio de la adquisición de un nuevo canal de internet para opera en modo de balanceó de carga.

1.3.2 Objetivos Específicos:

- Identificar las características de los protocolos disponibles para realizar balanceo de tráfico IP.
- Proponer topologías de redundancia en capa 3 para la empresa Telnova S.A.S.
- Elaborar diseño de red con balanceo de carga utilizando protocolos de uso general para todo fabricante de dispositivos de red.
- Evaluar la funcionalidad de la propuesta técnica por medio del simulador GNS3.

1.4 ALCANCE

Se realiza una propuesta técnica basada en un diseño de red probado en laboratorio bajo simulación de GNS3, en la cual se evalúa la funcionabilidad del diseño de red propuesto, para ser implementado en la empresa Telnova S.A.S

2 MARCO TEÓRICO

Se realiza la conceptualización de los principales protocolos que son utilizados en el desarrollo del trabajo, enfocando el capítulo en los protocolos de redundancia IP tales como VRRP, HSRP y GLBP. Es fundamentar recibir contextualización acerca de estos protocolos debido a que los mismos son la base de la investigación realizada en la cual se pretende brindar una solución de balanceo de carga utilizando los protocolos de redundancia y el protocolo BGP como único protocolo de enrutamiento en este documento.

2.1 VRRP (VIRTUAL ROUTER REDUNDANCY PROTOCOL)

El protocolo VRRP es seleccionado para ser implementado en la propuesta técnica presentada a la empresa Telnova S.A.S debido a que es un protocolo libre que puede ser utilizado en cualquier fabricante de equipos de telecomunicaciones, en la propuesta que se plantea se pretende utilizar el protocolo para segmentar la red en dos grupos, cada grupo tendrá salida a internet por un proveedor diferente de esta manera se logra aumentar el ancho de banda.

VRRP especifica un protocolo de elección que asigna dinámicamente la responsabilidad de ser el enrutador virtual en un grupo de routers que estén ejecutando el protocolo. El enrutador virtual es el encargado de realizar el reenvió de los paquetes que son recibidos por la IP virtual. De esta manera se define al protocolo VRRP como un protocolo de redundancia dinámico.[2]

El rol de enrutador virtual es asignado al router del grupo con el valor del parámetro priority más alto, este enrutador virtual será conocido como router en estado master, en dado caso que el router que está operando como enrutador virtual presente fallos otro enrutador del grupo asumirá el estado de master y continuará con el reenvió de los paquetes de tal manera que los hosts, usuarios finales del servicio no notarán la falla en el primer enrutador.[3]

VRRP es un protocolo de código abierto estandarizado por el IETF (Internet Engineering Task Force) bajo el RFC (Request for Comments) 2338 y su actualización a IPv6 bajo el RFC 5798 en la categoría de Standards Track, a continuación, se realiza la conceptualización de los principales Parámetros del protocolo VRRP.

2.1.1 Virtual IP Address:

Es la dirección IP escogida como puerta de enlace para los hosts, el tráfico que se envié a esta dirección IP será reenviado por el enrutador en estado master, la virtual IP Address estará disponible en la red siempre y cuando el protocolo VRRP este activo, asegurando de esta manera la alta disponibilidad del servicio.[4]

2.1.2 Priority:

Es el valor que será usado para determinar la elección del router maestro dentro del protocolo VRRP, el rango de valores de priority habilitado para ser configurado es de 1 a 254. [2]

2.1.3 Advertisement Interval:

El tiempo en segundos que se configura para determinar el intervalo entre él envió de las actualizaciones del protocolo VRRP en los miembros del grupo, el rango esta entre 1 a 254.[2]

2.1.4 Master Down Interval:

Es el tiempo que espera el router Backup antes de tomar el estado de master en caso de que el router master deje de responder las notificaciones de estado enviadas por el protocolo. Está determinado por la siguiente formula. (3 * Master_Adver_Interval) + (((256 - priority) * Master_Adver_Interval) / 256).[2]

2.1.5 Virtual Router MAC Address:

Dirección MAC virtual que el protocolo VRRP asigna a la dirección IP virtual con la cual dará respuesta ARP a los hosts que envíen paquetes a la IP virtual. [2]

2.1.6 Preempt Mode:

Contrala el cambio de estado master si el modo preempt está habilitado permite que un router que ingrese al grupo VRRP con un valor de priority mayor que el valor del router master tome el estado de master, si el modo preempt esta deshabilita no permite que un router con valor de priority mayor que el valor del router master se apropie del estado master de esta manera el cambio de estado master en dispositivos activos será realizado de manera manual.[3]

2.1.7 Estado Initialize:

El propósito del estado initialize es esperar a que ocurra un evento en el grupo VRRP, de esta manera todos los routers pertenecientes al grupo VRRP comienzan por este estado y comparten sus valores de priority para determinar el estado correspondiente. Dependiendo del valor del priority de mayor a menor, tomaran el estado master, backup o initialize.[3]

2.1.8 Estado Backup:

El propósito del estado backup es monitorear la disponibilidad del router master, de tal manera que si el router backup no recibe mensajes de protocolo VRRP antes de superar el tiempo determinado por el (master down interval), el router backup asumirá el estado de master.[3]

2.1.9 Estado Master:

En el estado master el router asumirá la función de ser el propietario de la IP virtual y la virtual MAC Address. De esta manera realizara el reenvió de los paquetes que se dirijan a la IP virtual del grupo VRRP.[3]

2.1.10 Diagrama de Transición de Estados:

Los estados del protocolo VRRP se presentan en un diagrama que representa la dirección del flujo que pueden tomar los estados el protocolo.

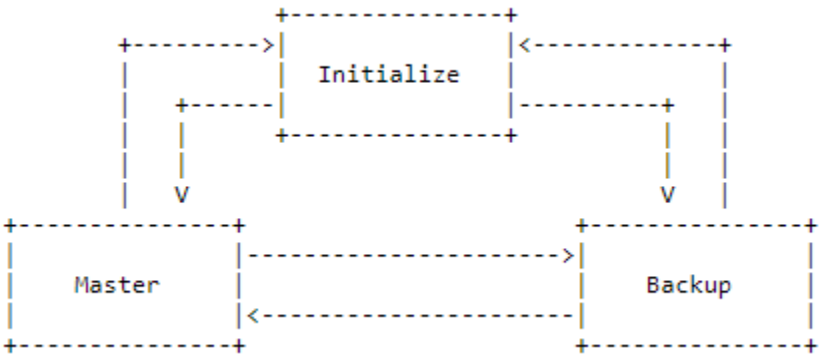

Ilustración 1 Diagrama de transición de estados del protocolo VRRP.

Internet Engineering Task Force RFC 5798 [3]

Como se observa en la imagen el estado del protocolo puede cambiar en sentido horario y viceversa, de tal manera que un conjunto de routers que se encuentren en el mismo grupo VRRP arrancan en estado initialize. Paso siguiente el router con el valor de priority más alto tomará el estado de master el router con el segundo valor más alto en el parámetro priority tomará el estado de backup, y un tercer router del grupo VRRP permanecerá en estado initialize, de esta manera si el router master llegara a salir del grupo, los estados se moverían en sentido horario pasando el router backup al estado de master, y el router initialize al estado de backup. De igual manera si el router con el valor de priority más elevado regresa nuevamente al grupo el diagrama de estados se movería en sentido anti horario pasando el nuevo router master a estado backup y el nuevo router backup ha estado initialize y así el router con el valor de priority más elevado recupera el modo master.[3]

2.1.11 Show VRRP:

En él cuadro de texto 1 se muestra un ejemplo del protocolo VRRP ejecutándose sobre un router, en el cual se observan los resultados de los parámetros mencionados anteriormente.

```
R1#show vrrp
FastEthernet0/0 - Group 1
  State is Master
  Virtual IP address is 223.0.1.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3.000 sec
  Preemption enabled
  Priority is 120
    Track object 1 state Up decrement 30
  Master Router is 223.0.1.3 (local), priority is 120
  Master Advertisement interval is 3.000 sec
  Master Down interval is 9.531 sec
R1#
```

Cuadro de texto 1 Show VRRP (resultado de los parámetro VRRP en ejecución).

2.2 HSRP (HOT STANDBY ROUTER PROTOCOL)

El objetivo del protocolo es permitir que los hosts aparenten utilizar un único enrutador como puerta de enlace predeterminada, cuando en realidad cuentan con un grupo de enrutadores, de tal manera que los usuarios no se afecten con pérdidas de servicio en caso de que un enrutador comience a fallar o se presente pérdida en la conexión de última milla del mismo enrutador. El protocolo asegura que un solo enrutador miembro del grupo será encargado de la recepción y reenvió de paquetes. El cual será denominado como enrutador virtual.[5]

El protocolo HSRP es propietario de la empresa de tecnología Cisco Systems, para uso exclusivo de sus sistemas operativos Cisco IOS (Internetwork Operating System), el protocolo HSRP se encuentra descrito por el RFC 2281 del IETF en la categoría de Informational.[6]

2.2.1 Active Router:

Es el router que actualmente reenvía los paquetes del router virtual, atendiendo las peticiones de los hosts de la red y los paquetes que se dirijan a los hosts.[7]

2.2.2 Standby Router:

Es el router de respaldo principal, el que se encuentra a la espera para tomar el papel de active router. [8]

2.2.3 Standby Group:

Es el conjunto de routers que participan en el proceso HSRP como miembros del grupo a la espera de tomar las funciones del router virtual. [6]

2.2.4 Hello Time:

Es el intervalo entre mensajes Hello HSRP enviado por un enrutador dado a los miembros del grupo.[8]

2.2.5 Hold Time:

El intervalo entre la recepción de un mensaje Hello y la presunción de que la transmisión del enrutador ha fallado, superando el umbral del hold time el router asume que el trasmisor del mensaje abandona el grupo.[9]

2.2.6 Priority:

Este parámetro es utilizado para la elección del active router y standby router el valor de priority mayor es el que determina el active router.[6]

2.3 GLBP (GATEWAY LOAD BALANCING PROTOCOL)

Es un protocolo orientado a proveer redundancia a las redes a nivel de capa 3, es un protocolo privado propiedad de la empresa Cisco Systems, al igual de HSRP. El protocolo GLBP está orientado nativamente a realizar tareas de balanceo de carga a nivel LAN entre un mismo grupo de enrutadores.

2.3.1 Active Virtual Gateway:

Active virtual Gateway (AVG) es el rol que asume el router principal el cual será designado por tener la prioridad más alta en cada grupo, en GLBP se configuran grupos los cuales pueden estar relacionados directamente a las VLAN. [5]

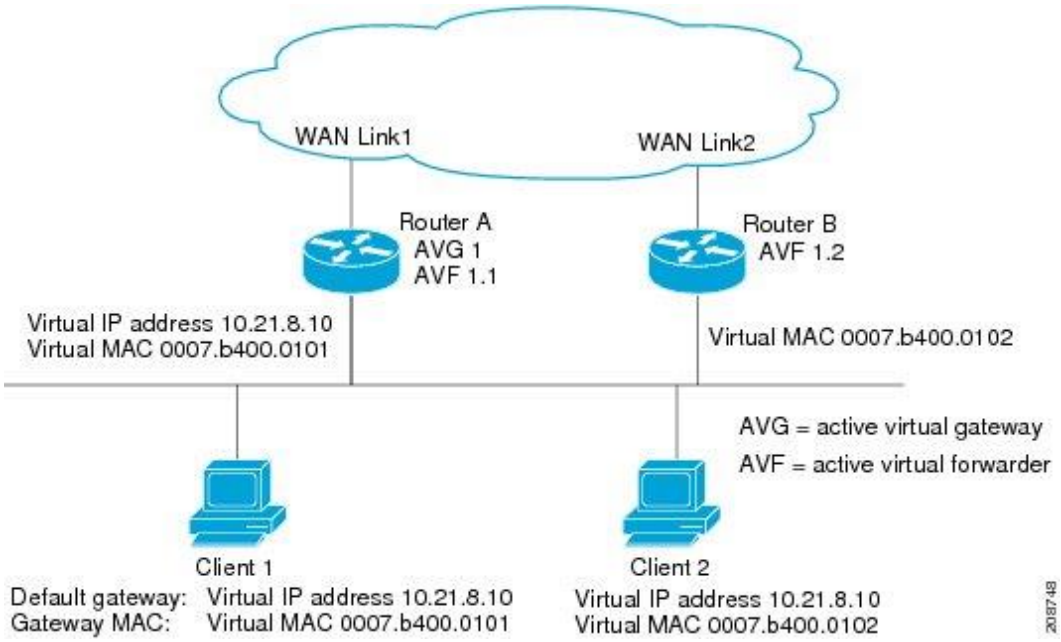

Ilustración 2 Conformación del protocolo GLBP.

First Hop Redundancy Protocols Configuration Guide, Cisco[5]

Cuando se cambia de AVG el nuevo AVG asume la dirección MAC virtual del router 1 y luego responde las solicitudes ARP con su dirección MAC y los nuevos paquetes los envía con la dirección MAC que le pertenece al AVF 2 (Active Virtual Forwarder).[5]

Las funcionalidades de balanceo de carga del protocolo GLBP pueden ser configuradas de las siguientes maneras:[10]

- Round Robin: es un método de equilibrio de carga predeterminado. Utiliza la dirección MAC de la siguiente AVF (basada en solicitudes) para cada nueva solicitud

de ARP para el virtual enrutador, se asigna un AVF diferente al anterior en cada solicitud.

- Weighted: el algoritmo utiliza valores de peso anunciados por la AVF. Cuanto mayor sea el valor de peso del AVF más equipos se conectarán al mismo, de esta manera se puede asignar más carga de trabajo a un router del grupo.

2.4 BGP (BORDER GATEWAY PROTOCOL)

Es importante contextualizar el protocolo BGP debido a que es el protocolo de enrutamiento dinámico mediante el cual un operador de telecomunicaciones comparte las tablas de enrutamiento con las demás empresas que conforman la red de internet. El protocolo BGP es fundamental en las topologías de redundancia por que permite anunciar las redes de tal manera que en internet no se presenten bucles de enrutamiento.

El protocolo de puerta de enlace de frontera se caracteriza principalmente por el manejo de las tablas de enrutamiento de manera dinámica y está orientado a las conexiones de gateway exterior, brindando la interconexión entre sistemas autónomos. Las características del protocolo BGP en su versión 4 están definidas sobre el número de RFC 4271 en la categoría Standards Track.[11]

La principal función del protocolo BGP es intercambiar información de las tablas de enrutamiento entre sistemas autónomos, resaltando el hecho de evitar bucles de enrutamiento con la política de selección de rutas basada en vector de ruta, por medio de la cual se descartan rutas repetidas y se busca el camino por medio del menor número de saltos de sistemas autónomos.[11]

2.4.1 Sistema Autónomo:

Un sistema autónomo es un grupo de redes de datos IP que son organizadas por uno o más administradores que poseen una clara y única política de enrutamiento.[12] Principalmente un sistema autónomo está conformado por una única empresa, también se suele presentar que una empresa que ha adquirido a otras organizaciones suela contar con más de un numero de sistema autónomo.

La numeración de 16 bits de los sistemas autónomos está definida bajo el RFC 1930 y es utilizada para la diferenciación de los diferentes sistemas autónomos utilizando números enteros del 0 al 65535.[13] debido a la rápida ampliación de internet fue necesario habilitar un rango extendido de numeración utilizando 32 bits para realizar la identificación de números enteros entre el rango de 0 al 4294967295. Esta numeración fue definida por la RFC 4893.[14]

3 RESUMEN DE ANÁLISIS DE RESULTADOS DE PROTOCOLOS DE REDUNDANCIA

El objetivo de este capítulo es resumir las principales conclusiones que han obtenido grupos de investigación científica a lo largo de los años, realizando comparaciones y evaluaciones de los protocolos orientados a redundancia de la red. Y con base en estos resultados tomar una decisión respecto a cuál protocolo implementar en la red de Telnova S.A.S.

Con base a la evaluación de rendimiento del protocolo HSRP y GLBP para servicios de transmisión de video, realizado en la universidad de Yakarta, Indonesia en el año 2019. Se logra concluir que el protocolo HSRP obtuvo mejor desempeño que el protocolo GLBP, comparando los siguientes parámetros:[7]

Ilustración 3 Comparación entre protocolo HSRP y GLBP.

Evalusi Kinerja Hot Standby Router Protocol (HSRP) dan Gateway Load Balancing Protocol (GLBP) untuk Layanan Video Streaming [7]

- El valor promedio del retraso de paquetes IP en el protocolo HSRP es de 0.0159 ms comparados con 0.0344 ms del protocolo GLBP, entendiendo que el protocolo HSRP con menor retraso presenta el mejor rendimiento en escenarios de trasmisión de video.[7]

- El porcentaje de perdida de paquetes en pruebas de trasmisión de video para el protocolo GLBP es de 1.46% mientras que para HSRP es de 1.08%, teniendo claridad que mientras menor sea el valor de pérdida de paquetes en la red, mejor será el desempeño por tal motivo el protocolo HSRP presenta el mejor rendimiento en este parámetro evaluado.[7]
- En la prueba realizada se evaluó el rendimiento de throughput de los dos protocolos dando como resultado HSRP con valor de 738 Kbps y GLBP con 693 Kbps, entendiendo el valor más alto como el mejor rendimiento.[7]

Tomando como referencia el estudio de evaluación de rendimiento de los protocolos de redundancia VRRP, HSRP y GLBP en el cual se evaluó parámetros de calidad de servicio tales como fluctuación, perdida de paquetes y tiempo de inactividad, mediante un modelo de simulación basado en etapas en el cual se logra llegar a la conclusión que el protocolo GLBP presenta mejores resultados en los parámetros evaluados. [15]

Se realizan pruebas con equipos reales en laboratorio basadas en los tiempos de respuesta aproximado para cada uno de los protocolos VRRP, HSRP y GLBP y como conclusión se obtiene que los resultados medidos indican que el rendimiento de los protocolos FHRP probados es casi equivalente, a continuación, se presenta la información. Expresada en segundos.[10]

Protocol	Hello inter-val [s]	Measuring type	Mean	Median	Variance	Standard deviation
HSRPv2	0.5	A	7.15	5.94	6.93	2.59
		B	21.08	21.01	0.47	0.7
	1	A	8.1	7.09	6.21	2.44
		B	21.3	21.51	1.34	1.17
	3	A	8.65	9.05	4.35	2.13
		B	21.32	21.5	1.27	1.15
VRRPv3	0.5	A	8.91	8.91	3.2	1.93
		B	20.57	20.82	0.77	0.86
	1	A	9.12	8.59	6.57	2.52
		B	20.96	20.97	1.79	1.31
	3	A	10.25	10.17	2.1	1.42
		B	20.92	20.54	0.91	0.93
GLBP	0.5	A	7.9	6.02	9.01	2.96
		B	21.1	20.8	0.85	0.91
	1	A	7.72	6.02	8.79	2.91
		B	21.17	21.01	0.9	0.94
	3	A	9.04	9.08	6.15	2.44
		B	21.41	20.54	2.47	1.56

Ilustración 4 Evaluación de retardos en Hello intervals.

Gateway redundancy protocols [10]

La siguiente ilustración representa los valores medidos del tiempo que tarda entre la activación de una nueva puerta de enlace predeterminada, estos tiempos se comparan con diferente valor de Hello Time para cada uno de los protocolos de redundancia VRRP, HSRP, GLBP.[10]

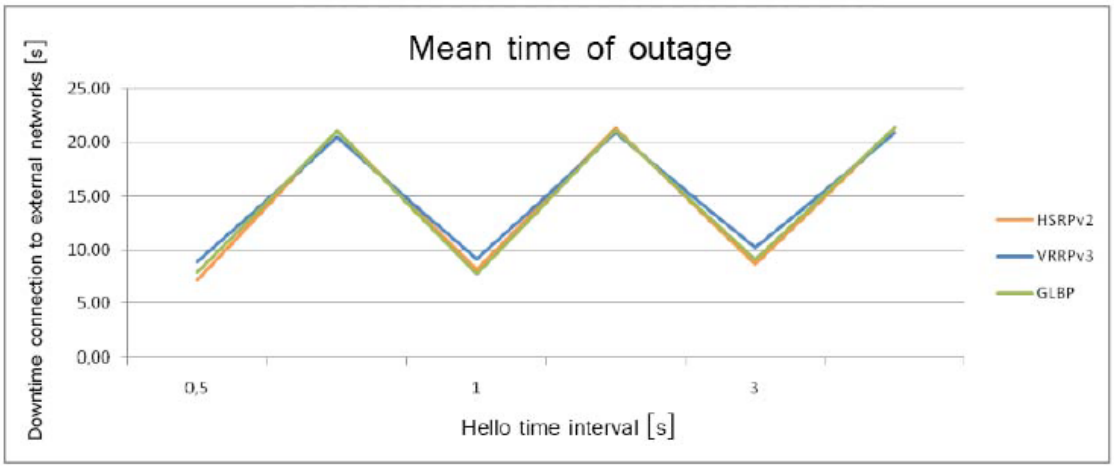

Ilustración 5 Grafica de evaluación de retardos en Hello intervals

Gateway redundancy protocols [10]

Observando el gráfico se logra interpretar que los Tiempos medidos de interrupción entre los protocolos VRRP, HSRP y GLBP es muy similar y no representa una diferencia significativa.[10]

Con respecto a la pérdida de paquetes en escenarios de convergencia en los cuales se realiza un cambio o caída de la red que implique que el tráfico de la red LAN deba saltar de un enrutador a otro se llega a la conclusión que la menor pérdida de paquetes se presenta cuando se implementa el protocolo GLBP debido a que el protocolo funciona en modo nativo como balanceador de carga a diferencia de los protocolos HSRP y VRRP que están a la espera de un cambio en la red para asumir el roll de router activo, lo cual genera pequeñas pérdida de paquetes mientras la red se estabiliza.[8]

El resultado del estudio y evaluación de parámetros en los protocolos de redundancia VRRP, HSRP y GLBP arroja como resultado, que los protocolos son muy similares en todos los campos que se evalúen y que dependiendo de la prueba que se realice uno u otro será mejor que los demás, sin representar una diferencia considerable, por tal motivo el parámetro que se tomará en cuenta para realizar la propuesta técnica a Telnova S.A.S es la propiedad intelectual y se escoge el protocolo abierto VRRP ya que el protocolo HSRP y GLBP son propiedad de la empresa Cisco. Esto con el fin de implementar la propuesta en equipos del fabricante al cual se tenga acceso.

4 TOPOLOGÍAS DE REDUNDANCIA EN EQUIPOS Y CONEXIONES DE ÚLTIMA MILLA

Se presentan posibles escenarios con los cuales una red puede disponer de redundancia a nivel de capa de red, los cuales son expuestos en este capítulo y una de estas topologías se tomarán como sugerencia para el desarrollo de la propuesta a la empresa Telnova S.A.S el diseño de red actual de la empresa puede ser consultado en el capitulo 5.1.

.A continuación, se aborda el concepto de última milla el cual está ampliamente difundido en la comunidad como el medio y tecnología por el cual un ISP brinda la conexión entre los CPE y los PE que conforman la red central del operador de telecomunicaciones.

La conexión de última milla puede ser implementada con diversas tecnologías enfocadas a brindar acceso al backbone IP de los proveedores de internet, en las cuales se encuentran xDSL., HFC, GPON, fibra óptica unifilar, fibra óptica bifilar, radio enlace, SDH, redes móviles 3g, redes móviles 4g, enlace satelital.[17]

4.1 DOS ÚLTIMAS MILLAS AL MISMO ISP CON UN SOLO CPE

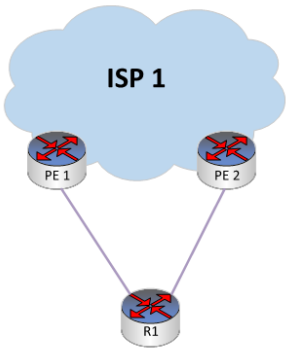

Ilustración 6 Dos últimas millas al mismo ISP con un solo CPE.
Configuring and Verifying the BGP Conditional Advertisement Feature [18]

Esta topología esta implementada por un router llamado CPE (customer-premises equipment), el cual cuenta con dos conexiones de última milla que conectan al CPE con el mismo backbone IP ya que las últimas millas pertenecen a un único ISP, esta topología brinda respaldo a la red del CPE pues si llegara a ocurrir un fallo en la conexión de última milla el tráfico conmutaría a la última milla backup.

Un posible inconveniente de esta topología es la ausencia de respaldo a nivel de quipos en el cliente, por tal motivo si ocurre una sobre carga que afecte la integridad del CPE o un daño a nivel físico en el equipo, por falta de mantenimiento o deterioro del mismo se perdería totalmente el tráfico de la red.

4.2 DOS ÚLTIMAS MILLAS AL MISMO ISP CON DOS CPE

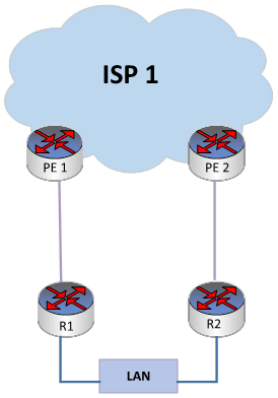

Ilustración 7 Dos últimas mil las al mismo ISP con dos CPE.
Highly Available Wide Area Network Design[19]

La topología de dos últimas millas y dos CPE soluciona el problema presentado en el punto anterior el cual menciona los problemas de tener un solo CPE, con esta topología se brinda a la red con un respaldo físico con el cual se disminuye la posibilidad de una pérdida de conexión con el backbone debido a la redundancia en CPE y en última milla.

Al implementar este diseño de red no se está exento de fallas en servicio, pues las dos últimas millas y los dos CPE están conectados a un mismo backbone IP, por lo tanto, si llegase a ocurrir una falla masiva en el mismo se perdería el servicio. Una falla de este tipo no se podría calcular o predecir, pero existe la posibilidad de que ocurra.

4.3 DOS ISP DIFERENTES CON UN SOLO CPE

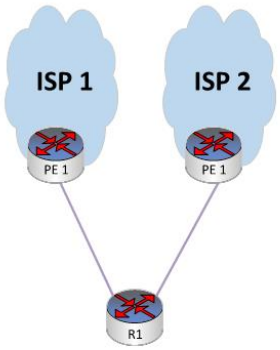

Ilustración 8 Dos ISP con un solo CPE.

Esta topología brinda solución a la problemática mencionada en el punto 3.2, pues en esta topología la red del CPE está conectado a dos ISP cada uno con un backbone IP diferente, por lo tanto, se tiene respaldo del servicio si llegase a ocurrir alguna falla en el backbone IP de la última milla principal.

Pero con este diseño la red del CPE estaría expuesta al problema de no contar con respaldo de CPE y a las posibles fallas que podría tener el mismo.

4.4 DOS ISP DIFERENTES CON DOS CPE

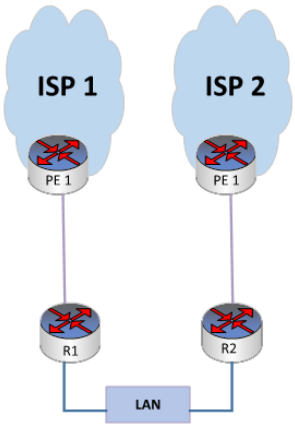

Ilustración 9 Dos ISP con dos CPE.

Esta topología brinda solución a los problemas abordados en los ítems anteriores pues se cuenta con dos CPE con los cuales se obtiene respaldo a nivel de equipos en la red y las conexiones de última milla de cada uno de los CPE se dirigen a dos ISP por lo tanto se cuenta con respaldo a nivel de backbone IP.

4.5 DEDUCCIÓN DEL CAPÍTULO TOPOLOGÍAS DE REDUNDANCIA

la topología de dos ISP diferentes con dos CPE brinda una menor posibilidad de fallas a nivel de servicio pues se cuenta con respaldo de infraestructura de equipos y las posibilidades de presentar fallas masivas en el núcleo de la red disminuye debido a que se cuenta a dos proveedores de internet independientes.

5 DESARROLLO

Con el objetivo de dar respuesta a la problemática presentada, la cual corresponde a realizar una ampliación del ancho de banda del canal de internet de la empresa Telnova S.A.S. en el menor tiempo posible se plantea un diseño basado en una topología de red redundante que aumente la capacidad del ancho de banda por medio de balanceo de carga utilizado el protocoló VRRP.

5.1 DIAGRAMA DE RED ACTUAL DE TELNOVA S.A.S.

La red está conformada por un único enlace a internet perteneciente a un proveedor local que para términos del diagrama lo nombramos como ISP 1, se ilustra la red LAN como un único bloque que conforma toda la infraestructura correspondiente a la red interna de la empresa.

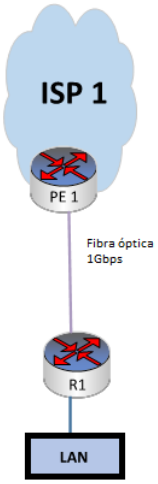

Ilustración 10 Diagrama de red actual de Telnova S.A.S.

La topología actual de la red tiene deficiencias a nivel de respaldo del servicio, puesto que una falla presentada en cualquiera de los puntos de la red, dejaría a la empresa sin conexión

a internet. Actualmente la empresa está expuesta a una indisponibilidad de tiempos elevados si se llegara a presentar algún corte sobre la única fibra óptica con la que cuenta la topología, sin olvidar los riesgos que se presentan a depender de un único equipo router, el cual está expuesto a presentar problemas físicos por condiciones medioambientales o fluctuaciones de flujo eléctrico.

5.2 PROPUESTA DE TOPOLOGÍA DE RED REDUNDANTE PARA TELNOVA S.A.S.

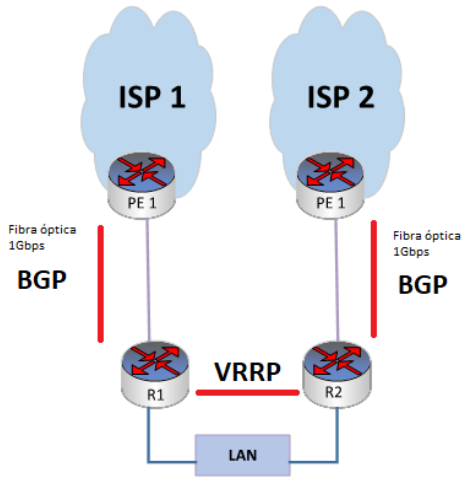

Ilustración 11 Propuesta de red para Telnova S.A.S.

Basado en el estudio de las tecnologías de balanceo de carga para tráfico IP a nivel de redes WAN desarrollado en el capítulo 3, se decide implementar una solución de balanceo de tráfico utilizando el protocolo VRRP ya que es un protocolo abierto para la implementación en cualquier fabricante de equipos de telecomunicaciones.

La empresa Telnova S.A.S. requiere ampliar su capacidad de ancho de banda en un corto plazo por tal motivo es necesario que adquiera un nuevo canal de internet. Para este caso se propone que sea implementada una nueva fibra óptica que provea la conexión hacia un segundo operador de telecomunicaciones que en el diagrama es nombrado como ISP 2. Para mitigar los riesgos de utilizar un único dispositivo de enrutamiento se sugiere que se

agregue un CPE más a la topología, para que de esta manera la topología cuente con dos conexiones a internet cada una de ellas conectada al backbone de un operador de telecomunicaciones diferente y en el extremo de la empresa se utilicen dos equipos CPE. Para garantizar una alta disponibilidad del servicio y adicionalmente lograr cumplir el objetivo propuesto, balanceando el tráfico por estos dos canales de internet y lograr un ancho de banda total de 2Gbps en el caso de contratar 1Gps en cada uno de los canales.

5.3 DISEÑO DE RED PARA IMPLEMENTACIÓN DE BALANCEO DE CARGA

A continuación, se presenta la ingeniería de detalle para la solución de balanceo de carga con protocolo VRRP en la cual se resalta el direccionamiento utilizado en las redes WAN y la red LAN la cual corresponde a un segmento de direccionamiento IPv4 público.

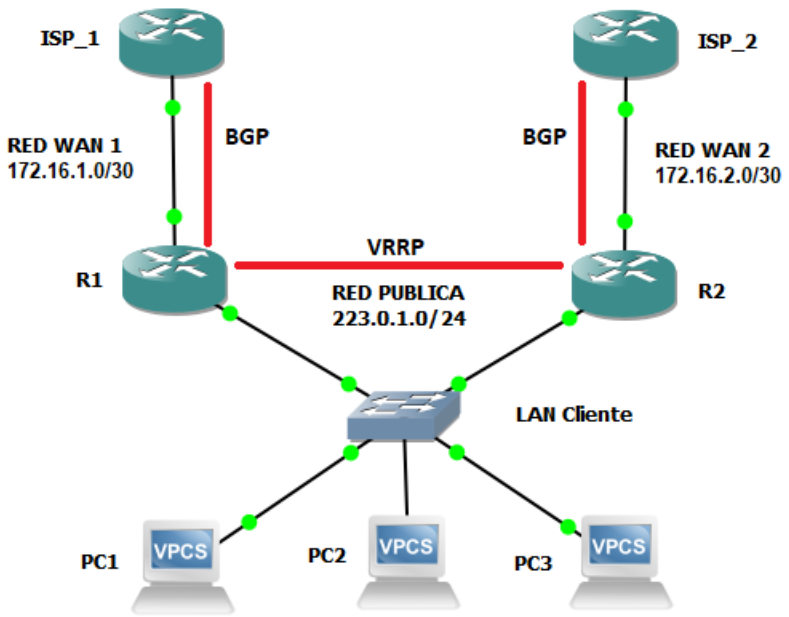

Ilustración 12 Diagrama de direccionamiento para la propuesta de red.

En el esquema se resaltan los protocolos que son implementados para el diseño de red. Para el enrutamiento se propone utilizar BGP el cual es el protocolo de enrutamiento dinámico utilizado para compartir las tablas de enrutamiento en internet. De tal manera que anuncie la red pública 223.0.1.0/24 hacia los demás sistemas autónomos de internet.

La función de balancear la carga hacia los dos routers implementados en Telnova se delega al protocolo VRRP que ha sido escogido por su característica de ser un protocolo abierto estandarizado por el IETF (Internet Engineering Task Force) bajo el RFC (Request for Comments) 2338, por tal motivo puede ser utilizado en cualquier fabricante de equipos de telecomunicaciones. El protocolo VRRP fue diseñado principalmente para brindar solución a la integración de varios routers de los cuales uno tomará el papel de Gateway en la red, dependiendo de que router tenga el valor de prioridad más alto. Aplicando la configuración adecuada se puede implementar varios Gateway y de esta manera balancear la carga hacia los diferentes enlaces WAN.

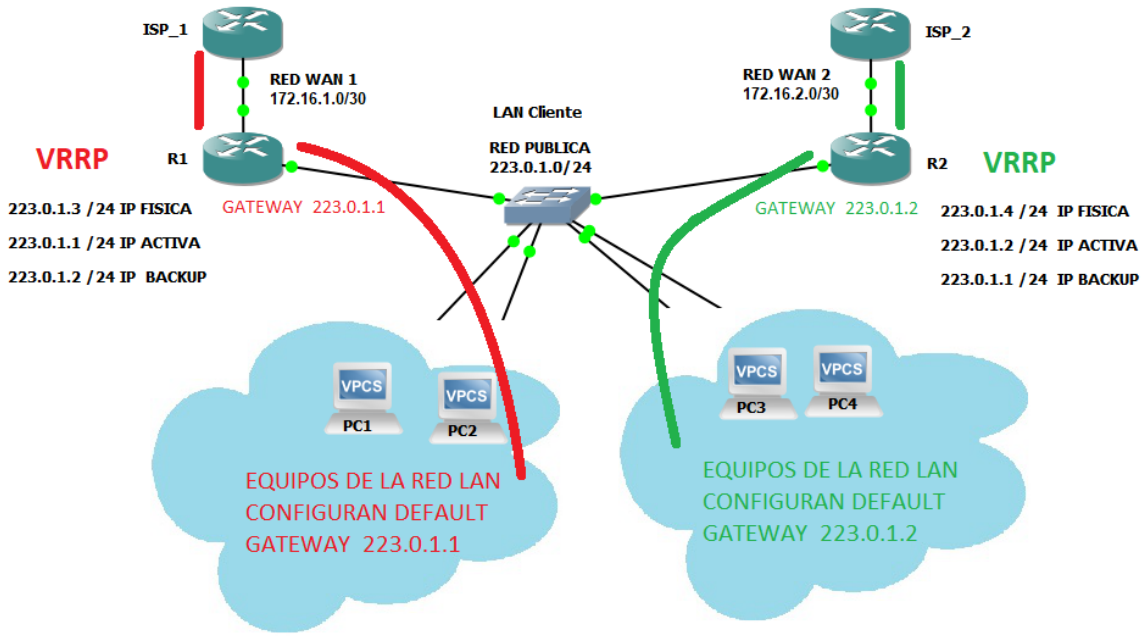

Ilustración 13 Diagrama de conexiones hacia los Gateway de red.

Como se muestra en la imagen anterior el balanceo se produce al dividir el segmento LAN en dos grupos, de tal manera que los dispositivos pertenecientes al primer grupo tienen configurado como Default Gateway una de las direcciones virtuales activas, de esta manera todo el tráfico que se desee enviar a internet tomara la ruta correspondiente a su Default Gateway o también llamada puesta de enlace predeterminada.

5.4 SCRIPT DE CONFIGURACIÓN EN FABRICANTE CISCO PARA IMPLEMENTACIÓN DE BALANCEO DE CARGA CON PROTOCOLO VRRP

Basado en el diseño de red presentado anteriormente, se realiza el script de configuración, teniendo en cuenta el esquema de direccionamiento y la topología de RED, en el script se incluyen todos los comandos requeridos para llevar a cabo la configuración sobre equipos físicos de la marca Cisco o equipos virtuales simulados por GNS3.

Se presenta la Configuración propuesta para el R1, a modo de cementerio se explica brevemente la función de las principales líneas de código dentro del script.

```
hostname R1
!
track 1 ip route 8.8.8.0 255.255.255.0 reachability !! Realiza seguimiento constante a la existencia de la ruta 8.8.8.0 sobre la tabla de enrutamiento, si no existe la ruta se marca como donw.
!
interface GigabitEthernet0/0
 description Vlan_Usuarios
 ip address 223.0.1.3 255.255.255.0 !! Configura la IP física sobre la interfaz.
speed 1000  !! Parámetro de velocidad de negociación de la interfaz.
 full-duplex
 vrrp 1 ip 223.0.1.1  !! Establece la dirección IP virtual del grupo 1.
 vrrp 1 timers advertise 3 !! Define 3 segundos como tiempo de espera entre cada envío de actualizaciones de estado.
!
 vrrp 1 priority 120  !! Marca la prioridad sobre el grupo 1 en 120.
 vrrp 1 track 1 decrement 30 !! Si el estado del track 1 es donw disminuye en 30 la prioridad configurada al grupo 1.
!
 vrrp 2 ip 223.0.1.2  !!  Establece la dirección IP virtual del grupo 2.
 vrrp 2 timers advertise 3 !! Define 3 segundos como tiempo de espera entre cada envío de actualizaciones de estado.
!
 vrrp 2 track 1 decrement 30 !! Si el estado del track 1 es donw disminuye en 30 la prioridad configurada al grupo 2.
!
interface GigabitEthernet1/0
 description WAN_cl01
 ip address 172.16.1.2 255.255.255.252 !! Configura la IP física sobre la interfaz.
 speed 1000
 full-duplex
!
router bgp 64271 !! Define el sistema autónomo del protocolo BGP.
network 223.0.1.0 !! Red que será anunciada por el protocolo BGP.
 neighbor 172.16.1.1 remote-as 14081 !! Se indica contra que IP se establece la vecindad BGP y el número de sistema autónomo al cual pertenece.
!
 neighbor 172.16.1.1 description WAN_cl01
 neighbor 172.16.1.1 timers 10 30 !! Se establece el tiempo de intervalo entre notificaciones de protocolos.
 no auto-summary
!
```

Cuadro de texto 2 Script de configuración para router R1.

El siguiente cuadro de texto presenta la configuración que se debe aplicar sobre el router 2 de la topología diseñada.

```
hostname R2
!
track 1 ip route 8.8.8.0 255.255.255.0 reachability
!
interface GigabitEthernet0/0
 description Vlan_Usuarios
 ip address 223.0.1.4 255.255.255.0
 speed 100
 full-duplex
 vrrp 1 ip 223.0.1.1
 vrrp 1 timers advertise 3
 vrrp 1 track 1 decrement 30
 vrrp 2 ip 223.0.1.2
 vrrp 2 timers advertise 3
 vrrp 2 priority 120
 vrrp 2 track 1 decrement 30
!
interface GigabitEthernet1/0
 description WAN_cl02
 ip address 172.16.2.2 255.255.255.252
 speed 100
 full-duplex
!
router bgp 64271
network 223.0.1.0
 neighbor 172.16.2.1 remote-as 14085
 neighbor 172.16.2.1 description WAN_cl02
 neighbor 172.16.2.1 timers 10 30
 no auto-summary
!
```

Cuadro de texto 3 Script de configuración para router R2.

Con la topología de Red escogida y el diseño realizado en base a ella, se ha elaborado y explicado la propuesta de configuración mostrada en los cuadros de texto anteriores. Teniendo esto claro, se procede a pasar a un entorno de pruebas controlado en el que se pueda evaluar el resultado de la propuesta brindada a la empresa Telnova S.A.S. por medio de una simulación del funcionamiento en el simulador GNS3, y un análisis de las trazas IP desarrollado en el siguiente capítulo.

6 SIMULACIÓN DE BALANCEO DE CARGA CON PROTOCOLO VRRP EN SOFTWARE GNS3

Con el objetivo de poner a prueba el script de configuración para equipos Cisco se elabora una simulación en la cual se logre evaluar el comportamiento de la solución propuesta, estas pruebas se realizan sobre la plataforma GNS3 en la cual se plantea un escenario que se acerque lo más posible al comportamiento del tráfico de la red de internet.

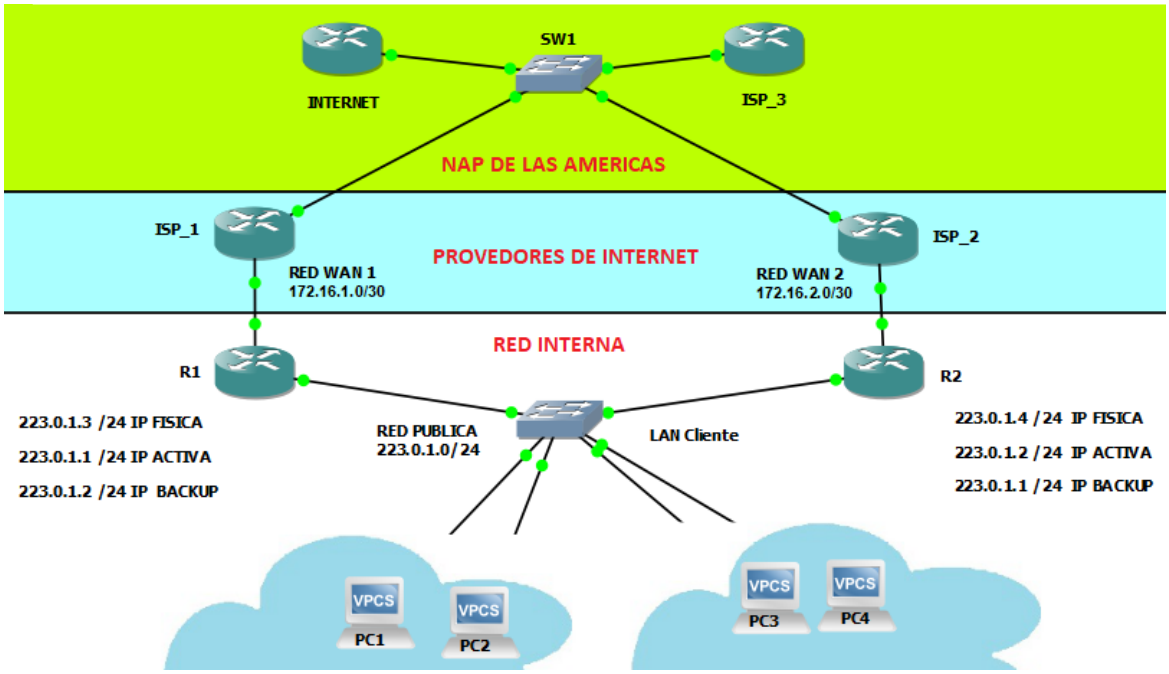

Ilustración 14 Capas del entorno de simulación.

Se plantea un entorno de pruebas en el cual su objetivo es identificar el comportamiento del tráfico originado desde equipos de la red LAN y con destino a direcciones IP públicas que de igual manera son simuladas en el escenario del laboratorio.

El entorno de simulación está compuesto de 3 capas lógicas, en la primera capa que corresponde a la red interna se encuentran los equipos alojados físicamente en la empresa y que brindan el acceso a la red. La segunda capa correspondiente a proveedores de internet pretende representar toda la infraestructura de un operador de telecomunicaciones desde su capa de acceso hasta su backbone y los equipos de borde hacia internet. Y la última capa nombrada como NAP (Network Access Point) representa el punto de interconexión de los diferentes ISP de nivel1 llamados Tier 1.

El resultado del comando show vrrp brief sobre el router R1 evidencia que la conformación de los grupos VRRP se realizó de manera correcta, para este caso se establece el router R1 como Master en el grupo 1, y asume la responsabilidad de recibir los paquetes enviados desde la red LAN con destino la dirección IP virtual 223.0.1.1 y dirección MAC virtual 0000.5e00.0101.

```
R1#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Fa0/0              1   120 9531      Y  Master  223.0.1.3       223.0.1.1
Fa0/0              2   100 9609      Y  Backup  223.0.1.4       223.0.1.2
R1#

R1#show vrrp
FastEthernet0/0 - Group 1
  State is Master
  Virtual IP address is 223.0.1.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3.000 sec
  Preemption enabled
  Priority is 120
    Track object 1 state Up decrement 30
  Master Router is 223.0.1.3 (local), priority is 120
  Master Advertisement interval is 3.000 sec
  Master Down interval is 9.531 sec

FastEthernet0/0 - Group 2
  State is Backup
  Virtual IP address is 223.0.1.2
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 3.000 sec
  Preemption enabled
  Priority is 100
    Track object 1 state Up decrement 30
  Master Router is 223.0.1.4, priority is 120
  Master Advertisement interval is 3.000 sec
  Master Down interval is 9.609 sec (expires in 6.673 sec)

R1#
```

Cuadro de texto 4 Resultado del protocolo VRRP en R1.

Igualmente se logra evidenciar que la configuración propuesta a nivel de protocolo VRRP se estableció de manera correcta en el router R2 y que este mismo asume el roll de Master en el grupo 2. Debido a la condición de tener el valor de priority en 120 siendo mayor que el router R1 para el router dos se asigna la dirección IP virtual 223.0.1.2 y dirección MAC virtual 0000.5e00.0102.

```
R2#show vrrp brief
Interface          Grp Pri Time  Own Pre State   Master addr     Group addr
Fa0/0              1   100 9609      Y  Backup  223.0.1.3       223.0.1.1
Fa0/0              2   120 9531      Y  Master  223.0.1.4       223.0.1.2
R2#
R2#show vrrp
FastEthernet0/0 - Group 1
  State is Backup
  Virtual IP address is 223.0.1.1
  Virtual MAC address is 0000.5e00.0101
  Advertisement interval is 3.000 sec
  Preemption enabled
  Priority is 100
    Track object 1 state Up decrement 30
  Master Router is 223.0.1.3, priority is 120
  Master Advertisement interval is 3.000 sec
  Master Down interval is 9.609 sec (expires in 8.225 sec)

FastEthernet0/0 - Group 2
  State is Master
  Virtual IP address is 223.0.1.2
  Virtual MAC address is 0000.5e00.0102
  Advertisement interval is 3.000 sec
  Preemption enabled
  Priority is 120
    Track object 1 state Up decrement 30
  Master Router is 223.0.1.4 (local), priority is 120
  Master Advertisement interval is 3.000 sec
  Master Down interval is 9.531 sec

R2#
```

Cuadro de texto 5 Resultado del protocolo VRRP en R2.

Como se verificó en los cuadros de texto anteriores la configuración para el protocolo VRRP funcionó de manera correcta, a continuación, se presenta la verificación del funcionamiento del protocolo BGP en el cual se establece el neighbor contra el ISP y se realiza de manera satisfactoria el proceso de compartir las tablas de enrutamiento.

```
¡ SE ESTABLECE EL PROTOCLO BGP EN  R1

R1#show ip bgp all summary
For address family: IPv4 Unicast
BGP router identifier 223.0.1.3, local AS number 64271
BGP table version is 23, main routing table version 23
21 network entries using 2520 bytes of memory
21 path entries using 1092 bytes of memory
4/3 BGP path/bestpath attribute entries using 496 bytes of memory
2 BGP AS-PATH entries using 48 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
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 4188 total bytes of memory
BGP activity 21/0 prefixes, 21/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.1.1      4 14081    5858    5235       23    0    0 14:31:44       20
R1#

¡ SE ESTABLECE EL PROTOCLO BGP EN  R2

R2#show ip bgp all summary
For address family: IPv4 Unicast
BGP router identifier 223.0.1.4, local AS number 64271
BGP table version is 22, main routing table version 22
21 network entries using 2520 bytes of memory
21 path entries using 1092 bytes of memory
5/4 BGP path/bestpath attribute entries using 620 bytes of memory
3 BGP AS-PATH entries using 72 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
Bitfield cache entries: current 1 (at peak 1) using 32 bytes of memory
BGP using 4336 total bytes of memory
BGP activity 21/0 prefixes, 21/0 paths, scan interval 60 secs

Neighbor        V    AS MsgRcvd MsgSent   TblVer  InQ OutQ Up/Down  State/PfxRcd
172.16.2.1      4 14085    6208    4758       22    0    0 13:12:15       20
R2#
```

Cuadro de texto 6 Establecimiento del protocolo BGP en R1 y R2.

6.1 VERIFICACIÓN DE LAS RUTAS DE TRAFICO

Con el fin de demostrar que el resultado de la propuesta fue exitoso. Se realizan pruebas de trazas sobre rutas IP para identificar el camino que están tomando los paquetes de los equipos pertenecientes a los grupos de balanceo dentro de la red LAN y de esta manera tener las evidencias de que el tráfico IP está cursando por los dos enlaces de internet contratados.

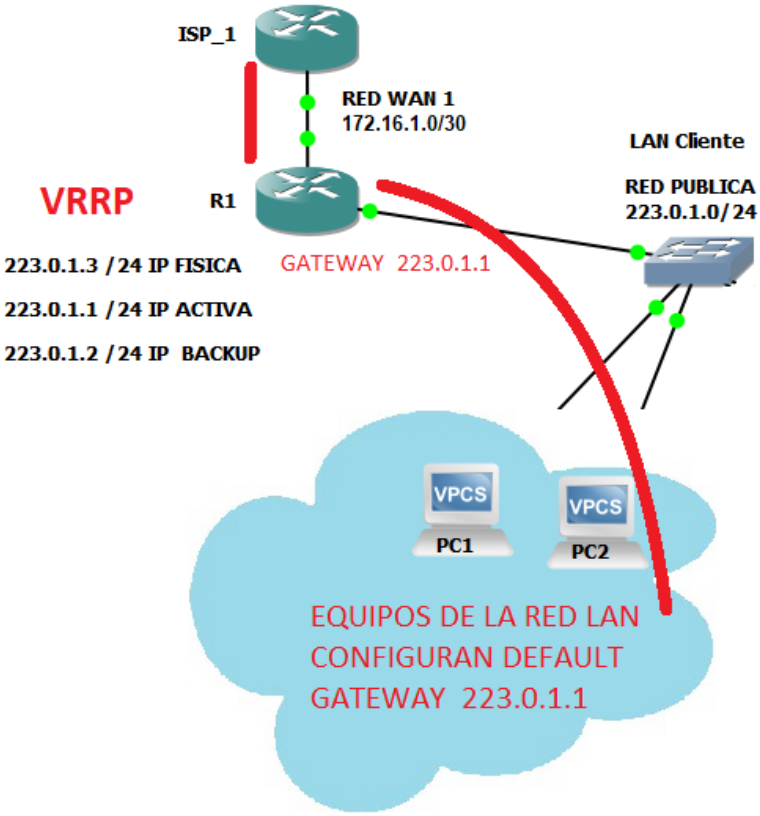

Ilustración 15 Diseño de tráfico para el primer grupo LAN.

En el siguiente cuadro de texto se presenta el resultado del comando show el cual despliega la configuración realizada sobre la interfaz LAN del PC1, mostrando la IP configurada, el

Gateway y la dirección MAC. Se ejecuta el comando ping 8.8.8.8 para verificar conectividad contra el servidor de internet simulado en GNS3 y por último se despliega el comando tracer 8.8.8.8 para hacer el seguimiento a los saltos que realiza el tráfico.

```
PC1> show

NAME   IP/MASK             GATEWAY         MAC               LPORT  RHOST:PORT
PC1    223.0.1.6/24        223.0.1.1       00:50:79:66:68:01  10015  192.168.147.128:10014
       fe80::250:79ff:fe66:6801/64

PC1>

PC1> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=46.934 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=40.524 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=253 time=36.554 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=253 time=47.067 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=253 time=48.057 ms

PC1>
PC1> tracer 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   223.0.1.3   10.508 ms  9.097 ms  8.825 ms
 2   172.16.1.1   30.039 ms  30.530 ms  30.019 ms
 3   *206.223.124.103   51.999 ms (ICMP type:3, code:3, Destination port unreachable)  *

PC1>
```

Cuadro de texto 7 Conectividad PC1 de la red LAN hacía internet.

Realizando el análisis de la información desplegada se observa que el comportamiento del tráfico es lo esperado ya que salta a la IP física del router R1 223.0.1.3 y continúa su ruta por medio del ISP1 hasta llegar a su destino en Internet.

En la siguiente imagen se presenta la ruta del tráfico para los equipos pertenecientes al grupo dos de la red LAN los cuales encontrarán su salida a internet por medio del router R2 y el ISP2 será el encargado de garantizar la navegación de la red.

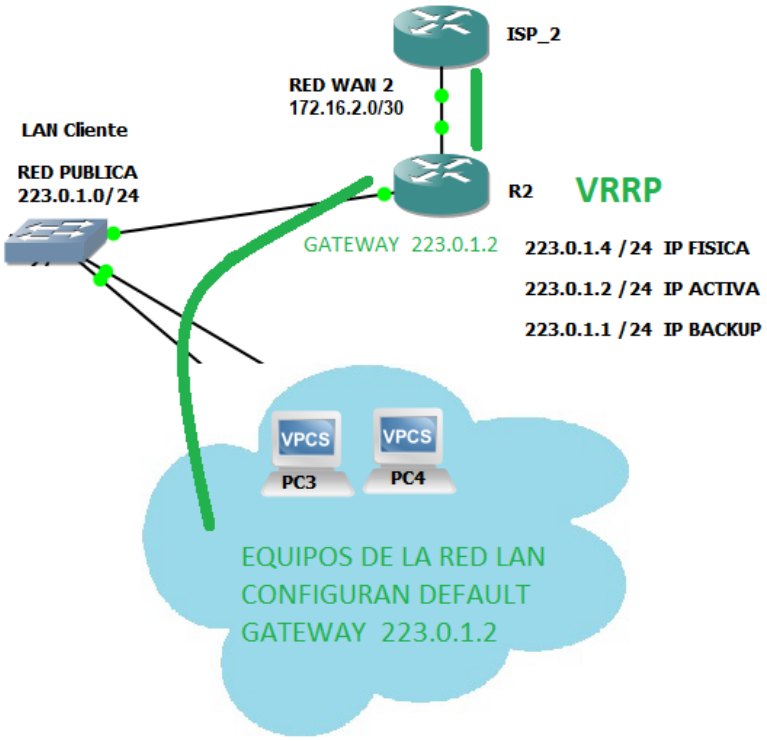

Ilustración 16 Diseño de tráfico para el segundo grupo LAN.

En el siguiente cuadro de texto se presenta el resultado de los principales comandos utilizados para el análisis de la información relevante en términos de conectividad en el equipo PC3 perteneciente al segundo grupo de la red LAN.

```
PC3> show

NAME   IP/MASK            GATEWAY          MAC               LPORT  RHOST:PORT
PC3    0.0.0.0/0          0.0.0.0          00:50:79:66:68:02  10018  192.168.147.128:10019
       fe80::250:79ff:fe66:6802/64

PC3>

PC3> ping 8.8.8.8

84 bytes from 8.8.8.8 icmp_seq=1 ttl=253 time=47.432 ms
84 bytes from 8.8.8.8 icmp_seq=2 ttl=253 time=49.025 ms
84 bytes from 8.8.8.8 icmp_seq=3 ttl=253 time=55.048 ms
84 bytes from 8.8.8.8 icmp_seq=4 ttl=253 time=47.566 ms
84 bytes from 8.8.8.8 icmp_seq=5 ttl=253 time=45.575 ms

PC3>
PC3> tracer 8.8.8.8
trace to 8.8.8.8, 8 hops max, press Ctrl+C to stop
 1   223.0.1.4   5.143 ms  9.559 ms  10.983 ms
 2   172.16.2.1   19.560 ms  30.519 ms  22.044 ms
 3   *206.223.124.103   31.618 ms (ICMP type:3, code:3, Destination port unreachable)  *

PC3>
```

Cuadro de texto 8 Conectividad PC3 de la red LAN hacía internet.

Realizando el análisis de la información desplegada se observa que el comportamiento del tráfico es lo esperado ya que salta a la IP física del router R2 223.0.1.4 y continua su ruta por medio del ISP2 hasta llegar a su destino en Internet.

6.2 ANÁLISIS DE AMPLIACIÓN DE ANCHO DE BANDA POR MEDIO DEL MÉTODO DE BALANCEO DE CARGA

El principal objetivo de implantar un método de balanceo de carga es ampliar la capacidad total de la navegación a internet con la que cuenta actualmente la empresa Telnova S.A.S., pasando de un único canal de 1Gbps a implementar dos canales de 1 Gbps para tener un total de 2Gbps en la red.

Para el escenario de pruebas se envió tráfico desde los equipos que conforman los dos grupos LAN y sobre las interfaces de los ISP se realizó captura del número de bps que cursa la interfaz en el momento exacto de la prueba lo cual arrojó el siguiente resultado.

```
ISP_1#sh policy-map interface FastEthernet1/0
 FastEthernet1/0

  Service-policy input: VELOCIDAD_1

    Class-map: class-default (match-any)
      33239 packets, 25746907 bytes
      5 minute offered rate 172000 bps, drop rate 0 bps
      Match: any
      police:
          cir 1024000 bps, bc 128000 bytes, be 128000 bytes
        conformed 33239 packets, 25746907 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 145000 bps, exceed 0 bps, violate 0 bps  !! Tráfico de upload en canal de ISP_1.

  Service-policy output: VELOCIDAD_1

    Class-map: class-default (match-any)
      35592 packets, 27307431 bytes
      5 minute offered rate 213000 bps, drop rate 0 bps
      Match: any
      police:
          cir 1024000 bps, bc 128000 bytes, be 128000 bytes
        conformed 35188 packets, 27267256 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop ,
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 274000 bps, exceed 0 bps, violate 0 bps !! Tráfico de download en canal de
ISP_1.


ISP_1#
```

Cuadro de texto 9 Análisis tráfico sobre ISP_1.

Como se muestra en el cuadro de texto anterior sobre el ISP_1 se detecta tráfico por 145000 bps correspondiente al tráfico de upload, al mismo tiempo se visualiza tráfico por 274000

bps en sentido de download valor que se aproxima al doble de la cantidad del tráfico de upload, este resultado refleja un comportamiento no esperado.

Se procede a realizar la captura de flujo de tráfico en bps en tiempo real sobre el ISP_2

```
ISP_2#sh policy-map interface  FastEthernet1/0
 FastEthernet1/0

  Service-policy input: VELOCIDAD_1

    Class-map: class-default (match-any)
      5419 packets, 3841985 bytes
      5 minute offered rate 96000 bps, drop rate 0 bps
      Match: any
      police:
          cir 1024000 bps, bc 128000 bytes, be 128000 bytes
        conformed 5419 packets, 3841985 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 162000 bps, exceed 0 bps, violate 0 bps !! Tráfico de upload en canal de ISP_2.

  Service-policy output: VELOCIDAD_1

    Class-map: class-default (match-any)
      1021 packets, 83297 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
      police:
          cir 1024000 bps, bc 128000 bytes, be 128000 bytes
        conformed 618 packets, 42021 bytes; actions:
          transmit
        exceeded 0 packets, 0 bytes; actions:
          drop
        violated 0 packets, 0 bytes; actions:
          drop
        conformed 0 bps, exceed 0 bps, violate 0 bps !! Tráfico de download en canal de ISP_2.
ISP_2#
```

Cuadro de texto 10 Análisis de tráfico sobre ISP_2.

Con la información suministrada se logra apreciar que la red LAN genera 162000 bps en sentido de upload, y se evidencia de manera irregular que no transita tráfico en sentido de download,

Analizando la información obtenida en las interfaces que interconectan los router R1 y R2 con los ISP_1 he ISP_2 respectivamente, se logra evidenciar que se presenta tráfico asimétrico, el cual se explica de manera gráfica en la siguiente imagen para facilitar el entendimiento.

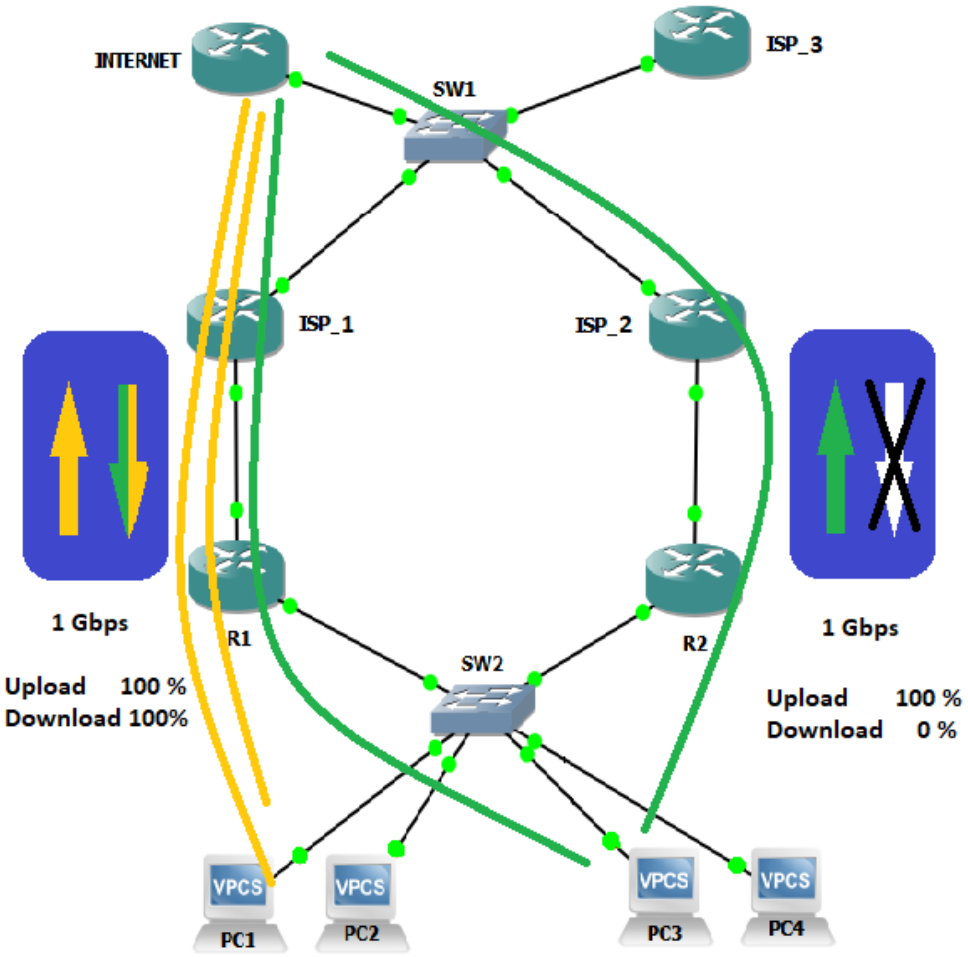

Ilustración 17 Tráfico asimétrico sobre los canales de internet.

Gracias al análisis de las capturas de tráfico tomadas sobre los puertos de los ISP, se logra interpretar que el tráfico que se envía por medio del ISP_2 solo circula en sentido de Upload

y que el tráfico que sube por este enlace tomo el camino de retorno a través del ISP_1, esto se refleja gráficamente con las líneas verdes en la ilustración anterior. Se resalta el hecho de que el ISP_2 no presenta tráfico en sentido de Download, como se mencionó anteriormente dicho tráfico retorna por el ISP_1 esto tiene la implicación de que el canal de Download en el ISP_1 comparte el ancho de banda con el tráfico que retorna a la red LAN, está es la razón por la cual en el diagrama la flecha descendiente está divida por dos colores verde y amarillo para simbolizar tráfico compartido de los dos enlaces.

Resumiendo, la información presentada, se logra concluir que la ampliación de ancho de banda por medio de balanceo de carga con el método del protocolo VRRP es posible pero el tráfico se desempeña de manera asimétrica, lo cual arroja como sumatoria de ancho de banda 2 Gbps en sentido de Upload y 1 Gbps en sentido de Download.

6.3 ANÁLISIS TÉCNICO DE ENRUTAMIENTO

Con el fin de entender el motivo por el cual se presenta tráfico asimétrico en la red se realiza análisis de las tablas de enrutamiento en la simulación elaborada, se obtiene como resultado 2 rutas aprendidas en el router de INTERNET, las dos rutas le indican al router de internet que tiene dos caminos posibles para alcanzar la red de la empresa 223.0.1.0/24, debido al manejo de tablas de enrutamiento que realiza el protocolo BGP se establece únicamente una sola ruta sobre la tabla de enrutamiento global. Esto implica que solamente existirá una ruta activa de retorno del tráfico y explica la razón por la cual el tráfico de download solo circula por el enlace perteneciente al ISP_2.

```
INTERNET#show ip route 223.0.1.0  !! Se consulta la ruta activa sobre la tabla de enrutamiento global.
Routing entry for 223.0.1.0/24
  Known via "bgp 14083", distance 20, metric 0
  Tag 14081, type external
  Last update from 206.223.124.101 05:14:46 ago
  Routing Descriptor Blocks:
  * 206.223.124.101, from 206.223.124.101, 05:14:46 ago  !! Ruta activa.
      Route metric is 0, traffic share count is 1
      AS Hops 2
      Route tag 14081

INTERNET#

INTERNET#show  bgp 223.0.1.0 !! Se consulta la ruta sobre la tabla de enrutamiento del protocolo BGP.
BGP routing table entry for 223.0.1.0/24, version 23
Paths: (2 available, best #2, table Default-IP-Routing-Table)
  Advertised to update-groups:
        1
  14085 64271
    206.223.124.104 from 206.223.124.104 (206.223.124.104) !! Ruta hacia la red pública a través del ISP_2.
      Origin IGP, localpref 100, valid, external
  14081 64271
    206.223.124.101 from 206.223.124.101 (91.0.0.1) !! Ruta hacia la red pública a través del ISP_1.
      Origin IGP, localpref 100, valid, external, best !! Marca la ruta como la mejor, y se establece en la tabla de enrutamiento global.
INTERNET#
INTERNET#

INTERNET#ping 223.0.1.6 source 8.8.8.8  !! Prueba de conectividad IP.

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 223.0.1.6, timeout is 2 seconds:
Packet sent with a source address of 8.8.8.8
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 84/106/140 ms
INTERNET#
INTERNET#tracer 223.0.1.6 source 8.8.8.8  !! Traza IP para identificar los saltos que realiza la ruta preferida por el router de INTERNET.

Type escape sequence to abort.
Tracing the route to 223.0.1.6

  1 206.223.124.101 44 msec 20 msec 16 msec
  2 172.16.1.2 [AS 14081] 80 msec 112 msec 92 msec
  3 223.0.1.6 [AS 64271] 124 msec 88 msec 80 msec
INTERNET#
```

Cuadro de texto 11 Análisis técnico de enrutamiento.

En el cuadro de texto se evidencia que la ruta activa hacia la dirección IP 223.0.1.0/24 toma el camino del ISP_1 con la dirección IP 206.223.124.101, además gracias al comando show bgp 223.0.1.0 se evidencia la existencia de dos rutas para enviar el tráfico al destino que es la empresa Telnova, pero únicamente se marca un camino como el mejor, el cual se establece en la tabla de enrutamiento global. Para evidenciar el comportamiento del tráfico IP se realizan trazas a los host dentro de la red LAN, tal cual como se evidencia en el cuadro de texto anterior.

7 CONCLUSIONES

- Por medio de la revisión teórica de artículos científicos referentes a los protocolos de redundancia VRRP, HSRP y GLBP se logra concluir, que los protocolos son muy similares en todos los campos que se evalúen y que dependiendo de la prueba que se realice uno u otro será mejor que los demás, sin representar una diferencia considerable.
- Las topologías de redundancia se pueden diseñar de la manera que se desee siempre y cuando se ajuste a las necesidades que se requieran solucionar en base al presupuesto.
- El diseño de un script de configuración para balanceo de carga en protocolo VRRP es sencillo de realizar y no contempla complejidad para ser adoptado en cualquier red que desee balancear el tráfico.
- Al intentar aumentar el ancho de banda con la técnica de balanceo de carga propuesta en el documento utilizando el protocolo VRRP, se obtendrá como resultado tráfico asimétrico en todos los escenarios de pruebas debido a que solo se tendrá una ruta para el retorno del tráfico a la red de la empresa así como se demostró en el análisis técnico de enrutamiento.

REFERENCIAS

[1] «poblacion DANE EdadesSexoMunicipiosDeptos.pdf». Accedido: may 30, 2021. [En línea]. Disponible en: https://www.pazdeariporo-casanare.gov.co/Transparencia/Indicadores%20Municipales/poblacion%20DANE%20EdadesSexoMunicipiosDeptos.pdf

[2] «rfc3768». https://datatracker.ietf.org/doc/html/rfc3768 (accedido jun. 16, 2021).

[3] «https://tools.ietf.org/rfc/rfc5798.txt». Accedido: jun. 16, 2021. [En línea]. Disponible en: https://tools.ietf.org/rfc/rfc5798.txt

[4] «Understanding VRRP | High Availability User Guide | Juniper Networks TechLibrary». https://www.juniper.net/documentation/us/en/software/junos/high-availability/topics/concept/vrrp-overview-ha.html (accedido jun. 16, 2021).

[5] «First Hop Redundancy Protocols Configuration Guide, Cisco IOS XE Release 3S - Configuring HSRP [Cisco IOS XE 3S] - Cisco». https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipapp_fhrp/configuration/xe-3s/fhp-xe-3s-book/fhp-hsrp.html (accedido jun. 17, 2021).

[6] «rfc2281». https://datatracker.ietf.org/doc/html/rfc2281 (accedido jun. 17, 2021).

[7] A. Akmaluddin, A. Arini, y S. U. Masruroh, «Evalusi Kinerja Hot Standby Router Protocol (HSRP) dan Gateway Load Balancing Protocol (GLBP) untuk Layanan Video Streaming», *Cyber Secur. Dan Forensik Digit.*, vol. 2, n.º 1, Art. n.º 1, may 2019, doi: 10.14421/csecurity.2019.2.1.1445.

[8] M. Mansour, «Performance Evaluation of First Hop Redundancy Protocols», *Procedia Comput. Sci.*, vol. 177, pp. 330-337, 2020, doi: 10.1016/j.procs.2020.10.044.

[9] «Performance Evaluation of First HOP Redundancy Protocols (HSRP, VRRP & GLBP)». Accedido: jun. 17, 2021. [En línea]. Disponible en: https://scholar.googleusercontent.com/scholar?q=cache:f_OjgZEW2EYJ:scholar.google.com/+hsrp+protocol&hl=es&as_sdt=0,5&as_ylo=2017

[10] J. Pavlik, A. Komarek, V. Sobeslav, y J. Horalek, «Gateway redundancy protocols», en *2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI)*, nov. 2014, pp. 459-464. doi: 10.1109/CINTI.2014.7028719.

[11] «rfc4271». https://datatracker.ietf.org/doc/html/rfc4271#page-4 (accedido jun. 15, 2021).

[12] «3. Distribución de Números de Sistema Autónomo (ASN)». https://www.lacnic.net/546/1/lacnic/3-distribucion-de-numeros-de-sistema-autonomo-asn (accedido jun. 16, 2021).

[13] «rfc1930». https://datatracker.ietf.org/doc/html/rfc1930 (accedido jun. 16, 2021).

[14] «rfc4893». https://datatracker.ietf.org/doc/html/rfc4893 (accedido jun. 16, 2021).

[15] I. Ristanti Julia, H. Bayu Suseno, L. Kesuma Wardhani, D. Khairani, K. Hulliyah, y A. Taufik Muharram, «Performance Evaluation of First Hop Redundancy Protocol (FHRP) on VRRP, HSRP, GLBP with Routing Protocol BGP and EIGRP», en *2020 8th International Conference on Cyber and IT Service Management (CITSM)*, oct. 2020, pp. 1-5. doi: 10.1109/CITSM50537.2020.9268799.

[16] «Innovations: xDSL Technology and The Internet (Part I)». https://www.copper.org/publications/newsletters/innovations/1998/04/xdsl-tech01.html (accedido jun. 20, 2021).
[17] «Gigabit Passive Optical Network (GPON) | Optical Solutions Australia». https://www.opticalsolutions.com.au/gigabit-passive-optical-network-gpon/ (accedido jun. 20, 2021).
[18] «Configuring and Verifying the BGP Conditional Advertisement Feature», p. 10.
[19] *Norberto P. Padín, Technical Solutions Architect, «Highly Available Wide Area Network Design».*

LISTA DE FIGURAS

LISTA DE CUADROS DE TEXTO